Disclaimer

Contents

Foreword

As the inaugural Chief of Joint Capabilities, I am pleased to introduce this issue of the *Australian Defence Force Journal*. Its publication coincides with the formation of Joint Capabilities Group, established in July 2017 as a part of the Australian Defence Force Headquarters.

Joint Capabilities Group is about maintaining a military warfighting edge, not a corporate edge. We are the linchpin of key capabilities that underpin our joint force, with our success or failure directly affecting those we support. We support Defence and Command by providing education and training, healthcare and logistics, and by ensuring that we lead in information warfare. We undertake these activities so as to assist our allies and protect against those who seek to do us harm.

It is important that the ADF's professional interests are reflected in the *Australian Defence Force Journal*. This publication has an established reputation as the journal of 'the profession of arms in Australia', which increasingly in recent years has focused on the 'joint' aspects of contemporary operations. I encourage all members of the ADF to contribute to our professional discourse through contributions to the *Journal*.

As identified in the *First Principles Review*, a critical aspect of the development of joint capabilities is a greater investment in intelligence, surveillance, reconnaissance, electronic warfare, space and cyber capabilities. The 'force multiplier' effect of C4ISR—command, control, communications, computers, intelligence, surveillance and reconnaissance—and an emphasis on building network-centric warfare capability lie at the heart of ADF capability development.

I am pleased that this issue of the *Journal*—and indeed most recent issues—contain articles on one or more of these capabilities, with cyber in particular being extensively addressed. I would welcome further discussion in future issues on these important joint capabilities, which will enable the ADF to exploit its 'knowledge edge' and better coordinate and synchronise its future military operations.

Air Vice-Marshal Warren McDonald, AM, CSC
Chief of Joint Capabilities

Chair's comments

Welcome to Issue No. 202 of the *Australian Defence Force Journal.*

I am particularly pleased that this is the first 'regular' edition in our new-look format, which is also being published in both electronic and hard-copy versions. The Board is optimistic that the reinstatement of the printed version will encourage an increase in contributions, recognising that many authors are keen to see their submissions published in the printed form.

This issue contains some very good quality articles on a range of topics, including several from relatively junior officers. The Board has selected the article by Sub Lieutenants Nick Boswell, James Keane and Connor Mooney-Collett as the best article in this issue. They will receive a certificate signed personally by the Chief of the Defence Force and the Secretary of the Department of Defence. The Board also 'highly commended' the article by Warrant Officer Class 2 Aaron Waddell, who will receive a similar certificate.

Readers will note that in addition to the redesigned format, we have made some structural changes to this issue, which will be replicated on the *Journal*'s new website (details of which will be publicised shortly).

In particular, we have grouped like contributions, in this case under the heading 'Cyber security in the ADF'. We intend to continue this practice and invite contributions for the November/December issue—ideally by mid-September—on the theme of veterans' mental health. Contributions can be in the form of articles or shorter commentary/opinion pieces, which could be <1500 words and without the need for endnotes. Of course, we will also welcome contributions, either as articles or shorter commentaries, on the normal range of general topics.

As always, we have also included a selection of reviews of books provided to the *Journal* by publishers both in Australia and overseas. If you are interested in becoming a reviewer, please send your details to editoradfjournal@internode. on.net

In closing, I would like to thank Colonel Andrew Hocking and Group Captain David Millar for their much-appreciated work as members of the Board. Their replacements are Colonel Ashley Collingburn and Group Captain Andrew Gilbert, representing Army and Air Force respectively. I would also like to welcome Dr Lacy Pejcinovic who, as Assistant Director Research at the Centre for Defence and Strategic Studies, is Defence's manager for administration and publication of the *Journal*.

I hope you enjoy this issue.

Ian Errington, AM, CSC
Principal
Centre for Defence and Strategic Studies
Chair Australian Defence Force Journal Board

Cyber test and evaluation in a maritime context

Sub Lieutenant Luke Boswell, Royal Australian Navy
Sub Lieutenant James Keane, Royal Australian Navy
Sub Lieutenant Connor Mooney-Collett, Royal Australian Navy

Since the development of the Internet in the 1960s, modern states have become completely dependent on their ability to communicate in the global information domain. Cyberspace, a key component of this domain, is defined in the ADF's 'Defence strategic cyber operations policy 2010' as:

> Cyberspace is a component of the global information domain consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers, and their resident data (ADF, 2010).

At the same time, technology has changed the way that nations project influence and power. This has driven significant changes within all modern navies, including the Royal Australian Navy (RAN). However, the accelerating growth of cyberspace is dynamic and unpredictable, which means that navies (and others) must continue to adapt in order 'to effectively conduct maritime operations in the information age' (Kirk, 2016).

This article outlines the significance of the effective management of cyber, particularly for the RAN, developing an argument for cyber as a key component of operational testing and evaluation. After introducing the key concepts, the article explores the drivers of change within the RAN, which have been categorised into three significant technology shifts: integration, connectivity and dependence. The article then discusses the role of testing and evaluation in achieving cyber-worthy capabilities, and introduces two frameworks, before concluding with a number of recommendations.

The militarisation of cyber

The world has progressed from analogue to digital, radio to fibre, and from phone lines to data packets. But information has continued to

be captured, stored and transmitted. In the context of information warfare (IW), where 'decision superiority' is predicated on information advantage, cyber technologies both reduce the material resources required to develop and deliver effects, and increase the speed with which those threats can evolve. In this information domain, cyber-weapons can also be used to destroy or disable critical infrastructure, which previously was only vulnerable to physical damage.

However, it is rarely possible to identify the source of a cyber-attack with certainty. Therefore, building an accurate picture of the threat in cyberspace is complicated, not least because of the blurring between state and non-state actors. Also, malicious activity in cyberspace is not just contained to the intangible domain of information. The widespread embarrassment of cyber-related failures has spilled into the physical domains. Consider the destruction of nuclear centrifuges in an Iranian enrichment plant from the Stuxnet virus. An increasing amount of civilian infrastructure, such as telecommunications, banking and transportation systems, is also increasingly vulnerable.

Within modern militaries, the trend towards cheap, modular and flexible networked and reconfigurable systems has driven acquisition patterns, including in the RAN. For example, where a valve may have been controlled by a mechanical switch in the past, it is now controlled by an electronic switch connected to a computer. Unlike their predecessors, these new systems exist in cyberspace and hence are vulnerable to cyber-attack.

The role of testing and evaluation

A common misconception is that all vulnerabilities can be identified and addressed before a system is deployed. Most vulnerabilities can be mitigated through good design and extensive testing. However, there are variables which exist only while the system is operational, the most significant of these being human error. This, combined with regular configuration change, necessitates an operational approach to cyber testing and evaluation.

To achieve their intent, a malicious actor may take advantage of one or more vulnerabilities. Where an actor has both the intent and capability to

exploit a vulnerability, this is known as a threat. A single vulnerability in isolation may be irrelevant in the same way an unlocked door may be of no interest to anyone. However, when combined with other vulnerabilities, it may be the crucial ingredient. Consider an unlocked vault inside the building with an unlocked door; this combination of vulnerabilities is potentially devastating. Therefore, it is essential to guide any search for vulnerabilities from an understanding of intent, which necessitates the testing of a system while it is operating normally, that is, configured as it is when deployed.

A common guide to cyber-security is Kerckhoff's principle, reproduced as Shannon's maxim, that 'one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them' (Shannon, 1949). The idea being that a system should be secure even if everything about the system, except the key, is public knowledge. Maintaining secrecy with respect to the design and configuration of a network is merely a layer of security, and not intrinsically any guarantee of its security. Hence, monitoring for malicious activity is not enough. It must be assumed that any system is capable of being compromised. Capabilities must, therefore, be engineered with the ability to recover from and continue functioning in a degraded information environment.

Cyber in the maritime domain

Warships are not beyond the reach of cyberspace, even at sea, and the RAN is obviously no exception. The implications of a cyber-attack stretch beyond the operational to the potential reputational impact on the RAN and its strategic alliances. When cooperating with other forces in a joint or combined task force, it will be essential that Australia's capability does not represent a potential vulnerability, and therefore a risk to the broader mission and other forces.

Increasing demand for more flexible maritime capability has driven changes within the RAN, which are broadly categorised as three significant technology shifts, namely the adoption of integrated architecture, increasing connectivity to external systems, and a deeper dependence on defence industry for logistics support. Each of these has contributed to the breaking down

of information 'silos', which results in greater interdependence between systems. Even though these shifts are a result of technological progress, they each represent sources of cyber risk to the RAN.

Integration

Many systems aboard modern warships are connected to each other and integrated into a single architecture. This is a result of the shift from federated towards integrated architectures. The most significant reasons for this are that integrated architectures are cheaper, more modular and reconfigurable in a way that allows for more capable platforms to be developed. However, this flexibility also represents a source of cyber risk due to vulnerabilities being difficult to find or potential adverse interactions between systems. This is because it is impractical to precisely define the relationships and interactions between systems during design. The greater degree of connectedness between the systems in an integrated architecture also means that vulnerabilities in one system can propagate to another.

The management of cyber risk must be considered throughout the whole capability lifecycle and not just during the acquisition phase. Securing a poorly designed system can be prohibitively expensive. Every time a system is added, its software modified, or the network itself reconfigured, there is an opportunity for new vulnerabilities to arise. For example, consider the installation of new washing machines with automated alarms being integrated into a ship's monitoring network. If the washing machine software is poor quality, it may contain a vulnerability which could adversely affect the ship's monitoring system. Establishing requirements for cyber-security has, among other benefits, the additional outcome of improving the quality of software that is developed. It is precisely the flexible nature of interactions between systems that increases the cyber risk a warship is exposed to.

Connectivity

The operational environment is inherently connected, with both joint and combined forces routinely operating together. To support this operational environment, maritime capability is becoming increasingly connected to systems in the sea, air, land and space domains. In addition, terrestrial networks have an increasing support and operational role on ship activities. Every transmission to and from a ship presents an opportunity for a hostile actor to either disrupt, deny, degrade, destroy or deceive the ship. This is because there is potential for a skilled actor to manipulate the electromagnetic spectrum or other transmission medium in a way that adversely affects the ability of the ship to perform its mission effectively.

Dependence

An increased dependence on support from external organisations has resulted from accelerating RAN acquisition of complex capability while simultaneously reducing the uniformed footprint. Core functions that were previously undertaken by the RAN, such as maintenance and logistics, are now being fulfilled through external organisations. These services are increasingly being transacted in cyberspace as Defence brings products and services online. For example, 'WebForms' are rapidly taking the place of paper to facilitate storing, processing and tracking of information. This progress is necessary to support additional capability with reduced manning, and it facilitates an increased volume and quality of communication between and within Defence units and external organisations. However, the impact of these services needs to be considered from a cyber security perspective to understand the risks that the RAN is exposed to.

By facilitating the breaking down of information 'silos', technological adoption facilitates an increased flow of information between support organisations. However, this greater degree of interconnectivity means that any vulnerabilities in one system can more readily propagate to and compromise other systems in the network. Consequently, the security of information now stored in cyberspace needs to be considered as there is increased dependence on connected systems and as integrated organisations are trusted to manage their cyber domain with integrity.

IW continues to play a significant role in the maritime context, especially as the RAN has moved

into cyberspace with more integrated, connected and dependent capability. It follows that the RAN must be proactive in its pursuit of measures to manage risks in cyberspace. The avenue proposed by this article for effective cyber defence is for cyber security to be introduced through Navy engineering and, specifically, for cyber testing and evaluation to be implemented as part of the seaworthiness framework to address the challenges associated with operating in the 21st century.

Testing and evaluation towards cyber-worthiness

The concept of 'cyber-worthiness' may be considered a cyberspace analogy to 'seaworthiness'. The implication being that RAN capability must be prepared to meet potential adversaries in cyberspace to continue the fight at sea. Accordingly, cyber-worthy should be included within existing policy alongside fitness for service, safety, and environmental compliance. This would ensure that cyber is considered at every stage of the capability lifecycle and as part of the Sea Release Assurance Framework. To achieve this, operational test and evaluation needs to be the primary driver for ensuring that RAN maritime capability is cyber-worthy.

As an analogy to seaworthiness, a ship that is cyber-worthy can operate effectively even while in a contested, degraded or operationally limited information environment. For maritime capability which depends on cyberspace to operate effectively, this would suggest that the ship (and its supporting elements) is resilient to adverse conditions in cyberspace. Therefore, cyber-worthiness could be seen as the process which assures that maritime capability is cyber-worthy; that is, well-suited for operations, and resilient to adverse conditions within cyberspace.

Paul Kirk asserts that a key challenge for the implementation of the RAN's 'Information warfare: Master Plan 2030' with respect to cyber has been an absence of clear strategy and

end-states (Kirk, 2016, p. 5). So the concept of cyber-worthiness and its incorporation into existing policy would seem to be the right way to respond to this challenge. This would require that 'objective quality evidence', specific for cyber, be developed as part of the Sea Release Assurance Framework, with the evolution of operational test and evaluation the natural candidate to drive this strategy.

The role of operational testing and evaluation in cyber-worthiness

Commenting on the importance of operational testing, the US Department of Operational Testing and Evaluation has asserted that:

> The cyber threat has become as real a threat to US military forces as the missile, artillery, aviation and electronic warfare…. Real-world cyber adversaries regularly demonstrate their ability to compromise systems and inflict damage. Operational testing must examine system performance in the presence of a realistic cyber threat (cited in Joiner, undated).

It follows that the tools of operational testing and evaluation, such as penetration testing and security audits, need to be employed to ensure that the capability is cyber-worthy. Existing RAN policy was originally developed for assets with long development times, defined operating envelopes, and long in-service life. However, the policy obviously now needs to be adapted to evolving technology, such as a process outlined at Figure 1.

The below is a simplistic illustration of the process used to evaluate an individual capability in a realistic environment. These steps are explained further as follows:

- **Understand requirements.** Develop the cyberspace context the system operates in. Examples include what systems are integrated, and what role the system has in supporting the mission.
- **Characterise attack surface.** Understand the interface between integrated systems

| Understand requirements | → | Characterise attack surface | → | Identify vulnerabilities | → | Conduct penetration testing | → | Operational assessment |

Figure 1: Operational test and evaluation process for cyber (Christensen, 2016)

and the potential methods an adversary could use to penetrate the system.

- **Identify vulnerabilities.** Analyse the system for potential failure modes or conditions which an adversary may use to their advantage.
- **Conduct penetration testing.** Interrogate the system to exploit vulnerabilities.
- **Operational assessment.** Evaluate test results to assess the ability of the system to resist realistic cyber threat.

Christensen's model represents a good reference for the RAN to develop its own process. However, establishing a process to evaluate individual capability is only the first step towards cyber-worthiness. In addition, there must be an overarching strategy or framework to guide its implementation.

The 'five pillars' framework

Symantec, a leader in commercial anti-virus software, has suggested a 'five pillars' framework to encourage organisations to revisit their security posture and move their focus towards cyber-resilience (see Figure 2). This framework explicitly avoids prescriptive behaviour, such as checklists, but instead promotes a risk-aware approach through evaluations based on a realistic picture of the threat environment as built and understood through active cyber intelligence (Kirk, 2016). This is where operational testing and evaluation would represent a natural fit for driving such an approach to cyber-worthiness within the RAN.

The five pillars represent key functions to manage cyber risk through a continual process of refinement, as explained as follows:

- **Identify.** Conduct an infrastructure and information assessment to establish a baseline understanding of known security vulnerabilities.
- **Protect.** Develop and implement safeguards for critical infrastructure and services to limit or contain the impact of an attack. How up to

date measures are for a system in its current configuration is a measure of how well the system is protected.

- **Detect.** Develop and implement processes to identify an attack in progress (real time), assess the systems that are affected (near-real time) and ensure appropriate and timely response. To achieve this, networks should be continuously monitored and relevant activity logged as indicators of a potential attack or for future analysis.
- **Respond.** The ability to respond to a cyber-attack and remediate effects is a measure of cyber-worthiness. This requires the ability to understand the likely effects of cyber-attack and develop a plan to coordinate a response.
- **Recover.** Develop and implement plans to restore data and services that may have been impacted during a cyber-attack.

This section has developed the concept of cyber-worthiness and argued for operational testing and evaluation as a key driver towards its implementation. Regardless of the path taken, the costs for delay or inaction are great. Therefore, the following section outlines three specific recommendations for RAN consideration.

Integrating cyber operational testing and evaluation

The RAN has adopted increasingly complex technological capabilities, however, its adoption of industry best practices has not kept pace. This is a type of technical debt, where the interest is unnecessary cyber risk exposure and the opportunity cost of poor technology utilisation.

In 2014, the Australian Signals Directorate published a document titled 'Strategies to mitigate targeted cyber intrusions', which outlined specific recommendations to combat elementary threats in cyberspace (Australian Signals Directorate, 2014). In addition to implementing those recommendations, this article suggests the RAN should consider the following.
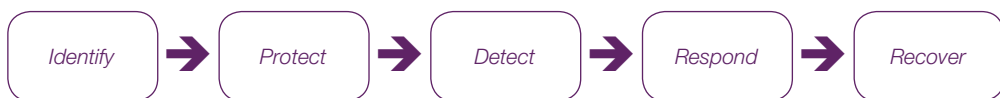
Identify → Protect → Detect → Respond → Recover

Figure 2: The 'five pillars' framework to evaluate individual capability (Symantec, 2014)

Establish RAN cyber capability

The RAN needs to develop its own cyber capability, which should include the concept of 'cyber-worthiness'. The reasons are three-fold. Firstly, effectively combating cyber demands a deep technical understanding not only of the technology but also the operating environment. This complexity cannot be outsourced to another department or organisation. Secondly, the RAN is ultimately accountable to deliver seaworthy material. This requires that decision-makers at every level of the command chain be aware of cyber. Responsibility cannot be outsourced because, like safety, it is the responsibility of everyone to practise good security. To achieve this, the RAN needs to ensure adequate training and develop a cyber-aware culture. Finally, cyber specialists must be embedded, or at least made available, within acquisition and sustainment projects, in order to facilitate a process of certification and accreditation of cyber-worthy material.

Integrate cyber-worthy into the seaworthiness framework

The seaworthiness framework is the natural place to integrate the concept of cyber-worthiness. Cyber-security must be as fundamental as ship stability or safety. Ideally, requirements for cyber-worthiness would be established early in the acquisition and design processes. However, existing capability must also be considered where it is vulnerable to cyber-attack. Addressing issues proactively, before they are realised, is far cheaper than the alternative.

Some consider cyberspace to be the realm of specialists with techniques that are difficult to understand and apply. However, there are established and readily adopted controls which do not require expert skills. These practices have analogies such as key control or monitoring logs. Essentially, good cyber-security is largely the diligent application of basic controls to manage risk (Kirk, 2016).

Collaborate with existing leaders to develop RAN policy

RAN policy is sparse on cyber at an unclassified level. Where cyber is employed, it is through specialists or by an external organisation. However,

this is an unsustainable model to deliver capability that is cyber-worthy. While specialists and external organisations can provide support in critical areas, they cannot be responsible for the entire RAN. Moreover, while much of the discussion on cyber is classified, this article has argued that to establish cyber-worthiness as a process, underlying every maritime capability, knowledge needs to be embedded in Navy's people.

To that end, the RAN must collaborate with existing leaders in cyber to develop its policy. The RAN has a unique operating environment but appropriating experience elsewhere would assist in developing relevant policy and practices. Industry generally has adapted quickly to cyberspace, and expertise already exists within Australia Government departments. The US Department of Defense has also been supportive of RAAF efforts on the Joint Strike Fighter project. The RAN should leverage these and other relationships to gain access to additional expertise. The importance of such collaboration has been summarised as:

> As our dependence on information networks increases, it will take a team to eliminate vulnerabilities and counter the ever-growing threats to the network. We can succeed in securing it by building strong partnerships between and within the private and public sectors, encouraging information sharing and collaboration, and creating and leveraging the technology that affords us the opportunity to secure cyberspace (Alexander, 2013).

Conclusion

With cyber-attacks on Australia and Australians increasing, even crossing into the physical domains, it is evident that the RAN is not immune. Technology shifts in the maritime domain have driven new and advanced capabilities, which have increased integration, connectivity and dependence on cyberspace, representing a significant risk. It follows that a modern warship is vulnerable to these risks, even at sea.

This article has argued for the concept of 'cyber-worthy' to be included in existing RAN policy, alongside fitness for service, safety, and environmental compliance. It has also argued that operational testing and evaluation should be the key driver of cyber-worthiness.

Employing the tools of operational testing and evaluation, such as regular penetration testing and security audits, provides the best way to manage this risk.

Two frameworks have been presented which explicitly avoid promoting prescriptive behaviour but instead deliver a risk-aware approach. The article has also suggested three specific recommendations for RAN consideration, namely that the RAN develops its own cyber capability, that cyber-worthiness be integrated into the seaworthiness framework, and that the RAN collaborates with best-practice leaders to develop its policy for cyber-worthiness.

Cyberspace represents a serious threat. However, as Australia and like-minded countries increasingly rely on cyberspace to enhance its warfighting capability, the opportunity arises to manage the risks of operating in cyberspace and, indeed, to turn Australia's command of the new battlespace to its benefit.

Sub Lieutenant Luke Boswell joined the RAN in February 2016 and is currently serving as an Assistant Weapons Electrical Engineering Officer on HMAS Adelaide. He is under training to be a professional engineer within the RAN, after graduating from The University of Melbourne with a Bachelor of Science and Master of Engineering degrees. While at university, he was President of the Electrical Engineering Student Society.

Sub Lieutenant James Keane joined the RAN while studying a Bachelor of Engineering (Honours) in Naval Architecture at the Australian Maritime College (AMC). He was president of the AMC Autonomous Technologies Society and involved in a number of maritime automation projects, with the results of his research published, including in China and the US. He is currently completing Engineering Officer training while serving as Assistant Marine Engineering Officer on HMAS Leeuwin.

Sub Lieutenant Connor Mooney-Collett joined the RAN in June 2014 and is currently serving as an Assistant Weapons Electrical Engineering Officer on HMAS Stuart. He studied a Bachelor of Engineering (Electrical) at the University of Queensland, where he was a member of the Electrical Engineering Student Society and worked on a number of computing and electronics project teams.

References

Alexander, K., (2013), 'Commander of US Cyber Command and National Security Agency Director, General Keith Alexander, to Keynote Day One of Black Hat USA 2013', *PR Newswire* [website], 14 May 2013, available at <http://www.prnewswire.com/news-releases/commander-of-us-cyber-command-and-national-security-agency-director-general-keith-alexander-to-keynote-day-one-of-black-hat-usa-2013-207361951.html> accessed 18 November 2016.

ArsTechnica (2016), 'Cisco confirms NSA-linked zeroday targeted its firewalls for years', *ArsTechnica* [website], available at <http://arstechnica.com/security/2016/08/cisco-confirms-nsa-linked-zeroday-targeted-its-firewalls-for-years/> accessed 4 October 2016.

Australian Broadcasting Corporation (2013), 'Brandis confident ASIO "dealt with" hacking attack', *ABC* [website], 29 May 2013, available at <http://www.abc.net.au/news/2013-05-29/brandis-briefed-by-asio-on-china-hacking-claims/4719886> accessed 4 October 2016.

Australian Broadcasting Corporation (2016), 'Turnbull confirms weather bureau cyber attack', *ABC* [website], 21 April 2016, available at <http://www.abc.net.au/news/2016-04-21/australia-admits-it-can-launch-cyber-attacks-turnbull/7343620> accessed 4 October 2016.

Australian Centre for Cyber Security (2016), 'Proposal for an Australian Cyber Corps', *University of New South Wales at Australian Defence Force Academy* [website], available at <https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/publications/Australia%20cyber%20civil%20corps%20Draft%20concept.pdf> accessed 4 October 2016.

Australian Cyber Security Centre website available at <https://www.acsc.gov.au/> accessed 14 April 2017.

Australian Cyber Security Centre (2016), 'ACSC threat report 2016', *Australian Cyber Security Centre* [website], available at <https://www.acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf> accessed 17 November 2016.

Australian Defence Force (2010), 'Defence strategic cyber operations policy 2010: Australian Defence cyber operations lexicon', unclassified draft in possession of author(s).

Australian Signals Directorate website available at <https://www.asd.gov.au/> accessed 14 April 2017.

Australian Signals Directorate (2014), 'Strategies to mitigate targeted cyber intrusions', *Australian Signals Directorate* [website], available at <http://www.asd.gov.au/publications/Mitigation_Strategies_2014.pdf> accessed 26 October 2016.

CERT Australia website available at <https://www.cert.gov.au/> accessed 14 April 2017.

Christensen, P., (2016), 'ZEIT8231 - course notes, systems development practices closely aligned to T&E', University of New South Wales at Australian Defence Force Academy, Canberra, held by author(s).

Department of the Prime Minister and Cabinet, 'Australia's cyber security strategy: enabling innovation, growth and prosperity', *Department of the Prime Minister and Cabinet* [website], 2016, available at <https://cybersecuritystrategy.dpmc.gov.au/> accessed 14 April 2017.

Engadget (2016), 'Critical security flaw found in Lenovo PCs … again', *Engadget* [website], available at <https://www.engadget.com/2016/07/04/critical-security-flaw-found-in-lenovo-pcs-again/> accessed 4 October 2016.

Joiner, K., (undated), 'Integrating cyber survivability into future ADF platform development and acceptance', *University of New South Wales at the Australian Defence Force Academy* [website], available at <https://www.unsw.adfa.edu.au/australian-centre-for-cyber-security/sites/accs/files/uploads/Cyber-survivability%20TnE%20-%20Dr%20Joiner%20PPP.pdf> accessed 18 November 2016.

Kirk, P., (2016), 'Navy information warfare: developing an information warfare strategy for the Royal Australian Navy', Master's thesis at the University of New South Wales at Australian Defence Force Academy, abstract available at <https://oatd.org/oatd/record?record=oai%5C%3Aunsworks.unsw.edu.au%5C%3A1959.4%5C%2F56982> accessed 14 April 2017.

Lehmann, M., (2014), 'Chinese national interests and cyber capabilities: a 'red team' future', *Australian Defence Force Journal*, Issue No. 195, pp. 12-20.

Nguyen, N., (2015), 'Evolution of the battlefield: strategic and legal challenges to developing an effective cyber warfare policy', *Australian Defence Force Journal*, Issue No. 196, pp. 60-9.

Prime Minister Malcolm Turnbull, M., (2016), 'Cyber security strategy', *Prime Minister* [website], 21 April 2016, available at <https://www.pm.gov.au/media/2016-04-21/australias-cyber-security-strategy> accessed 14 April 2017.

Royal Australian Navy (2011), *Information warfare Master Plan 2030*, Defence Publishing Service: Canberra.

Shannon, Claude (1949), 'Communication theory of secrecy systems', *Bell System Technical Journal*, Vol. 28, No. 662.

Sydney Morning Herald (2016), 'Census cyber attacks likely from low-level hacktivists but origins may never be proved, experts say', *Sydney Morning Herald* [website], 11 August 2016, available at <http://www.smh.com.au/federal-politics/political-news/census-cyber-attacks-likely-from-lowlevel-hacktivists-but-origins-may-never-be-proved-experts-say-20160811-gqqkag.html> accessed 4 October 2016.

Symantec Corporation (2014), 'The cyber resilience blueprint: a new perspective on security', *Symantec* [website], available at <https://www.symantec.com/content/en/us/enterprise/white_papers/b-cyber-resilience-blueprint-wp-0814.pdf> accessed 27 October 2016.

Thompson, M., (2012), 'The cyber threat to Australia', *Australian Defence Force Journal*, Issue No. 188, pp. 57-70.

Developing cyber-security policies that penetrate Australian defence acquisitions

Stuart Fowler
Captain Craig Sweetman, Australian Army
Flight Lieutenant Sibi Ravindran, Royal Australian Air Force
Dr Keith F. Joiner, CSC, University of NSW
Dr Elena Sitnikova, Australian Cyber Security Centre

Technological edge on the battlespace has been one of Australia's military advantages within Southeast Asia. This is partly due to the relative larger size of the Australian economy and its ability to procure advanced defence systems compared to the region. However, by 2030, it is envisaged that Australia will slip to being the 23rd largest economy in the world, slightly smaller than Thailand's and similar in size to Malaysia's (Hawksworth and Chan, 2015). This will significantly erode Australia's financial advantage, as other regional nations will be able to afford advanced weapon systems, including cutting-edge cyber capabilities.

As all nations continue to develop their offensive cyber capabilities, Australian defence systems will become increasingly vulnerable. Joiner (2017) has reviewed the options of the Australian Department of Defence (Defence) for cyber-security test and evaluation and has highlighted that there are significant difficulties in attributing and predicting the final effects of cyber threats

that are currently manifesting, making it very difficult for Australia to rely on the deterrent effect of a potential response from an ally like the US.

In an attempt to address these challenges, cyber security has become an increasing focus for Defence. The release of the *2016 Cyber Security Strategy* (Commonwealth of Australia, 2016) and the *2016 Defence White Paper* (Australian Government, 2016) shows that decision-makers at all levels have demonstrated an understanding of the importance of cyber security. However, this enthusiasm for protecting Defence capability from hostile cyber attacks has yet to translate into a comprehensive and coordinated set of policies at the working level (Joiner, 2017).

This is not necessarily due to ignorance or indifference. Translating the aspirations of a cyber-hardened and cyber-resilient arsenal of military systems into a workable and robust set of policies is a difficult challenge. It is amplified

by the large expenditure of public funds and the lengthy acquisition process typically associated with Defence's capability development, often cultivating a culture of risk aversion and an environment where a cyber-resiliency policy cannot simply be iteratively developed over a number of projects in any reasonable timeframe. If new Defence capability lifecycle policies are not implemented properly, cyber resiliency may be overlooked and a vulnerability may develop, or there may be significant wastage that does not materially contribute to the cyber resiliency of the capability being procured.

This article examines how Australian defence acquisition policies can adapt, mainly using US Department of Defense experiences, to deal more effectively and systematically with cyber resilience.

Project lifecycle challenges

Capability development

The capability lifecycle within Defence begins with an analysis of a desired capability concept and the development of system requirements for a solution that is ultimately procured through contracts. While this process needs to account for the entire lifecycle, there are general challenges that are faced during the early design stages that can impact the cyber resilience of major capabilities.

The capability lifecycle is based on the 'waterfall' project management model, which is suited to projects where the requirements and needs do not change over time (Bergmann, 2013). Due to the dynamic nature of the threat in a hostile cyber environment, agile iterative development practices are more suited for the cyber-security aspects of procurements wherever there are software-intensive subsystems.

Obsolescence and vulnerability management of software and hardware must be considered, and systems under evaluation must be future-proofed as much as possible. Most projects establish a technology baseline to support system integration, and test and evaluation. When this baseline is coupled with delays in acquisition, the resultant system accepted by Defence may be outdated and have known vulnerabilities,

creating unnecessary risk to the capability, and potentially depriving Defence of a technological edge.

Of course, it would be misguided to see agile engineering methodologies as a panacea for the cyber-security challenges faced by Defence. On large, complex and tightly integrated systems, the level of design volatility inherent in the agile methodology can be a costly venture if contractual arrangements do not accommodate this volatility. Much of the traditional systems-engineering process is about controlling the level of design volatility to minimise risk. However, this process will need to evolve if it is to adequately address the challenge of cyber security.

An agile approach can require an increased ability to manage change, as change must be rapidly folded back into the system requirements and design to maintain the proper cadence of iterative releases. It seems clear that rising to this challenge will require a marriage between agile processes and traditional systems-engineering. This remains an ongoing research area. However, perhaps specific subsystems can follow an agile process within the confines of the requirements and constraints allocated to the subsystem, albeit with a traditional systems-engineering process at the system level.

Defence's requirements

One tempting solution for incorporating cyber resilience into Defence's capability lifecycle is simply to place cyber-resilience requirements within the functional performance specification which then becomes the basis of a prime contract with defence industry. Digging deeper, we find that it is not obvious what those requirements should be and how they should be decomposed. There is a temptation to incorporate general requirements that form the basis of security certification and accreditation, such as the *Information Security Manual* (Australian Signals Directorate, 2016) and the various emissions security standards, as part of the system specification.

However, these sorts of requirements offer thousands of controls, many of which may not be applicable to all systems, and often give little guidance on which of these controls are most important within the context of the specific capability program or known threats to the system.

Additionally, these controls focus primarily on ensuring the confidentiality of classified networks, rather than the integrity and availability of safety-critical or mission-critical systems, making them largely unsuitable for specifying cyber resilience.

More worryingly, due to their risk-based nature, it is entirely possible to meet these sorts of prescriptive requirements without providing a sufficient level of cyber resilience or even cyber-defence testing. The *Information Security Manual* is a strong resource when applied to strategic or corporate ICT systems but a reliance on this document to ensure cyber resilience of deployed systems is a flawed model.

One way to overcome this would be to specify the need for cyber resilience in a general sense, where a desired output is specified—a system which is cyber resilient—rather than specific input-driven requirements. The major downside to this approach is that this sort of requirement is not particularly measurable or quantifiable, making it difficult to formally verify and validate. To examine this issue more thoroughly, we can look at how similar problems have been addressed within broader Defence acquisitions; and the two parallels drawn here are with system safety and system survivability.

System safety shares the problem of being difficult to specify through requirements, and having a high-level desired output that can be difficult to measure, that is, that a system must be safe. It also operates at the intersection of defined engineering standards and risk assessments, much like cyber resilience. System safety is typically handled as part of the contractual 'statement of work', rather than as a technical system requirement, and this tends to achieve a more holistic outcome. The safety risk assessment, review and acceptance process itself is mandated contractually, and culminates in a safety case report that summarises the safety analysis performed, the state of any safety controls and the residual risk levels.

By necessity, system-safety processes take a holistic approach that, when done properly, helps transcend contractual boundaries. Taking a similar approach to incorporating cyber resilience into Defence's capability lifecycle has some merit, as it would allow for a more

consistent approach across projects, encourage a collaborative approach between contractual parties, and provide a standard framework for which cyber-related risk is captured.

The US Department of Defense has recently incorporated into its standard acquisition policies the concept of a Program Protection Plan (Reed, 2015; Brown *et al,* 2015), which is a customer-owned document that captures cyber-related issues, plans and resolutions. The program protection plan is a consistent and comprehensive plan that covers a wide range of project-specific cyber-security information, from classification guidance to threat intelligence, supply chain, architecture and risk assessment, and can be viewed as analogous to a safety case but in the cyber-security domain.

If a program protection plan could be developed in parallel with an operational concept document and functional performance specification, the maintenance of the program protection plan, along with other process-based cyber-security issues such as risk assessments, certification and accreditation, could be mandated within the contractual statement of work for the prime contractor. This would free up the functional performance specification to contain specific functional requirements that support the cyber resilience of the system, while ensuring the foundational 'cyber-hygiene needs' are still flowed down to the contractor.

System survivability, the ability of a system to survive within a contested environment, also shares some challenges with cyber resilience. Both require continued operation within an unpredictable situation where a hostile entity is actively trying to degrade or destroy the system by evolving the threat. Again, this can be a difficult attribute to specify in a requirement that does not atrophy quickly, because the concept of setting a minimum acceptable floor for system survivability is difficult to rationalise, given the ambiguous constraints of active hostile action.

Any honest measure of survivability would shift over time as hostile capabilities increased, and it is an attribute that needs to be maximised within other constraints, rather than simply meeting an arbitrary minimum level. The standard approach to system survivability is to treat it as a key performance parameter, or a measure

of effectiveness, within the system itself. Again, this is often treated separately from functional requirements.

The US has recently incorporated cyber resilience and cyber survivability into its standard system survivability key performance parameter (Office of the Secretary of Defense, 2014). Contractors are required to show their performance against these parameters at project milestones and design reviews, and are required to meet thresholds for these parameters or risk their projects being defunded. While this may not be directly applicable to the Australian context, given different funding arrangements, there is a strong argument for including a cyber-survivability or cyber-resilience key performance parameter in acquisition contracts, perhaps with incentive payments tied to the level at which the key performance parameter is met.

Architecture and design

A striking difference between the Australian and US acquisition contexts is that Australian projects are more focused on the integration of off-the-shelf components or the acquisition of existing platforms from international partners (Joiner, Sitnikova and Tutty, 2016, p2). The reluctance, both of prime contractors and the government, to carry the risk of significant development activities in a climate of off-the-shelf acquisitions can place a constraint on the cyber-security design and development of a cyber-resilient architecture. This approach drives architectures during the tendering phases of an acquisition project to focus on off-the-shelf solutions that provide lower costs while meeting the minimum functional requirements.

The trade-off made in this methodology is the loss of flexibility in dealing with traditional non-functional quality attributes, such as cyber security and system safety, relying instead on test and evaluation to identify the risks being accepted. This approach can also increase the integration and interoperability risk for Defence if the off-the-shelf system uses proprietary protocols which can be difficult to integrate into wider Defence systems. Limited integration of systems may reduce the ADF's effectiveness in the battlespace, as an integrated force is a force multiplier and a cornerstone of the ADF's strategy and doctrine.

Strong and comprehensive cyber-security requirements need to be reinforced during tender evaluations by treating cyber resiliency as an integral capability discriminator. A tender reviewer would not compromise on the ability of a fighter plane or naval ship to dispense chaff or electronic countermeasures—and they need to take the same mindset when reviewing the ability of the system to resist cyber threats, as they can be just as damaging to mission effectiveness, safety and human life as kinetic threats.

Another challenge presented by the off-the-shelf approach is that there is very little ability to alter the native capabilities of the products, and many of the commercially available security appliances are poorly suited for defence systems; such as often assuming the presence of a stable internet connection or high data rate connectivity to a central server. A potential solution to this issue may be to start incremental risk reduction activities to look at this issue in advance of major capability projects.

An example of small-scale cyber-resilience projects is the High-Assurance Cyber Military Systems (HACMS) program developed by the US Defense Advanced Research Projects Agency. It is software designed to 'thwart cyber-attacks once deployed in any context, like a defence system or an unmanned aerial vehicle' (Paganini, 2014). The goal of the program is to develop technology for high-assurance cyber physical systems using 'clean slate, formal methods based approach to enable semi-automated code synthesis from executable, formal specifications' (Richards, 2016). In a demonstration using an unmanned helicopter, the program was able to prevent hackers from disrupting critical systems, despite the hackers having 'unfettered access' to the aircraft's computer (Slezak, 2015).

Similarly, the development of the Resilient Hull, Mechanical, and Electrical Securities (RHIMES) system by the US Navy was in response to the threat of an attack on control systems. RHIMES is a cyber-protection system with the design purpose of increasing the cyber resilience of shipboard mechanical and electrical control systems. The resilience is provided by preventing an attacker from taking control of programmable logic controllers that manage such functions as damage control, firefighting, anchoring, climate

control, electrical power, hydraulics, steering and engine systems. In the words of Rear Admiral Mat Winter, Chief of US Naval Research, 'the purpose of RHIMES is to enable us to fight through a cyber-attack' (Freeman, 2015).

Incremental risk reduction activities could focus on the development of a cyber-resiliency toolkit; a series of modules, components or products that are specifically crafted to work within the context of deployed systems that could be incorporated into a larger architecture in an off-the-shelf fashion. These modules would encompass traditional cyber-defence strategies, such as boundary protection, system management, intrusion detection, cyber-defence execution and cyber-state visualisation, as well as more complex cyber-resilience principles, such as adaptiveness, deception, diversity, unpredictability and reconstitution. The consistent implementation of these modules across projects would prevent the implementation of bespoke systems with a different look-and-feel on different platforms, and lessen the training burden of developing a new generation of cyber-smart military personnel.

Such projects could be completed through a partnership between the ADF's single-Services, strategic security agencies, defence industry, the Defence Science and Technology Group, universities and relevant security stakeholders, and could include research into self-hardening networks, tailored network-monitoring solutions or utilise modern virtualisation and container technologies to build on existing research into self-reconfiguring networks (Beraud *et al*, 2011) and self-reconstituting networks (Ramuhalli *et al*, 2013).

Test and evaluation

Cyber-security test and evaluation is another area where Defence's acquisition policy needs to be improved (Joiner, 2017). The vast majority of cyber-security test and evaluation within Defence's capability lifecycle is focused on ensuring confidentiality of information on classified networks though the certification and accreditation process. It is worth noting that a highly-critical system, such as a platform control system or navigation system, will typically not be assessed with as much rigour from a cyber-security perspective as a system that processes classified data. Cyber resiliency, however, needs to focus primarily on these critical systems to ensure they can continue to operate in a cyber-threat environment.

Joiner (2017) argues for cyber-security test and evaluation to become a larger part of the broader test and evaluation component of the capability lifecycle. This is an important step that needs to be taken, because it is the one point in the lifecycle where the cyber resilience of the system can be measured and reviewed. A robust cyber-security test and evaluation program can identify the residual risks in the system and validate the risk assessments that have been performed during early design activities.

The conduct of vulnerability and exploit assessments during detailed design reviews and developmental test and evaluation will increase the likelihood that any vulnerabilities are discovered and can be resolved before the design process is finalised. Potential vulnerabilities are cheaper to rectify early in the design process than after production, where significant engineering changes may be required. This process mitigates the risk that new cyber-security vulnerabilities are discovered as part of the acceptance test and evaluation, and operational test and evaluation, allowing these activities to focus on the analysis of, and where necessary acceptance of, residual risk.

While the conduct of cyber-security test and evaluation will not prevent poor security by design, real-world experience would be gained by the testers, and this could drive the specification of more relevant and specific cyber-security requirements for future capabilities. The collected lessons learnt from cyber-security test and evaluation would flow into existing capabilities, and into the initial design of future capabilities, ensuring security and resilience is built from the ground up.

This test and evaluation of cyber resilience requires that defence industry is able and appropriate to test that resilience against Defence's cyber threats. If the US Defense acquisition is any guide, such test and evaluation, once it begins in earnest, is likely to be Commonwealth-led with restricted access for many industry system developers, providing mainly recommended changes to software architectures without

necessarily explaining why, at least at a threat-level. Such Commonwealth-led cyber resilience evaluation may need to adjust Defence's preferred contracting models in Australia and some of the cultural preferences in Australian Defence acquisition of who should own what aspects of the designs at various stages of the system life-cycle.

Change management

General change-management policies also need to be reassessed to understand their impact on cyber security. One area where this is particularly important is in the application of security patches and upgrades to software in critical systems. Any change to a system that controls critical systems, such as weaponry or platform functionality, will trigger a recertification and functional regression testing of the system. This is often very costly and can act as a barrier to change within the system, with the resultant effect of leaving these critical systems running on unsupported or unpatched versions of software.

This regression test is required for good reasons; ordnance control and personnel safety rightly outweighs cyber-security concerns, so these tests should not be discarded. However, there needs to be a reasonable compromise between maintaining certification boundaries in critical systems and applying security patches, and any unnecessary process overheads must be streamlined.

Dedicated test environments where these security updates can be quickly tested must be maintained as part of platform sustainment, and it is recommended that the inability of this environment to implement security updates in a timely fashion be treated as a security risk in and of itself (McGinn, 2015). Automation of regression testing is the one feasible way to achieve the level of agility required to implement patches and security updates on mission and safety critical systems, and this must be part of any change-management policy that addresses cyber security.

Organisational challenges

Defence industry

Currently, Australia's defence industry sector is not usually the pioneer of cutting-edge technology (Ercis *et al,* 2015). Innovative industries such as start-up companies and small businesses sometimes cannot afford, nor survive, the

timelines and costs associated with Defence's bureaucracy (Müller and Fischer, 2014).

Agility can be highly beneficial in many aspects of defence acquisition, and small, agile industry participants do have an important role to play in ensuring a cyber resilient defence force. Through defence innovation hubs, they can tackle the incremental risk reduction activities advocated for previously to develop solutions and components which can be incorporated into major system acquisition projects.

However, defence acquisition for major projects is typically risk averse, and defence organisations would often rather pay a premium to engage with an established business within the defence industry. The start-up mantra of 'fail fast, fail early, fail often' does not hold much credence when spending billions of dollars in public money, where politically, defence organisations cannot afford such a hit-and-miss approach. Consequently, for major acquisitions, they usually look toward the recognised businesses which can be held responsible if something goes wrong, and which are established enough that they will absorb the costs to resolve an issue rather than simply declaring bankruptcy. This mitigates the risk to Defence by shifting some of it to industry.

The downside to the current approach to industry engagement is that defence-related acquisition and development projects tend to focus on industry's ability to satisfy the specific functional requirements to which they are to be contracted, with less consideration given to the attributes of the system to which they are not directly measured yet, such as cyber resilience and as argued earlier, system survivability more generally.

Due to the evolving nature of the cyber threat, security issues must often be addressed during the in-service phase of the capability lifecycle, and if contracting models do not adequately account for this eventuality, addressing these threats may be considered out-of-scope for the industry participants. If any additional costs are beyond the project's budget and Defence cannot afford the solutions, it must accept the risk of the vulnerabilities, which can lead to systems with significant residual risks being accepted. Consequently, if sustainment contracts are not cognisant of this need for addressing emerging cyber vulnerabilities, the management of

cyber-security vulnerabilities that are detected during the in-service phase of the capability risks consuming a higher proportion of the system sustainment budget than should be the case.

It is therefore vital that industries that specialise in identifying and quantifying cyber vulnerabilities must be engaged throughout the lifecycle, from requirements through acquisition to disposal, to ensure mission assurance and effectiveness for Defence in cyber-intensive environments. To achieve this, Defence must work collaboratively with prime contractors to ensure this cyber-vulnerability support is part of the engineering design and development processes. Therein, the program protection plan referred to earlier is key to such industry support being appropriately scoped and engaged.

One way to implement this would be as an extension to the Infosec Registered Assessors Program, currently administered by the Australian Signals Directorate. This program brings together cyber-security experts who can be engaged by government agencies and their contractors to audit and assess ICT systems which process Australian government information. A complementary program could be implemented that would provide a group of independent experts who could be engaged by prime defence contractors, or by Defence itself, to assess designs and systems for cyber resilience and cyber worthiness on behalf of Defence.

Defence's cyber systems

The cyber-security landscape in a software intensive mission system or platform is inherently complex and dynamic. Most Defence systems are acquired through a project led by the Capability Acquisition and Sustainment Group, which is then delivered to the responsible capability manager within Defence. The personnel who acquire the system may not be involved during operations and sustainment, and Capability Acquisition and Sustainment Group is often measured against the timeliness and cost of a capability, which risks incentivising short-sighted thinking to get a project to its final operating concept milestone rather than the necessary deeper analysis to address complicated cyber-resiliency challenges. The problems of incentives in US Defense acquisition are covered extensively in a meta-analysis by Smith *et al* (2016).

From a Defence perspective, the cyber-security landscape is further complicated with different organisations responsible for the provision of ICT systems at the strategic, operational and tactical levels. This risks dilution of accountability and control of system cyber security due to the various organisations involved with overlapping roles. It also risks diminished accountability to record, control and monitor cyber-security issues. These risks are concerning for a tightly integrated small military force like that of Australian Defence, as a highly effective network-centric warfare system is paramount to maintain dominance over numerically superior forces, and a lack of organisational coordination can have a negative impact within this paradigm.

A single organisation should be responsible for managing Defence's cyber-security risk, responsible to the Chief of Joint Capabilities as the capability manager for joint C4ISR, space and cyber. As the challenges in cyber security are highly technical, the organisation must contain both technical and operational expertise on Defence's various software-intensive mission systems and platforms. Furthermore, the organisation should contain a mixture of people from the different Services, Reserve forces and external contractors, who are specialists in the cyber domain.

Snyder *et al* (2015) assert that managing cyber-security risk has three components, namely, minimising vulnerabilities to systems; understanding the threat to those systems; and minimising the impact to operational missions. The recommended organisation must cater for these components and implement a comprehensive cyber-risk management system for all Defence mission systems, which would require it to be involved in all lifecycle states of software-intensive mission systems. There are numerous cyber-risk management methodologies that are currently available and could be leveraged (such as Cherdantseva *et al,* 2016). Another source of guidance is the risk-management strategies used by allied forces for their cyber-defence risk quantification.

During the lifecycle of a defence-related mission system, the recommended organisation needs to:

- Influence decisions that shape the software architecture, underpinned by rigorous and timely test and evaluation, so as to ease cyber-security management and

troubleshooting of the system in the later lifecycle stages. Cyber-security issues identified during design may result in significant cost-savings;

- Ensure that cyber security of the system is part of the design across the entire lifecycle of the system by developing and championing specific project protection plans;

- During the procurement, developmental and operational testing phases, ensure that the system complies to a cyber-security risk management framework;

- Ensure consistent and timely change management of the software-intensive systems across platforms including but not limited to upgrades, patches, modifications, technology refreshes etc;

- Continually monitor the cyber-security landscape, the changes in military concepts of operations and its effect on the software systems to continuously ensure that these changes do not introduce new vulnerabilities; and

- Ensure that the disposal of software-intensive military systems is performed without compromising other military systems by revealing vulnerabilities.

The recommended organisation must also have rapid prototyping capabilities and laboratory facilities that can simulate Defence's mission-system environments in a controlled environment (Van Antwerpen, 2015). This would also give Defence the ability to experiment and learn about the current mission systems, including their vulnerabilities, and provide an opportunity to experiment with emerging technologies and understand their limitations in a tactical environment. The knowledge gained from these rapid prototyping facilities would also allow Defence to be a 'smart buyer' as detailed in the recent first principles review of defence acquisition and sustainment.

The involvement of this recommended organisation during the pre-acquisition phases of a project is also likely to have the effect of encouraging defence industry to act on these sorts of concerns by making it clear that this capability is a discriminator in the selection process. An organisation such as the one described could become a strong influence for cyber security across Defence, provided its powers of review

and oversight were enabled within acquisition contracts, much like they currently are for safety regulators. There may be a temptation to merge this organisation with existing security regulators, such as the Australian Signals Directorate or the Chief Information Officers Group. However, this article would argue that the impact of cyber vulnerabilities should be managed by the capability manager for joint C4ISR, space and cyber.

Conclusion

Within Defence, cyber resiliency must be incorporated across the entire capability lifecycle, and the associated policy development needs to be cognisant of this holistic need. The specification of cyber-resiliency requirements needs to be improved, further importance needs to be placed on cyber security in the architecture and design phases, and cyber-security test and evaluation needs to be an integral part of overall test activities. To achieve this, a new Defence organisation has been proposed and its broad responsibilities outlined. The burning question that remains is what sequence of actions do we need to take to organise the Defence enterprise to adapt to the rapidly changing cyber environment?

The first step should be to implement program protection plans across major acquisition projects, move foundational cyber-hygiene processes into the statement of work, rather than the functional performance specification, and reserve those functional cyber security requirements for only those needs specific to the capability being acquired.

The second step would be to build the cyber-security test expertise and infrastructure through targeted trials to create a body of knowledge that can be leveraged by newer systems to enable more resilient design. The third step should be the joint development of a cyber-resiliency toolkit through a series of risk reduction activities, which would provide off-the-shelf modules that can be incorporated into acquisition projects. The final step should be the adoption of a key performance parameter for cyber resilience, and articulated outcomes for cyber-security test and evaluation on future projects.

This sequence would allow for all stakeholders to develop their cyber-resiliency capabilities over time, and the shared responsibility would drive a collegial partnership to ensure the outcome of a more cyber-hardened and cyber-resilient Defence. Industry, academia and the government in Australia would all need to work together to achieve this vision. The free flow of threat information, security solutions and best practice between these participants would also be essential in providing a cyber-secure future for Defence.

Stuart Fowler is a Systems Engineer working in the Australian defence industry. He has worked on major naval acquisition projects, with a primary focus on information assurance and cyber security. He holds a Bachelor degree in Mechanical and Mechatronic Engineering, and a Masters degree in Engineering Management.

Captain Craig Sweetman, Royal Australian Corps of Signals, has served in a variety of regimental and staff appointments. He has a Bachelor degree in Science (Computer Science and Information Systems), and Masters degrees in Science (Information Technology), Project Management, and Cyber Security Operations. He is currently attending the Capability and Technology Management College at the Australian Defence College.

Flight Lieutenant Sibi Ravindran graduated from Monash University with a Bachelor (Honours) of Engineering (Mechatronics). His postings have included 1 Combat Communication Squadron, Project Zodiac (assessing operational and deployed communication systems) and the Land Network Integration Centre. Flight Lieutenant Ravindran has a Masters degree in Cyber Security and is currently working in Electronic Warfare Operations at the Air Operations Centre, Air Command.

Dr Keith Joiner joined the Royal Australian Air Force in 1985 and, over a 30-year career, became an aeronautical engineer, project manager and teacher. From 2010 to 2014, Group Captain Joiner was the Director-General of Test and Evaluation for the ADF. In 2015, he joined the University of NSW as a senior lecturer in test and evaluation. Dr Joiner is a Certified Practising Engineer and a Certified Practising Project Director.

Dr Elena Sitnikova is a researcher and academic within the Australian Centre for Cyber Security at the University of NSW, teaching inter alia cyber governance. Her main research interests are in critical infrastructure protection and cyber security, quality assurance and enterprise process capability improvement. Elena currently leads the critical infrastructure area, carrying out research projects in cyber security and process control systems with industry, and state and Federal government partners in Australia.

References

Australian Government, *2016 Defence White Paper*, Department of Defence: Canberra, 2016.

Australian Signals Directorate, 'Information Security Manual', *Australian Signals Directorate* [website], available at <https://www.asd.gov.au/infosec/ism/> accessed 31 March 2017.

Beraud, P., A. Cruz, S. Hassell and S. Meadows, 'Using cyber maneuver to improve network resiliency', paper presented at Military Communications Conference, Baltimore, 8-10 November 2011, pp. 1121-6, available at <http://ieeexplore.ieee.org/document/6127449/> accessed 23 June 2017.

Bergmann, K., 'Capability development reform: a work in progress', *Asia-Pacific Defence Reporter*, Vol. 39, Issue 10, 2002, p. 34 (subscription only).

Brown, C., P. Christensen, J. McNeil and L. Messerschmidt, 'Using the developmental evaluation framework to right size cyber T&E test data and infrastructure requirements', *ITEA [International Test and Evaluation] Journal,* Vol. 36, Issue 1, 2015, pp. 26-34 (subscription only).

Cherdantseva, Y., P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby and K. Stoddart, 'A review of cyber security risk assessment methods for SCADA systems', *Computers & Security,* Issue 56, 2016, pp.1-27 (subscription only).

Commonwealth of Australia, *Australia's Cyber Security Strategy: enabling innovation, growth & prosperity*, Department of the Prime Minister and Cabinet: Canberra, 2016.

Ercis, A. and M. Unalan, 'Analysis of the world's most innovative companies on the basic of industry: 2005-2014', *Procedia-Social and Behavioral Sciences*, Issue 195, 2015, pp. 1081-6, available at <https://openaccess.firat.edu.tr/xmlui/bitstream/handle/11508/8385/Analysis%20of%20The%20World%27s%20Most%20Innovative%20Companies%20on%20The%20Basic%20Of%20Industry%3A%202005-2014.pdf> accessed 30 May 2017.

Freeman, B., 'A new defence for Navy ships: protection from cyber attacks', *Office of Naval Research* [website], 17 September 2015, available at <https://www.onr.navy.mil/en/Media-Center/Press-Releases/2015/RHIMES-Cyber-Attack-Protection> accessed 20 May 2016.

Hawksworth, J., and D. Chan, 'The world in 2050: will the shift in global economic power continue?', *PricewaterhouseCoopers* [website], February 2015, available at <http://www.pwc.com/gx/en/issues/the-economy/assets/world-in-2050-february-2015.pdf> accessed 15 July 2016.

Joiner, K., 'How Australia can catch up to US cyber resilience by understanding that cyber survivability test and evaluation drives defense investment', *Information Security Journal*, Vol. 26, Issue 2, 2017, abstract available at <http://www.tandfonline.com/doi/abs/10.1080/19393555.2017.1293198> accessed 30 May 2017.

Joiner, K., E. Sitnikova and M. Tutty, 'Structuring defence cyber-survivability T&E to research best practice in cyber-resilient systems', paper presented at Systems Engineering Test and Evaluation Conference, Melbourne, 2016, available at <http://search.informit.org/documentSummary;dn=255735974744392;res=IELENG> accessed 23 June 2017.

McGinn, K., 'A centralized holistic approach to information assurance testing', *ITEA Journal*, Vol. 36, No. 3, September 2015, pp. 208-10 (subscription only).

Müller, J.P., and K. Fischer, 'Application impact of multi-agent systems and technologies: a survey', in Onn Shehory and Arnon Sturm (eds.), *Agent-oriented software engineering: reflections on architectures, methodologies, languages and frameworks*, Springer Berlin Heidelberg: Heidelberg, 2014, pp. 27-53, abstract available at <https://link.springer.com/chapter/10.1007%2F978-3-642-54432-3_3> accessed 30 May 2017.

Office of the Secretary of Defense, 'Procedures for operational test and evaluation of cybersecurity in acquisition programs', memorandum dated 1 August 2014, available at <http://www.dote.osd.mil/pub/policies/2014/8-1-14_Procs_for_OTE_of_Cybersec_in_Acq_Progs(7994).pdf> accessed 30 May 2017.

Paganini, P., 'Hack-proof drones possible with HACMS technology', *InfoSec Institute* [website], 2014, available at <http://resources.infosecinstitute.com/hack-proof-drones-possible-hacms-technology/> accessed 23 May 2016

Ramuhalli, P., M. Halapanavar, J. Coble and M. Dixit, 'Towards a theory of autonomous reconstitution of compromised cyber-systems', paper presented at 2013 IEEE International Conference on Technologies for Homeland Security, 2013, subsequently published in *Homeland Security Affairs,* Supplement 6, April 2014, available at <http://cryptome.org/2014/05/cybersys-reconstitution.pdf> accessed 30 May 2017.

Reed, M., 'System security engineering for program protection and cybersecurity', paper presented at 18th Annual NDIA Systems Engineering Conference, Springfield, Virginia, 29 October 2014, available at <http://www.acq.osd.mil/se/briefs/16994-2014_10_29-NDIA-SEC-Reed-SSE-PP-vF.pdf> accessed 30 May 2017.

Richards, R., 'High assurance cyber military systems', *Defense Advanced Research Project Agency* [website], 2016, available at <http://www.darpa.mil/program/high-assurance-cyber-military-systems> accessed 20 May 2016.

Slezak, M., 'Unhackable kernel could keep all computers safe from cyber attack', *New Scientist*, 16 September 2015, available at <https://www.newscientist.com/article/mg22730392-600-unhackable-kernel-could-keep-all-computers-safe-from-cyberattack-2> accessed 21 May 2016.

Smith, N.C.; E.D. White, J.D. Ritschel and A.E. Thal, 'Counteracting harmful incentives in DoD acquisition through test and evaluation and oversight', *ITEA Journal*, Issue 37, 2016, pp. 218-26 (subscription only).

Snyder, Don, James D. Powers, Elizabeth Bodine-Baron, Bernard Fox, Lauren Kendrick and Michael Powell, 'Improving the cybersecurity of US Air Force military systems throughout their life cycles', *RAND Corporation* [website], 2015, available at <http://www.rand.org/pubs/research_reports/RR1007.html> accessed 30 May 2017.

Van Antwerpen, C., and D.K. Bowley, 'An Australian approach to concept development and experimentation: linking strategy to capability', *Journal of the Operational Research Society*, Vol. 63, Issue 2, pp. 278-92, abstract available at <https://link.springer.com/article/10.1057/jors.2011.28> accessed 30 May 2017.

Indigenous pride, national security and the Regional Force Surveillance Units

Warrant Officer Class 2 Aaron Waddell, Australian Army

Aboriginal and Torres Strait Islanders have been a longstanding part but much under-acknowledged element of the ADF. These first Australians have served with distinction from the Boer War to the modern Afghanistan and Iraq campaigns. Often, they served as single soldiers, and often without official recognition of their indigenous ethnicity. In World War 2, some indigenous units and sub-units were raised for domestic war service but with little real recognition of ethnicity or equality in service recognition. Nevertheless, indigenous men and women who served Australia did so with courage and tenacity, regardless of whether they were officially recognised as Australians.

Since those times, and particularly after then Prime Minister Kevin Rudd apologised to the 'stolen generation' in February 2008, the speed of acceptance and inclusion of our first people and their numerous and distinct cultures into contemporary mainstream society and the Australian military has seen lightning changes. Now, with numerous governmental campaigns underway, it is time to closer link the Regional Force Surveillance Units—the Pilbara Regiment, the North West Mobile Force (NORFORCE) and 51st Battalion Far North Queensland Regiment (51 FNQR)—to the indigenous population of Australia, not only in their operating regions but for all indigenous Australians.

It is also important to link their service in their own units with the national security of Australia. This article argues that these units should become metaphorically owned by all indigenous Australians by displaying their Aboriginal and Torres Strait Islander symbology and with an indigenous unit lineage to carry their own customs and traditions into the future, while making a significant mark on the protection of Australia's national security.

Becoming Australian

Times and attitudes have changed, and reconciliation between the broader Australian society and the first Australians has now gained a level of success and tempo that many in both indigenous and non-indigenous communities never thought possible. For example, despite neither being recognised as Australians, but to differentiate Aboriginal and Torres Strait Islanders for administrative reasons, Queensland's *Torres Strait Islanders Act 1939* legally recognised Torres Strait Islanders as a separate indigenous race in Australia.[1]

Becoming 'Australian' commenced with the *Commonwealth Nationality and Citizen Act* of 1948 that gave citizenship to Australia's indigenous people but no right to vote.[2] The pathway to the right to vote began in 1962 when the *Commonwealth Electoral Act 1918* was amended to allow Aboriginal and Torres Strait Islanders the right to vote in Federal elections.[3] However, it was not until 1967, in amending the Australian Constitution, that our society fully recognised our first Australians as part of the Australian population.[4]

Indigenous war service to Australia

With the outbreak of World War 1, many young Australian men patriotically answered the call to arms, most often with a view for adventure, and enlisted in droves. This fervour and desire for adventure was not limited to the 'white man', as many young indigenous men also answered the call as they too sought the adventure promised by war. They tried to enlist despite the *Commonwealth Defence Act 1903* exempting 'persons who are not substantially of European origin or descent'.[5] The introduction of a universal military training scheme in 1911 also did little to change interpretations of legislation and subsequent military policies. Hence, both policies and attitudes made indigenous enlistment a challenge.

Despite these contemporary attitudes, in a dim light of recognition of the contribution that Australian indigenous people could play in the defence of northern Australia, Major W.O. Mansbridge of the 84th Infantry (Gold-Fields Regiment)

suggested in the *Military Journal* of January 1912 that:

> I beg to submit suggestions whereby his services could be utilized, and I am of the opinion that he would become a very useful ally in case of an invasion in those parts.[6]

Sadly, it appears that Major Manbridge's suggestions fell on deaf ears as there was little Australian appetite for inclusivity, particularly in the military, as the universal military training scheme of 1911 echoed the ethnicity sentiments of the *Commonwealth Defence Act 1903.* Ultimately, while all government military policies were not directly aimed at indigenous Australians, they—as the largest ethnically different group in Australia—suffered the consequences because of the lack of recognition of them as part of the Australian population.

Enlistment struggles aside, as Philippa Scarlett presents in her book *Aboriginal and Torres Strait Islander volunteers for the AIF: the Indigenous response to World War One,* indigenous men had been individual members of all Australian Light Horse Regiments and 60 of the 62 Australian Infantry Battalions of the 1st Australian Imperial Force (AIF).[7] However, these were only the fighting arms of the Australian land element—there is little to no information on indigenous employment in the logistic elements of that force or the Navy.

Despite some indigenous men having the chance to serve Australia, they fought in units that were raised with the customs and traditions of British regiments, and those that had no lineage to Britain reflected the broader 'white' society of Australia. When indigenous soldiers came home, they disappeared back into their communities, the attitudes of 'white' Australia continued, the units disbanded, and ex-service associations took the mantle of returned veterans and unit commemorations.

As a result, many indigenous ex-soldiers were not around to march or commemorate, often finding themselves returned to their remote homelands; those who were living in towns were refused entry and service in bars and clubs, and were refused permission by local authorities to march on ANZAC day.[8] Thus, Aboriginal and Torres Strait Islanders were not truly represented or commemorated as a formed fighting force,

rather only as a gap-fill in units that reflected 'white' Australian society and British Army lineage. They had no ex-service organisation or standing unit to call their own.

In the interim war years, there is very little information on the extent to which indigenous men continued in military service, suggesting there were few if any indigenous men serving in the land force or the newly formed RAAF. There is photographic evidence that the RAN employed some indigenous men in Far North Queensland, albeit in very limited numbers, notably aboard HMAS *Geranium* when it was engaged in hydrographic surveys of the Great Barrier Reef.[9]

As World War 2 loomed, and particularly after it commenced in September 1939, the spirit of adventure again gripped men of all ethnicities. Again, Aboriginal and Torres Strait Islander men could only enlist as individuals in units of the military, all now bearing the lineage and battle honours of the AIF units—one step away from Britain but still not representative of the efforts of indigenous AIF soldiers.

It was not until 1941, when the war for Australia was taking a dark turn as Japanese forces had entered the war and were advancing south with great speed, that fear of invasion gripped

Australia and the government-of-the-day sought to strengthen the northern borders. Against this background, the acting Prime Minister of Australia, Arthur Fadden, announced in May 1941 that 'approval has been given in principle to the raising of one company of Torres Strait Islanders for service on Thursday Island for the duration of the war and twelve months after'.[10]

Thus Australia, for the first time in its military history, raised an indigenous majority-staffed military unit, the Torres Strait Independent Infantry Company. While largely manned by Torres Strait Islanders, although commanded by non-indigenous officers and sergeants, there were also some Aboriginal men on the unit establishment. On 1 March 1943, the unit was officially formed into an infantry battalion, titled the 'Torres Strait Light Infantry Battalion'. Interestingly, a 1945 order, outlining the unit's war establishment, continued to reflect the 'non-Australian' status of indigenous personnel by differentiating between (white) 'Australian personnel' and 'Torres Strait personnel'.[11] The unit was disbanded with no fanfare in 1946.

After the establishment of the Torres Strait Independent Infantry Company, the Northern Territory Special Reconnaissance Unit was raised in Arnhem Land in February 1942 as a wholly

Aboriginal auxiliary unit. It was commanded by a RAAF Officer, Flight Lieutenant Donald Thomson, a pre-war anthropologist who had studied and lived with Aboriginal people in northern Australia. However, the unit was short-lived, being disbanded in April 1943.

It is important to note that none of the indigenous men of the unit were formally enlisted into the military or paid, receiving only three sticks of tobacco a week in remuneration. On being disbanded, its remaining members were transferred to the 2/1st North Australian Observer Unit, which had been raised in May 1942. Available information suggests that the unit was largely manned by white 'light horse' soldiers, with its indigenous members valued for acting in auxiliary roles and as guides.[12] The unit, which had a notable number of indigenous personnel but was not an indigenous-majority unit, was disbanded in March 1945.

By the close of World War 2, many of the indigenous ex-soldiers were to suffer the same fate of those who had served with honour in World War 1—lost in time by the war's end and often fading back into obscurity. The Australian Army's only-ever solely indigenous unit, the Torres Strait Light Infantry Battalion, despite active service in the coastal regions of Dutch New Guinea, had been written off the Australian Army's order of battle to become nothing more than a memory.

The major conflicts following World War 2, namely the Korean war and the Vietnam war, again saw indigenous soldiers serving as 'non-citizens' in individual units. These units all had links back to World War 1 and World War 2, carrying on the battle honours of white units and white history, but with no links to the Torres Strait Light Infantry Battalion, the Northern Territory Special Reconnaissance Unit or the Northern Australian Observer Unit.

Regional Force Surveillance Units

It was not until the 1970s that, once again, out of national security fears of Indonesian military activity in northern Australia, the Australian Government sought to use Aboriginal and Torres Strait Islanders in the defence of Australia, particularly as the Special Air Service Regiment (SASR)—once charged with the responsibility of northern surveillance—was unable to fulfil that duty.[13] Thus, the Australian Army decided to form three regional force surveillance units, charged with conducting unconventional operations in northern Australia to ensure adequate surveillance and better national security.

The Pilbara Regiment

Planned in the late 1970s to conduct unconventional military operations in north-west Australia, the Pilbara Regiment started as the 5th Independent Rifle Company, before being upgraded to the Pilbara Regiment in December 1981.[14] Initially operating from Headquarters 5th Military District, it later moved to Campbell Barracks in Perth, with one platoon at Tom Price and one at Newman.

The establishing cadre was drawn from the 'special conditions' element of 28th Independent Rifle Company, Royal West Australian Regiment (RWAR), which was the indigenous element, recruited under specific conditions that reflected the special conditions of service of indigenous regional recruits. This avenue of enlistment still exists, now named the Regional Force Surveillance List, which gives commanding officers the ability to waive a particular enlistment criterion.[15]

Notably, though, the history of the army units that grew the Pilbara Regiment did not reflect any indigenous nature; rather, they continued the battle honours of World War 1 and World War 2-related 'white' Australian Army units. Its antecedents were (arguably) the 2/5th Commando Squadron, a Victorian-raised World War 2 special operations unit, established in 1942 and disbanded in 1946, and the West Australian 28th Battalion AIF, which was raised in 1915 and disbanded in 1919 before being re-raised and disbanded numerous times until settling as the 11/28th Battalion RWAR in 1987.

The 5th Independent Rifle Company title ultimately kept the unit organically West Australian by using the Military District numbering of 'five' but also largely kept the battle honours of the New Guinea and Borneo operations of the 2/5th Commando Squadron in living memory.[16] Furthermore, staffing the unit with a cadre from the 28th Independent Rifle Company RWAR fed

the history of that unit into the fabric of the new regional force surveillance unit although, again, it was the honours of Gallipoli and the Western Front, and World War 2 operations in New Britain that were not forgotten and extended beyond that of the 11/28th Battalion RWAR.

The transformation of the unit from the 5th Independent Rifle Company into the Pilbara Regiment occurred after a series of sporadic unit growth and training activities. The move of the headquarters element to Port Hedland and the formation there of a Support Platoon, along with participation in Exercise KANGAROO 1983, proved the unit as a regional surveillance force. Thus, on 26 January 1985, the unit officially became the Pilbara Regiment, with 'Australia day' being used to re-establish the unit, yet with no consideration of dates relevant to its indigenous personnel or the special considerations and nature of the unit. Further changes since 1985 have met Army needs rather than endeavouring to strengthen national security by tying the community closer to the Army by better utilising the unit's special enlistment criteria.

While many general observers would likely see the Pilbara Regiment as representative of and staffed by the indigenous peoples of the region, this is only partially correct. The Regiment is predominantly staffed by a Regular Army cadre of non-indigenous personnel, who hold all command and key positions. The unit has never had an indigenous commanding officer nor an officer commanding or company sergeant major of any of its squadrons. The unit's indigenous personnel rarely go beyond the rank of sergeant and usually hold little more than a patrol commander's position. While it is not being suggested that there is any deliberate limiting of advancement for indigenous personnel, the unit still operates much like the pre-1973 Papua New Guinea Defence Force (PNGDF), in which senior command and key positions were held by Australian-provided personnel.

The North West Mobile Force

In line with the need to ensure a persistent northern military presence, the central unit in the network of surveillance units was named the North West Mobile Force (NORFORCE) on 1 July 1981. The unit derived from several World War

2 forebears, including the Darwin Mobile Force and the Northern Territory Special Reconnaissance Unit, although it most closely resembled and was given the history and insignia of the 2/1st Northern Australia Observer Unit. Again, however, despite the popular image that the 2/1st Northern Australia Observer Unit was an indigenous unit, NORFORCE was far from that stock.

Initially, NORFORCE was staffed with men from the disbanded 7th Independent Rifle Company, an independent infantry company under command of Headquarters 7th Military District. The history of the 7th Independent Rifle Company can arguably be traced to the Darwin Infantry Battalion, which in late 1941 was designated the 19th Battalion Australian Military Forces, a militia battalion that took the customs and traditions of the World War 1-origin 19th Battalion AIF.

Later, the 19th Battalion, which was raised and located in Sydney, became completely divorced of its Darwin history, being re-raised in 1966 as the 19th Battalion, Royal New South Wales Regiment (RNSWR). In 1971, it was amalgamated with another Sydney-based battalion, the 1st Australian Infantry Battalion, to become the 1/19th Battalion RNSWR, carrying the battle honours of both World War 1 and World War 2 service, including Darwin. Thus, one of the forebears of NORFORCE carried no link to indigenous servicemen nor incorporated any customs or traditions of the Aboriginal people in the Northern Territory.

The Northern Territory Special Reconnaissance Unit, a majority manned Aboriginal auxiliary unit tasked with an early warning mission, was disbanded in April 1943, with some of its indigenous personnel absorbed into the 2/1st Northern Australia Observer Unit. Regardless of the unique nature of the Northern Territory Special Reconnaissance Unit—and its majority manning of indigenous personnel—the short-lived unit created no customs or traditions or even insignia. On being taken onto the auxiliary strength of the 2/1st Northern Australia Observer Unit, the history and operations of the Northern Territory Special Reconnaissance Unit seemingly vanished. It was not until 1992 that those who had served in the unit were recognised by the Australian Government with World War 2 service medals and pay.

The establishment of the 2/1st Northern Australia Observer Unit came about at the suggestion of W.E.H. Stanner (later Major), an anthropologist with a significant knowledge of northern Australia and a staff member in the office of the Minister for the Army. He was interviewed by Major General Herring, General Officer Commanding Northern Territory Force on the feasibility of a surveillance, reconnaissance and scouting force within the region, which resulted in the decision in May 1942 to establish the 2/1st Northern Territory Observer Unit as part of the 2nd AIF.[17]

Once formed, the unit was established along the lines of a traditional Australian Light Horse unit, preferring horses over vehicles and seeking volunteers with horsemanship skills, previous 'bush' experience and a willingness to undertake arduous duties in the north of Australia. Accordingly, many of the volunteers came from pre-war Light Horse Regiments and those who had lived in the Northern Territory for many years. Many of these men were not indigenous, and the majority of roles for indigenous men and women were supporting tasks, such as horse-breaking, cooking and tracking on long-range patrols.

Later, towards the end of 1943, the unit became dismounted, and most of its personnel were reposted and its field companies disbanded. The much leaner unit continued more limited operations until March 1945, when it was disbanded. In the years between 1945 and 1981, therefore, there was no on-ground military surveillance in the region, other than periodic surveillance patrols and exercises by the SASR.

Accordingly, it can be said that the building blocks of NORFORCE were not based on significant or historical indigenous traditions or legacy. Once raised, the modern NORFORCE has been closely linked with local indigenous communities. However, like the Pilbara Regiment, NORFORCE has never had an indigenous commanding officer, officer commanding or company sergeant major, although the Australian Army's website notes that 'Australian Aboriginal soldiers form 60 per cent of NORFORCE personnel'.[18]

51st Battalion, Far North Queensland Regiment

Much like its two sister battalions in the north of Australia, the 51st Battalion, Far North Queensland Regiment (51 FNQR) was envisaged to fill the need for both a persistent military presence in the Torres Strait and to fill the void of regional surveillance following the cessation of that role by the SASR.

Raised as the last of the three RFSUs, 51 FNQR has no indigenous history. The 51st Battalion AIF was raised in Egypt in early 1916 for service on the Western Front. Staffed from men of the West Australian 11th Battalion, the new unit carried the battle honours of the 11th Battalion's Boer war service and from World War 1, where the unit fought in the well-known battles at Mouquet Farm, Messines, Polygon Wood and Villers-Bretonneux.[19]

Following the cessation of hostilities, the 51st Battalion AIF was disbanded in May 1919. It was reinstated on the Army's order of battle in 1921, when it was moved briefly to West Australia, then NSW, before finally being established on 1 October 1936 as the 51st Battalion FNQR, located in Cairns and with the lineage of the 51st Battalion AIF. During World War 2, the unit served as a militia unit, later seeing active service in New Guinea as the 31st/51st Battalion. It also saw action in the Solomon Islands as an AIF battalion, experiencing particularly heavy fighting at Tsimba Ridge and Porton Plantation on Bougainville Island. The unit was disbanded on 4 July 1946.

The unit was again raised in Cairns in 1950, amalgamating in later years with 31st and 42nd Battalions to become the 2nd Battalion, Royal Queensland Regiment (RQR), before again becoming 51 FNQR, before settling in 1976 as the 51st Independent Rifle Company RQR. All through the turbulent life of the post-war reorganisations, the unit carried the colours and traditions of the 51st Battalion AIF.

In 1985, in line with the desire to form the RFSUs, the 51st Independent Rifle Company RQR once again became 51st Battalion FNQR, with a new unconventional surveillance task as the third of the three RFSUs. However, the unit has no indigenous wartime history and its link

with the Cairns region was as a World War 2 militia battalion. It is also fair to contend that the unit very likely had no interaction with the indigenous population of Far North Queensland as that mantle had been taken by the Torres Strait Light Infantry Battalion.

Following the battalion's reformation as a RFSU, it used local recruitment to capitalise on the knowledge of both the Aboriginal and Torres Strait Islander populations in the region to enhance its ability to conduct its mission. However, the unit's headquarters, located in Cairns, is housed in Porton Barracks, named after the significant battle involving the 31st/51st Battalion AIF on Bougainville in 1944. In 2016, 51 FNQR celebrated its World War 1 history at Villers-Bretonneux and paraded its colours on the Champs-Élysées in Paris. There was no representation of the unit's indigenous contribution in World War 2 or during the modern period.

It can reasonably be argued, therefore, that the unit does not adequately represent the indigenous population of the region and commemorates only its non-indigenous wartime history. 51 FNQR, like its sister battalions, has never had an indigenous commanding officer, officer commanding or company sergeant major. The Aboriginal and Torres Strait Islander personnel form approximately 30 per cent of the rank and file, which is certainly not representative of the indigenous population of Far North Queensland.[20]

Aboriginal and Torres Strait Islander symbology

A symbol is generally defined as a thing or representation that bears significant meaning to a group. Historically, each nation, person and race holds a symbol near and dear to their identity; in this circumstance, Aboriginal and Torres Strait Islanders hold the flag of each race as important to their culture.

The Aboriginal flag, designed in 1971 and granted the status of a flag of Australia under the *Flags Act 1953* on 14 July 1995, has become a nationally recognisable symbol for the Aboriginal people of Australia.[21] The symbol, which can variously be seen as a flag on Australian Government flagpoles, graffiti on a wall, or as a tattoo on the arm of both indigenous and non-indigenous Australians, has gained a significant position in both the Australian Government's policy decisions on Australian symbology and for the Aboriginal people of Australia.

The Torres Strait Islander flag, designed and recognised by the Aboriginal and Torres Strait Islander Commission in 1992, was also granted the status of a flag of Australia under the *Flags Act 1953* on 14 July 1995.[22] While not as universally recognised as the Aboriginal flag, it nevertheless holds significant importance to the people of the Torres Strait and is a permanent feature in all Australian state and federal institutions.

Ultimately, both these flags are part of a series of symbols, language, culture and dance of Australia's indigenous peoples. Hence, it is important that they are used in a manner that connects institutions to their respective race.

Indigenous community ownership of the RFSUs

Despite the demonstrated non-indigenous histories of the three RFSUs, there is certainly an element of indigenous community 'buy in' to them notwithstanding that, since their formation in the 1980s, the units have quintessentially been 'colonial' in their unit composition. For its part, the ADF does not discriminate by race and many an Aboriginal and Torres Strait Islander has held a majority of ranks within the ADF, albeit none has ever been promoted beyond the rank of Lieutenant Colonel.

In an effort to change the status quo and the future of indigenous service, the Chief of Army issued a directive in November 2008 titled 'Army Indigenous Strategy', addressing the recruitment and retention of indigenous personnel.[23] However, although this document has been revised biennially, with the latest revision dated June 2014, it has not captured the need to reflect indigenous command and control of the RFSUs.

Also, given the geographic locations of the three RFSUs and the available recruiting pool (in addition to the ability to waive certain enlistment requirements), it would certainly be wise to take

every step to bring each unit closer to the community. This could be achieved by the specific targeting of prospective leaders for key positions within the RFSUs. For example, recruiting prominent indigenous individuals, such as Johnathan Thurston, captain of the North Queensland Cowboys, or Adam Giles, former Chief Minister of the Northern Territory, to senior leadership positions within the RFSUs, would have significant cultural dividends.

Another suggestion would be to employ the RFSUs within the Australian Special Operations Command, which is beyond the scope of this article but perhaps worthy of consideration, especially given the history of the SASR in regional surveillance. These and other options—such as making greater strategic use of the Army Aboriginal Community Assistance Program to link indigenous communities to the RFSUs—would certainly strengthen community pride and interconnectivity with the Army and the Australian Government more broadly.

Aboriginal ownership

Given the locations of the Pilbara Regiment and NORFORCE, one such symbolic method of Aboriginal community ownership would be to allow these two units to wear the Aboriginal flag as a feature of identity on their Army uniform. Much like soldiers in the modern-day PNGDF wear the PNG flag on the left arm of their uniform and the national symbol, the Kumul, as a patch on their left breast, these units could wear the Australian flag on their left arm and the Aboriginal flag as a patch on their left breast (symbolically close to the heart and thus a person's individual worth and reason for being). Such symbology, together perhaps with a newly designed hat badge, would create an instant rapport with the entire Aboriginal races of Australia, and symbolically give an 'air' of Aboriginal ownership.

Torres Strait Islander ownership

Reorganising 51 FNQR to better reflect the region's indigenous wartime history is as simple as it is complicated. The easy part is that the Chief of Army presumably could recommend to the Minister for Defence his approval of an instrument to disband 51 FNQR and replace it with a re-raised Torres Strait Light Infantry Battalion.

The major complication is that any proposal to disband 51 FNQR would likely attract considerable opposition from veteran groups associated with its 2nd Division history.

However, disbanding 51 FNQR is not a new proposition. Its antecedents have been disbanded and re-raised several times over the past 100 years. Moreover, using a special date, such as the centenary of the end of World War 1, could provide a timely opportunity to disband the unit and lay up its colours with dignity. Subsequently reforming the unit on a day of significant cultural importance and linking it with the history of Australia's only majority indigenously staffed unit would undoubtedly be invaluable in forging much closer ties and bonds between the unit and the local community.

As suggested in the previous section, the targeted recruitment of high-profile indigenous Torres Strait Islanders for leadership positions, in addition to the wearing of Torres Strait Islander symbology, all wrapped in the envelope of a link to the World War 2 history of the Torres Strait Light Infantry Battalion, would substantially enhance unit morale and effectiveness.

Conclusion

In closing, this article is not about significantly changing the status quo or excluding non-indigenous soldiers from serving in an RFSU. It is about highlighting the histories of the RFSUs that were largely born of policies from a period when indigenous concerns did not sit highly in the considerations of government and Army's policy-makers.

The article has also sought to present a number of alternatives and suggestions, some of which are contentious and impact on long-established customs and traditions of the Army. However, the status quo, while often comfortable, is not necessarily right. The Chief of Army's indigenous strategy directive is very welcome but only goes part of the way. The next step would be to reform the RFSUs to become a source of indigenous community pride and ownership. Providing a more inclusive connection between Australia's indigenous population and the Army as a national institution should also improve the operational effectiveness of these units.

Warrant Officer Class Two Aaron Waddell enlisted in the Australian Army Reserve in 1987, serving in the Townsville-based 31st Battalion Royal Queensland Regiment. He later joined the Australian Regular Army in 1989, serving in the 1st Aviation Regiment until transferring to the Army Intelligence Corps in 1991. He has since served in various Intelligence Corps postings, and as an instructor at the 1st Recruit Training Battalion and later the Royal Military College, Duntroon. Warrant Officer Waddell has a Master of National Security Policy (with merit) from the Australian National University.

References

1 Queensland *Torres Strait Islanders Act*, assented to 12 October 1939, available at <http://www.austlii.edu.au/au/legis/qld/hist_act/tsiao19393gvn7382/> accessed 12 April 2017.

2 Australian Electoral Commission, 'Events in Australian electoral history', *Australian Electoral Commission* [website], available at <http://www.aec.gov.au/Elections/Australian_Electoral_History/reform.htm> accessed 23 March 2016

3 Australian Electoral Commission, 'Events in Australian electoral history'.

4 *Constitution Alteration (Aboriginals) 1967*, No. 55 of 1967, assented to 10 August 1967, sections 51(xxxvi) and 127, available at <http://www.austlii.edu.au/au/legis/cth/num_act/ca1967551967395/> accessed 12 April 2017.

5 *Defence Act 1903*, paragraph 61(h), available at <http://www.austlii.edu.au/au/legis/cth/consol_act/da190356/> accessed 12 April 2017.

6 W.O. Mansbridge, 'A scheme for training the Aboriginal native in the northern portions of the Commonwealth', *Military Journal*, January 1912 pp. 99-100, cited in *Australian Light Horse* [website], available at <http://alh-research.tripod.com/Light_Horse/index.blog/1972061/aboriginals-in-the-aif-a-scheme-for-training-the-aboriginal-natives-in-the-northern-portions-of-the-commonwealth-by-major-wo-mansbridge/> accessed 12 April 2017.

7 Philippa Scarlett, *Aboriginal and Torres Strait Islander volunteers for the AIF: the indigenous response to World War One*, 1st edition, Macquarie: Canberra, 2011.

8 Rebecca Franks, 'Aboriginal and Torres Strait Island war heroes "vanished" from the ANZAC legend', *The Daily Telegraph*, 21 April 2014

9 Australian War Memorial, 'A question of numbers – between the world wars', *Australian War Memorial* [website], available at <https://www.awm.gov.au/indigenous-service/indigenous-service-in-Australias-armed-forces-in-peace-and-war/question-of-numbers-pt3/> accessed 12 April 2017.

10 Robert Hall, *The black Diggers: Aborigines and Torres Strait Islanders in the Second World War*, Aboriginal Studies Press: Canberra, 1997, p. 37.

11 Australian Army, 'Torres Strait Light Infantry Battalion – war establishment', Order III/64/3, issued 17 May 1945, available at <http://www.warestablishments.net/Australia/Infantry/Torres%20Strait%20Light%20Infantry%20Battalion%20May%201945.pdf> accessed 12 April 2017.

12 Helen Walker and Richard Walker, *Curtin's cowboys: Australia's secret bush commandos*, Allen & Unwin: Sydney, 1986, pp. 138-9

13 Hugh White, 'What Indonesia's rise means for Australia', *The Monthly* [blog], June 2013, available at <https://www.themonthly.com.au/issue/2013/june/1370181600/hugh-white/what-indonesia-s-rise-means-australia> accessed 12 April 2017.

14 Australian Army, 'Organisational Instruction 592/81, the raising of the 5th Independent Rifle Company, the Pilbara Regiment', cited in *Digger History* [website], available at <http://www.diggerhistory.info/pages-army-today/state-regts/pilbara.htm> accessed 12 April 2017.

15 Department of Defence, 'ADF enlistment requirements - Patrolman', *Department of Defence* [website], available at <http://www.defencejobs.gov.au/army/jobs/Patrolman/?entryTypeId=17> accessed 12 April 2017.

16 Editorial, 'Army reorganization', *Army Journal*, No. 274, March 1972, pp. 3-33, available at <http://www.army.gov.au/~/media/Army/Our%20future/Publications/AAJ/1970s/1972/AAJ_274_Mar_1972.pdf> accessed 12 April 2017.

17 Armoury Vane, 'The surveillance of Northern Australia – its history: the story of Stanner's Bush Commando 1942', *Defence Force Journal*, No. 14, January/February 1979, pp. 15-30, available at <http://www.adfjournal.adc.edu.au/UserFiles/issues/14%201979%20Jan_Feb.pdf> accessed 12 April 2017.

18 Australian Army, 'North West Mobile Force', *Australian Army* [website], available at <http://www.army.gov.au/Our-people/Units/Forces-Command/2nd-Division/North-West-Mobile-Force> accessed 18 November 2015.

19 Neville Browning, *Fix bayonets: the unit history of the 51st Battalion*, AIF, Neville Browning: Bayswater, 2000.

20 Australian Army, '51st Battalion, Far North Queensland Regiment', *Australian Army* [website], available at <http://www.army.gov.au/Our-people/Units/Forces-Command/2nd-Division/51st-Battalion-Far-North-Queensland-Regiment> accessed 15 May 2015.

21 Commonwealth of Australia, *Commonwealth of Australia Gazette*, Special Number S259 dated 14 July 1995.

22 Commonwealth of Australia, *Commonwealth of Australia Gazette*, Special Number S258 dated 14 July 1995.

23 Australian Army, 'Army Indigenous Strategy', *Australian Army* [website], available at <https://www.army.gov.au/our-people/army-indigenous-community/army-indigenous-strategy> accessed 12 April 2017.

The increasing convergence of the role and function of the ADF and civil police

Captain John Sutton, Australian Army

One of the characterising features of the early 21st century, both in Australia and among English-speaking democracies, is the phenomenon of the military becoming increasingly involved in areas traditionally considered the responsibility of police, while elements of the police are simultaneously becoming more militaristic.[1] Historically, a close ideological and operational alliance between the police and military has been associated with repressive regimes.[2]

There are also residual concerns about the use of the ADF for domestic security purposes. At its core is the question of whether the government can be trusted to use the ADF legally and wisely and, indeed, whether the ADF can be trusted to respect civil liberties.[3] These concerns find their foundation in the well-established but often ill-defined tradition in Western democracies that governments must be constrained in their use of the armed forces by constitutions, laws, conventions, the judiciary and parliament.[4]

Conversely, we expect the police to protect us from crime, arrest drug dealers, investigate serious crime, stop armed robbers, and keep the peace at demonstrations. Frequently, there are public outcries when a suspect is shot dead by police before he or she can be tried. The public is disturbed at seeing police wearing riot gear at demonstrations. When police begin using paramilitary tactics and techniques, the essential nature of their role is redefined, switching from protection and peacekeeping to active aggression.

This convergence in roles has coincided with the erosion of a number of geopolitical, economic and social-order assumptions. Principal among these shifts has been the rise of global terrorism and the ushering in of the so-called fourth-generation warfare paradigm.[5] Arguably, counter-terrorism has provided a vehicle for the militarisation of the police and the integration of the military into 'internal security'.

This article will contend that this convergence is socially and politically undesirable, as well as legally questionable as it undermines the legitimate mandate of the ADF and the division of powers under the Australian Constitution.[6] To support this argument, it will demonstrate that the *Defence Act 1903*, together with its subsequent amendments, is an appropriate and proportionate power conferred to the ADF when responding to a domestic security incident, and that it is the ADF—not the police—which possesses a stronger legal, political and social mandate to respond to this type of incident.[7]

Modern warfare: business as usual?

The ending of the Thirty Years' War in Europe in 1648, also known as the 'Peace of Westphalia', arguably constituted a paradigm shift in the development of the present state system.[8] The key notion is said to be the principle of the sovereign equality of states, which has been at the core of international law ever since. From this concept ultimately flowed the law of armed conflict, which codified the footing on which armed forces ought to prosecute warfare.

Since that time, warfare has obviously undergone a number of generational transformations. These have not been discrete events but rather a continuum, with ideas and technology driving the change, although the central feature has been the premise that states fight states.[9] The most notable features of the latest and so-called 'fourth generation' of warfare are that the state is losing its monopoly on war and that state militaries are increasingly fighting non-state opponents, colloquially known in Western democracies as terrorists.

The development of the law of armed conflict

The modern footing for the law of armed conflict flows from two distinct but intertwined historic streams: the Geneva Conventions and The Hague Conventions. Both outline acceptable practices while engaged in war and armed conflict. The Geneva Conventions are a series of international treaties concluded in Geneva between 1864 and 1949, aimed at limiting the prosecution of warfare and, specifically, the amelioration of the effects of war on soldiers, civilians and their property. The Hague Conventions are concerned with the rights and duties of belligerents, and the means that parties may rely on to employ violence.

Relevantly, The Hague Conventions define the distinction between civilians and combatants.[10] Rule 1 stipulates that 'attacks may only be directed against combatants…. [and] must not be directed against civilians'. Rule 3 defines a 'combatant' as 'all members of the armed forces of a party to the conflict … except medical and religious personnel'. These definitions, and indeed both conventions, are arguably premised on the assumption that the purpose of warfare is to overcome an enemy state, which includes the defeat or nullification of its combatants.[11]

However, the principle of distinction and the definition of a combatant have less utility in a modern context, where the idea of symmetrical conflicts fought between near peers is not the normal practice. More commonly, armed conflicts take place within a sovereign territory between governmental forces and non-state actors whose aim is to advance a political, religious or ideological cause.[12] This represents a significant departure from the traditional footing of the prosecution of warfare, which typically has related to the defence or redefining of territorial boundaries between two or more states.

If these definitions and assumptions are outdated, is it not time they were reviewed? As Françoise Bouchet Saulnier has said, 'law is always late for war'.[13] Proactively considering the assumptions that underlie and inform the legitimate use of the ADF in combating non-state actors, including on Australian territory, is a critical legal, political and social discussion. The associated question is whether state-level police forces are best suited, equipped and trained to fight non-state actors.

Domestic social and political framework

The role of the ADF

The ADF's traditional role has been the conduct of conventional military operations, together with peace-keeping and disaster-relief type

operations within the region, with domestic security the responsibility of the relevant federal, state and territory police and intelligence agencies. However, the Hilton bombing in Sydney in 1978 ushered a paradigm shift in political and social thinking towards domestic security and the role the police and military play in maintaining peace and security within Australia.[14] From this vantage point, one can look back and view the academic, political and social discussion and legal reforms that flowed from this pivotal event.

The vast majority of commentary relates to mooted changes to the *Defence Act 1903* in order to clarify or broaden when and how the military might be used internally.[15] Other areas of significant commentary relate to concerns over the steady militarisation of the police.[16] A common theme has been that if the ADF were to be given wider powers to respond to a domestic security incident, those powers may be abused.[17] Often cited has been a concern that the ADF may be used to counter the threat posed by the activities of dissidents, which would repudiate the basic democratic right to freedom of political expression.[18]

Many of these concerns flow from the publication in the early 1980s of the Australian Army's Manual of Land Warfare relating to 'Aid to the civil power'.[19] It outlined a very broad role for the military in areas normally considered covered by police law enforcement. The 'threats' identified in the pamphlet also encompassed many forms of legitimate political dissent. What tends to be overlooked, however, is that the provisions of Part IIIAAA of the *Defence Act 1903* expressly prohibit the employment of the ADF to stop or restrict any protest, dissent, assembly or industrial action, except where there is a reasonable likelihood of the death of, or serious injury to, persons or serious damage to property.

Nevertheless, the reality is that the ADF has a wide range of capabilities that could be deployed rapidly and efficiently to respond to virtually any internal incident. The ADF also has a strong culture of obedience to political direction and discipline in command.[20] Furthermore, over the past three decades of high operational tempo, the ADF has gained a wealth of experience in security operations in a number countries, which has well equipped the ADF and

its personnel with the tactics, techniques and procedures to respond to a range of domestic security incidents.

Regardless, there are deeply held, imperfectly understood reservations within Australian society about the employment of the ADF in response to a domestic security incident.[21] In Justice Robert Hope's report (the *Protective Security Review*, 1979) written in response to the Hilton bombing, he observed:

> Use of the military other than for external defence, is a critical and controversial issue in the political life of a country and the civil liberties of its citizens. [Quoting the 19th century Irish statesman Edmund Burke, he contended that] 'An armed disciplined body is in its essence dangerous to Liberty: undisciplined, it is ruinous to Society'. Given that there must be a permanent Defence Force, it is critical that it be employed only for proper purposes and that it be subject to proper control.[22]

These reservations seem to be rooted in the concern that left unchecked, the executive might use control over the ADF to reinforce its political will, and take actions that are difficult to call to account in a court of law. There has also been significant judicial consideration of the potential danger to a constitutional democracy of unchecked executive power, with High Court Justice Sir Owen Dixon asserting in the *Communist Party Case* in 1951 that:

> History and not only ancient history, shows that in countries where democratic institutions have been unconstitutionally superseded, it has been done not seldom by those holding the executive power. Forms of government may need protection from dangers likely to arise from within the institutions to be protected.[23]

The role of the police

While reservations within Australian society about the employment of the ADF in response to a domestic security incident have stimulated considerable commentary and legal opinion, there has been far less discussion or criticism regarding the increasing militarisation of the police in Australia. Indeed, following the Bali bombing in 2002, Aldo Borgu, for example, writing for the Australian Strategic Policy Institute, advocated that the entire counter-terrorism

capability within the ADF should be moved to federal and state police forces, arguing that:

> Federal and State police forces … will almost always be able to get to a terrorist scene more quickly than the ADF, and are on a surer legal footing to undertake such operations. NSW and Victoria have made important steps to further develop their own counter-terrorist and response capabilities. But this approach needs to be mirrored across all States and Territories. This would free up the ADF Special Forces to focus on their overseas missions.[24]

Yet the development of these paramilitary units raises a number of questions that do not seem to enter political debate, let alone public consciousness. For example, why have these units been established; what are the implications to the civilian police force of military-style training and collaboration with the ADF when it filters down to general duties police officers; how does this blurring of the distinction between civil and military forces influence police culture, and why are both forms of militarisation needed?

Originally established to combat terrorism, paramilitary police units have been used in a wide variety of policing operations, including dealing with dissent and social and industrial protest.[25] Often not mentioned is that paramilitary police units have been used in some highly controversial political circumstances against trade unions and their members. As such, some might argue that it is the paramilitary police units, rather than the ADF, that the public ought to fear, not least because their existence may herald an increasingly militarised approach to everyday policing.

Perhaps the most alarming aspect regarding the development of paramilitary police forces is that they train with and adopt many of the practices of ADF Special Forces. This style of training provides paramilitary police units with the ability to survive armed confrontations by taking aggressive counter-action, unlike their general duties counterparts who are trained to avoid such confrontations where possible. In a Victoria Police Force review conducted in the late 1990s, its Special Operations Group was found to be responsible for 30 per cent of the deaths by shooting during the review period.[26] At a coronial inquest into one such death, it was contended that:

> The policy of the Victoria Police Force and its SOG [Special Operations Group] accepts … the use of force, forced entry, consequential firearms confrontation, consequential instinctive use of police firearms with legal justification, consequential personal risk to police members being exposed to a person with a gun, and consequently and ultimately condones shooting by police members with legal justification.[27]

This and similar policy in other states has resulted in the deaths of several innocent victims. In one incident in NSW in 1989, a man was shot dead in his bed by paramilitary police during an early morning raid on his home. In a subsequent Royal Commission, it was found that the death occurred because the police officer in question 'had not been trained to cope with an unarmed, near-naked man who reacted angrily when woken from his sleep by armed men bursting into his house'.[28] No charges were laid. There has also been criticism levelled at the NSW Police's handling of the Lindt café siege that resulted in the death of three civilians.

In addition, there are concerning second- and third-order effects that increased militarisation may have on civilian police culture. These include the potential impact and pervading influence of military-style practices on everyday policing practices, including the suggestion of increased police aggression in handling non-life-threatening confrontations. Aside from the serious social and cultural questions around the desirability of the normalisation of paramilitary tactics and attitudes in everyday policing, there may also be an argument as to the constitutional legitimacy of these policing units within Australian states and territories.[29]

Legal framework

The civil police/military divide

In Australia's federal system, the primary responsibility for maintaining internal law-and-order lies with the states; no express legislative head of power confers any such general power on the Commonwealth.[30] Importantly, upon federation, constitutional arrangements required the states not to raise or maintain any navel or military force without the consent of the Commonwealth Parliament. Conversely, the Commonwealth

took over responsibility of protecting 'every state against invasion' and, at the request of the executive government of the state, 'against domestic violence'.

Relevantly, neither 'military force' nor 'domestic violence' are defined in the Constitution, nor are they defined in the *Defence Act 1903* or its regulations. No judicial definition exists either. The expression 'domestic violence' seems to have been borrowed from article IV of the US Constitution, which specifies that the US shall protect each state, on the application of its legislature, against 'domestic violence'. The statutory embodiment of this provision in US legislation uses the more specific term 'insurrection', suggesting that a serious level of rebellion must be involved.[31] However, it seems unlikely that the framers of Australia's Constitution would have been contemplating the need for the states to train and arm their police forces to quell a serious level of rebellion.

Consideration must also be given to the legitimacy of the states militarising elements of their police forces. While the Constitution prohibits the states from raising and maintaining a military force, there is no case law on whether the militarisation of state and territory police forces is prohibited and accordingly unlawful. Yet all states and territories in Australia now have their own 'paramilitary' policing units which share startling similarities with elements of the ADF.[32] Most also have close training and liaison arrangements with the ADF. Indeed, the selection processes, culture, organisational hierarchy, weapons, vehicles, tactics, techniques and procedures relied on by paramilitary policing units typically render them all but indistinguishable from their ADF counterparts.

How, therefore, ought one objectively characterise what is a police force, what is a military unit and what is a paramilitary unit? In their pioneering analysis of paramilitary forces, Andrew Scobell and Brad Hammitt asserted that state-sponsored paramilitary units tend to fall between that of the regular police and the military.[33] However, distinguishing between paramilitary police units and elements of the military has proven to be problematic.[34]

On the one hand, it could be argued that police and military have distinctly separate roles. A police force is mostly involved in domestic law enforcement and peacekeeping, where its primary adversary is the individual criminal or small group of criminals, usually without political objectives. Police also typically operate in pairs or alone, and rarely rely on coordinated, deliberate actions to apprehend their adversary. Conversely, militaries are employed against external adversaries, and typically operate in formed bodies utilising a range of offensive and potentially highly destructive weapons. On the other hand, however, the two organisations share similar cultures and structures, where members of the police force, like the military, usually wear a uniform and have a hierarchical rank structure. It can be argued, therefore, that all police organisations are 'paramilitary' in nature; where they differ is the degree of their militarisation.

Perhaps the strongest argument to support the notion that paramilitary police units are closer to the military than the police—aside from their weapons, tactics, training and techniques—is that they do not deal as individual officers with individual citizens in a legalistic context. Indeed, we do not see paramilitary police units on routine patrols, making arrests or investigating crimes, much like we do not see the military engaged in such tasks. When we do see paramilitary police units in action, they are typically involved in coordinated and synchronised activities relying on detailed planning, orders and rehearsals— much like the military. Consequently, it would seem reasonable to conclude, with one eye on the definitions in the Geneva Conventions, that a paramilitary police unit is objectively a military force, and that Australian states and territories are prohibited by the Constitution from raising and maintaining such forces.

Domestic security

Section 119 of the Constitution provides that 'the Commonwealth shall protect every state against invasion and … against domestic violence'. This section clearly contemplates an internal security role for the Commonwealth, and indeed implies that the Commonwealth will provide the necessary means for such protection. However, until recently in Australia's federal history, finding the authority for the ADF's involvement in domestic security was more elusive.

For the first 100 years of federation, the Commonwealth relied on the so-called executive

power in section 61 of the Constitution and the residual prerogative powers of the Crown for the control and disposition of the ADF. In 2000, amendments to the *Defence Act 1903* provided a statutory footing for most potential domestic security actions by the ADF.[35] Further amendments in 2006 provided for members of the ADF to defend property designated as critical infrastructure, even without direct threat to life.[36]

These amendments also provide for the use of lethal force by the ADF to destroy certain aircraft and ships at sea, as well as the powers to cordon and search, both at sea and ashore. The key pre-conditions are that 'domestic violence' must be occurring (or likely to occur) and the relevant state or territory is not able to protect national interests. Importantly also, the amendments provide a degree of protection from liability for ADF members acting under orders in the implementation of such tasks.

Of particular relevance are the powers and protections conferred to individual members of the ADF in dispensing their duty under Part IIIAAA of the *Defence Act 1903*, particularly section 51I, when compared to powers and protections under state or territory laws for civil police in similar domestic law enforcement scenarios. This section provides that a member of the ADF may prevent or put an end to violence; protect persons from acts of violence; detain a person whom they believe on reasonable grounds has committed an offence; control the movement of persons or means of transport; and conduct searches of persons, locations or things and seize things related to domestic violence.

This may be contrasted with the powers provided to officers under the *Australian Federal Police Act 1979*, many of which are analogous to the powers conferred on Defence members under the *Defence Act 1903*. [37] Also, given that many recent deployments of the ADF have been on peace-keeping or nation-building roles, there ought to be little concern over whether the ADF can dispense these duties and obligations with due regard to liberal democratic notions.

Conclusion

The Australian public's seeming reluctance to support the use of the ADF in domestic security operations may be explained in part by historic examples where the military was employed on home soil, such as in breaking the coal-miners' strike in NSW in 1949. However, the premises on which these concerns are based have little relevance in a modern world where fourth-generation warfare is now the predominate paradigm.

This article has argued that public concern should instead be focused on the largely unchecked and seemingly unconstitutional development of paramilitary police units around Australia. The continued development of paramilitary police units, which train with the ADF, are equipped with weapons and vehicles used by the ADF, and see themselves akin to special-force soldiers, foreshadows a deeply concerning development in civil policing culture, as such practices and attitudes may percolate down to the general duties police officer. Left unchecked, the very concerns that society has towards relying on the ADF in domestic security operations may become reality, as the police, who have vastly more coercive powers, are the very agents to bring these concerns to reality.

Captain John Sutton is a full-time LLB(Hons) candidate at the University of Queensland. He graduated from the Royal Military College, Duntroon in 2007 as an Army Reserve infantry officer. He has served in 9th Battalion, The Royal Queensland Regiment and 25th/49th Battalion, The Royal Queensland Regiment, as well as a Civil Military Cooperation tactical support team. He is currently on the staff of the Army Personnel Administration Centre-South Queensland.

References

1 Michael Head, 'Calling out the troops and the *Civil Contingencies Act*: some questions of concern', *Public Law*, Vol. 231, Issue 430, 2010, p. 433; and Jude McCulloch, 'War at home: national security arrangements post 11 September 2001', *Alternative Law Journal*, Vol. 27, No. 2, 2002.

2 Jude McCulloch, 'Paramilitary surveillance: S11, globalisation, terrorists and counter-terrorists', *Current Issues in Criminal Justice*, Vol. 13, No. 1, 2001.

3 Hugh Smith, 'Calling out the troops', *Australian Army Journal*, Vol. 7, Issue 2, 2010.

4 Margaret White, 'The executive and the military', *University of NSW Law Journal*, Vol. 28, Issue 2, 2005.

5 White, 'The executive and the military'.

6 David Gadd, 'In the aftermath of violence: what constitutes a responsive response?', *British Journal of Criminology*, Vol. 55, Issue 1, 2015.

7 The scope of this research is limited to non-maritime and non-Air Force use of the ADF in an aid to the civil power capacity.

8 Stephane Beaulac, 'The Westphalian model in defining international law: challenging the myth', *Australian Journal of Legal History*, Vol. 11, Issue 1, 2004.

9 Pat Phelan, 'Fourth generation warfare and its challenges for military and society', *Defence Studies*, Vol. 11, Issue 1, 2011.

10 Specifically, The Hague Conventions of 1899 and 1907.

11 William S. Lind, 'Understanding fourth generation war', *Military Review*, Vol. 84, Issue 5, 2004.

12 *Criminal Code* 1995 (Cth) section 100.1, Chapter 5, Part 5.3, Division 100.

13 Françoise Bouchet Saulnier, *Practical guide to humanitarian law*, 3rd ed., Rowman & Littlefield: Lanham, 2014.

14 Kate O'Donnell and Simon Bronitt, 'The Hilton bombing, calling out the troops and turning points in history', *Criminal Law Journal*, Vol. 38, Issue 59, 2014.

15 See, for example: Head, 'Calling out the troops and the *Civil Contingencies Act'*; Simon Bronitt and Dale Stephens, 'Flying under the radar – the use of lethal force against hijacked aircraft: recent Australian developments', *University Commonwealth Law Journal*, Vol. 7, Issue 2, 2012; White, 'The executive and the military'; and Cameron Moore, 'Calling out the troops – the Australian military and civil unrest: the legal and constitutional issues', *Melbourne University Law Review*, Vol. 33, Issue 1022, 2009.

16 Jude McCulloch, *Blue army: paramilitary policing in Australia*, Melbourne University Press: Melbourne, 2001.

17 See, for example: Cameron Moore, *The Australian Defence Force and executive power: limiting the indefinable*, Australian National University: Canberra, 2014.

18 Michael Head, *Calling out the troops: the Australian military and civil unrest*, Federation Press: Annandale, 2009, p. 144.

19 Australian Army, *Manual of Land Warfare, Part One, Vol. 3, Pamphlet No 2: Aid to the civil power*, Department of Defence: Canberra, 1983.

20 Head, *Calling out the troops*, p. 140.

21 White, 'The executive and the military'.

22 Commonwealth of Australia, *Protective Security Review Report* (unclassified version), Australian Government Publishing Service: Canberra, 1979.

23 *Communist Party Case* (1951) 83 CLR 1.

24 Aldo Borgu, 'Beyond Bali', *Australian Strategic Policy Institute* [website], November 2002, available at <https://www.aspi.org.au/about-aspi/press-releases/beyond-bali> accessed 10 May 2017.

25 Head, *Calling out the troops*, p. 144.

26 Jenny Hocking, *Beyond terrorism: the development of the Australian security state*, Allen & Unwin: Sydney, 1993, p. 160.

27 Quoted in Hocking, *Beyond terrorism*.

28 John Haldon Wotten, 'Report of the inquiry into the death of David John Gundy', in *Royal Commission into Aboriginal Deaths in Custody*, national report, Australian Government Publishing Service: Canberra, 1991, p. 4.

29 See Benjamin R. Beede, 'The roles of paramilitary and militarized police', J*ournal of Political and Military Sociology*, Vol. 36, Issue 1, 2008; Donald J. Campbell, 'Soldiers as police officers/police officers as soldiers: role evolution and revolution in the United States', *Armed Forces & Society*, Vol. 36, Issue 2, 2010; and Sam Mullins, 'Counter-terrorism in Australia: practitioner perspectives', *Journal of Policing, Intelligence and Counter Terrorism*, Vol. 11, Issue 1, 2016.

30 White, 'The executive and the military'.

31 US Code Title 10 Armed Forces, Subtitle A (General military law), Part I, Chapter 15, section 331, *Legal Information Institute* [website], available at <https://www.law.cornell.edu/uscode/text/10/subtitle-A> accessed 10 May 2017.

32 Australian Federal Police: Special Response Group; New South Wales Police Force: Tactical Operations Unit and State Protection Support Unit; Northern Territory Police: Territory Response Group; Queensland Police: Special Emergency Response Team; South Australian Police: Special Tasks and Rescue; Tasmanian Police; Special Operations Group; Victoria Police: Special Operations Group and Critical Incident Response Team; Western Australia Police; Tactical Response Group.

33 Andrew Schobell and Brad Hammitt, 'Goons, gunmen, and gendarmere: towards a reconceptualization of paramilitary formations', *Journal of Political and Military Sociology*, Vol. 26, Issue 213, 1995.

34 Beede, 'The roles of paramilitary and militarized police'.

35 These amendments were enacted via *Defence Legislation Amendment (Aid to Civilian Authorities) Act 2000*, see *Federal Register of Legislation* [website], available at <https://www.legislation.gov.au/Details/C2004A00711> accessed 10 May 2017.

36 These amendments were enacted via *Defence Legislation Amendment (Aid to Civilian Authorities) Act 2006*, see *Federal Register of Legislation* [website], available at <https://www.legislation.gov.au/Details/C2006A00003> accessed 10 May 2017.

37 *Australian Federal Police Act 1979*, Part 3, Division 3.

Shock and awe? An examination of the terrorist group ISIL and its future prospects

Lieutenant Colonel Mark Smith, Australian Army

Islamic State of Iraq and the Levant (ISIL) leapt to public prominence when the Iraqi city of Mosul fell to its forces in 2014, demonstrating a spectacular military success for ISIL but also being portrayed as a strategic shock to the West.[1] However, rather than reinforcing this 'strategic shock' narrative, this article will argue a countervailing view that ISIL did not emerge spontaneously but rather over the preceding decade as a consequence of the broader 'war on terrorism', the failure of the Arab Spring and the alienation of Sunni populations in Iraq.

Over the course of its evolution, despite changing names and affiliations, ISIL's activities have generally been oriented towards achieving a Sunni Islamic caliphate. In particular, ISIL's success has been relatively unique in the sense that it has asserted (and proven capable of defending) a territorial claim. Western strategy against ISIL has typically focused on containment, using airstrikes and 'advise and assist' mentoring teams. However, ISIL's skilful and extensive use of media operations has allowed the group to achieve disproportionate influence relative to other groups. Its methodology has led to a high influx of foreign fighters and local acts of terrorism inspired by a so-called 'self-radicalisation' process driven by ISIL propaganda.

This article does not contend that ISIL presents an existential threat to Australia's national security; indeed, it acknowledges that other challenges, such as the re-emergence of China as a major power, are far more pressing in the strategic domain. However, it will be argued that ISIL does present a significant security threat to Australian interests, a view echoed by the Australian Government in the *2016 Defence White Paper,* which asserted that:

> [A] major threat … [Australia] is currently facing is from violent extremism perpetrated or motivated by terrorist groups such as Daesh, al-Qa'ida and others that claim to act in the name of Islam. The anti-Western narrative of terrorists means that Australians will continue to be targeted at home and abroad.[2]

Clearly, a comprehensive examination of every aspect of ISIL is beyond the scope of this article. Accordingly, it focuses on three key stages of ISIL: its emergence as a terrorist group, its evolution, and its future prospects. Each of these areas will be examined with a selection of critical elements analysed in depth. The analysis concludes that while ISIL's fortunes have ebbed and flowed, generally the group has proven resilient, is capable of learning and adapting quickly, and is likely to maintain a competitive advantage over other groups for a considerable period.

Emergence

In describing ISIL's emergence, several elements will be examined; first, ISIL's declaration as a terrorist organisation; second, the history of religiously-motivated terrorism; third, a summary of the influence of ISIL's founder and his affiliations with other groups; and fourth, the group's fractious relationship with al-Qa'ida.

While ISIL rose to public prominence in 2014, its antecedents can be traced back well into the preceding decade. In 2013, the Australian Government, mirroring other nations, listed ISIL as a terrorist organisation under the *Criminal Code Act (Commonwealth) 1995,* based on it being 'one of the world's deadliest and most active terrorist organisations [which] conducts daily attacks on security forces and civilians'.[3] The proclamation noted also that ISIL adheres to a global jihadist ideology and, in so doing, prepares, plans, assists and fosters terrorist acts with the aim of establishing a Salafist-orientated Islamic State spanning Iraq, Syria and the Levant.

Significantly, in making this listing, the Australian Government described previous determinations relating to the group, including the listing of pre-cursor groups such as *Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn* (Al-Qa'ida in Iraq [AQI]) in 2005, and later *Dawla al-Islamiya (Islamic State) in 2014.*[4] These name changes, which will be explored shortly, reflect changes in the group's operating area and its aspirations for an Islamic caliphate.

ISIL is certainly not the first group to invoke religion as a catalyst for political change. ISIL follows the practice of a multitude of organisations and individuals, such as the Sikh Khalistani movement in India, the Catholic Irish Republican Army and the ultra-Christian Timothy McVeigh in the Oklahoma bombing.[5] Similarly, groups such as the Islamic *Kharijites* of the 7th century and, more recently, the Muslim Brotherhood—established in 1928 and with a presence in over 70 countries—invoke religion in their goals to restore a fundamentalist version of Islam and establish a caliphate for Muslims.[6] This article asserts that ISIL's deliberate leveraging of religion for political power has been essential to its emergence and has, in the Clausewitzian sense, provided the group with its 'centre of gravity' from which it has drawn strength and inflamed the passions of the people.[7]

Clearly, the role of a terrorist organisation's founder is important, and ISIL is no different. The group's founder, Abu Musab al-Zarqawi, was born in Jordan, where he was involved in criminal groups, before joining the group *Tablighi Jamaat.* It was here, in 1989, that his tactical ability and ruthlessness was recognised while fighting Soviet forces (and other local factions) in Afghanistan.[8] Following these exploits, he returned to Jordan where he joined *Jund al Sham* and undertook a number of operations before being captured by Jordanian authorities. During his incarceration, he become further indoctrinated in jihadi views and adopted a strict application of Sharia law.[9] Following his release in 1999, he flew to Afghanistan (via Pakistan) following an unsuccessful bombing planned at the Jordanian Radisson Hotel.[10]

Central to ISIL's overall philosophical approach was al-Zarqawi's personal beliefs. He had been strongly influenced by the teachings of Muhammad ibn 'Abd al-Wahhab. Wahhab, who lived in the 17th century, argued for an interpretation of the Quran that aimed to restore the 'purity of Islam in Arabia … [and which] violently suppress[ed] all Arab Muslims who resisted his fundamentalist version of Islam'.[11] These Wahhabi-inspired practices would see ISIL targeting Shi'a Muslims, a practice that would encourage sectarian killings and ultimately pit ISIL against al-Qa'ida's strategic direction.[12]

Al-Zarqawi initially affiliated himself with al-Qa'ida—including meeting with and receiving funding from Osama bin Laden to establish training camps—before fighting alongside al-Qa'ida in Afghanistan.[13] In anticipation of US-led operations, Al-Zarqawi travelled to Iraq and

commenced preparations for insurgency-based activities. He renamed his group *Tanzim Qa'idat al-Jihad fi Bilad al-Rafidayn* (AQI) and swore allegiance to Osama bin Laden.[14] AQI's stated aims were to create an insurgency to topple the Iraqi government, kill regime collaborators, target Shi'a civilians and establish an Islamic state.[15]

While many similarities exist between al-Qa'ida's general Salafist/Wahhabist approach and that of AQI, the latter adopted a more austere Hanbalist Salafi interpretation, wherein AQI believed that only Sunni Muslims were true Muslims and hence gravitated towards sectarian violence.[16] This philosophy saw Shi'a being considered subject to *takfir* (subject to death) and legitimised them as targets.[17] Al-Zarqawi's methodology differed from the broader al-Qa'ida approach in that it deliberately targeted Shi'a Muslims and sought to exploit social media far more effectively than al-Qa'ida.

A contributing factor to the emergence of ISIL lay in Western strategy itself, being the application of a 'disaggregation' policy, which sought to break the 'global jihad' franchise into smaller localised issues.[18] The policy, while initially successful, later proved to be ineffective in the sense that it treated every insurgency as a localised issue, and led to strategic dissonance with differing (and often contradictory) narratives regarding the global war on terror.[19]

Such dissonance led to inconsistent messaging to counter what was a 'global jihad' franchise system and to strategically short-sighted decisions, such as the decision to invade Iraq itself and a failure to appreciate (or commit) the requisite forces needed to maintain law and order in Iraq. An exemplar of this dissonance can be found in the Iraqi Provincial Authority's decision to reduce the influence of the prominent Bath party from the Iraqi government, which further degraded the Iraqi indigenous capacity not only in the security sector but across finance, education and science. This led to a volatile security situation, failing essential services and a power vacuum that provided AQI an opportunity to expand its influence.

The consequences of AQI's approach were twofold: first, al-Qa'ida became increasingly alarmed at the group's targeting of Shi'a and broke ties with al-Zarqawi; second, it provoked the predominantly Shi'a government to over-react against Sunnis. By leveraging sectarian violence, al-Zarqawi had gained political opportunity and power, and he branded AQI as 'all that stood between Sunnis and the Shi'a death squads, giving people no choice but to support … [AQI] regardless of what they thought of [its] ideology'.[20]

The violence between Shi'a and Sunnis continued to escalate and was exacerbated by community perceptions that the Shiite Iraqi Prime Minister Maliki was indifferent to Sunni concerns. This perception supported AQI's narrative and encouraged the group's strategy of attrition.[21] Al-Qa'ida continued to protest AQI tactics and, in a series of envoys and letters, the disagreements between the groups escalated. Shortly afterwards, on 7 June 2006, al-Zarqawi was killed by an airstrike after being tracked by US forces, having reportedly been 'sold out' by al-Qa'ida leaders.[22]

Evolution

Having described ISIL's emergence, key 'evolutionary' stages will now be examined through the prism of the group's learning and adaptation, political objectives and the strategic environment. Specifically, four evolutionary stages will be analysed: first, AQI's amalgamation with other groups and changes in US strategy in Iraq; second, the opportunity provided for organisational growth within Camp Bucca; third, the group's adaptation following the Arab Spring into a 'hybrid force' capable of both insurgency-based and conventional warfighting; and, finally, ISIL's ability to assert and maintain its territorial claims in Iraq and Syria.

The first evolution of ISIL occurred in the months following al-Zarqawi's death, as the group changed into a nascent version of ISIL as we understand it today. In October 2006, the group united with other groups and Sunni tribes to form the Islamic State of Iraq (ISI), with Abu Omar al-Baghdadi announced as the organisation's Caliph.[23] In contrast to al-Qa'ida's notion of global Islamic uprising, the newly formed ISI prescribed the creation of a real-world caliphate as an immediate objective, and determined that continuing the violence against the Shi'a was the fastest road to achieve it.[24]

Concurrent with this significant evolutionary step, a number of external events were occurring that would degrade the group's newfound growth. Two of these events reflected changes in the coalition's strategy, the first being the adoption of a counterinsurgency approach (in contrast to the previous counter-terrorism approach), and the second being the coalition's support to the 'Sunni awakening'.[25] Ultimately, these twin occurrences seriously degraded the group to the extent that, in 2006, ISI described itself as being 'in extreme'.[26]

The US, recognising that the mission to Iraq risked strategic if not operational failure, invested in the 'surge' of 2007, which saw significant numbers of troops committed in a counterinsurgency role, supported by a new doctrine crafted by General David Petraeus.[27] Part of this strategy saw Petraeus (and the US President) more actively involved in dealing with Iraqi Prime Minister Maliki, which started to curtail his biases and shape him to be more inclusive in his decision-making, which significantly reassured Sunni Muslims.[28]

Encouraged by the changes in US strategy, the 'Al-Anbar awakening' (later the Sunni awakening), saw Sunnis adopt a local patrolling and militia approach to protecting their communities. Some of these groups, such as the 'Sons of Iraq', saw local sheiks turn against AQI and other insurgencies and offer their support to coalition forces and the Government of Iraq.[29]

The consequence of these changes in the operating environment was dire for ISI, as the grievances they sought to exploit were now being resolved (relatively) peacefully and through legitimate channels. Essential services were being restored, and security was improving as a consequence of the surge and Sunni awakening. This significantly damaged the group's value proposition in relation to its supporters and competitors. In 2010, General Raymond Odierno, Commander of US Forces in Iraq, remarked in a press conference relating to the death of ISIL's latest leader, Abu Omar al-Baghdadi, that '80 per cent of the ISI's top 42 leaders, including recruiters and financiers, had been killed or captured, with only eight remaining at large'.[30]

Providentially (for ISIL), the Coalition's success in neutralising the previous leadership now provided an opportunity for the group's second significant evolution—the introduction of ex-Ba'athists into the group's leadership. ISI's new leader, Abu Bakr al-Baghdadi, had been captured by the Coalition and imprisoned at Camp Bucca, an internment facility of some 20,000 Iraqis. Al-Baghdadi thus found himself perfectly positioned to attract new recruits to ISI and stiffen its membership with ex-Ba'athists, many of whom were veterans of the Iraqi Army.[31]

ISI thus emerged with new leadership, having undergone significant learning and adaptation (through the sharing of lessons learned), which saw the group emerge with 'the ideological fervour of [ISI and] … the organisational skills of [ex-Ba'athists]'.[32] The group, newly empowered, was thus perfectly positioned to take its next evolutionary step, one that would be provided by the failure of the Arab Spring.

The Arab Spring was a democratic uprising that began in Tunisia and quickly spread across Egypt, Libya, Syria, Yemen, Bahrain, Saudi Arabia and Jordan.[33] These uprisings met with mixed results but, in the case of Syria, disenchantment with the ruling Assad regime and wider Shi'a-Sunni disputes led to the start of violent civil war.[34] These Syrian events would be critical to ISI's third significant evolutionary step—expansion into Syria using hybrid warfare and asserting territorial claim.[35]

In 2013, ISI expanded into Syria and became known as the Islamic State of Iraq and Syria (ISIS) as it partnered with the Syrian group *Jabhat al-Nusra*. Initially, ISIL, while not allied to the Syrian Assad Government, adopted what has best been described as a 'non-confrontation footing' with Assad, which provided a relative safe haven for the group to operate in.[36] However, this footing changed as the group commenced combat operations using a mix of both insurgency-based and conventional-combat operations in Raqqah province, ultimately establishing a presence in Al-Hasakah province and intimidating a number of other provinces to swear allegiance to ISIL.[37]

Thus, by 2014, ISIL achieved its fourth evolutionary step; it was able to assert a territorial claim in northern Iraq and Syria, and with a fighting force of some 20,000 fighters, was capable of defending it, while implementing Sharia law

within the areas it now controlled.[38] Following these accomplishments, al-Baghdadi publicly declared that the Islamic Caliphate had been established and called on all Muslims to emigrate to the caliphate, with a stated expectation that they would defend it.[39]

This final evolutionary stage saw ISIL expanding and capturing additional territory, including Mosul, Fallujah and even moving into Kurdish territory. With this expansion, the realised tangible benefits, such as the opportunity to seize abandoned and captured military equipment, raid financial reserves and capture oil and gas fields, allowed ISIL to profit from the use or sale of these commodities.[40] In addition, as the organisation matured, it restored a wide assortment of essential services normally associated with government, including medical care and security, but also dispute-resolution courts, which allowed ISIL to demand taxes from its new constituents.[41] These measures marked ISIL as distinctly different from many groups that had preceded it: it no longer required donations but was capable of producing its own domestic product, becoming largely self-sufficient and 'the richest terrorist organisation' to date.[42]

Thus, it is argued that by the end of the 'fourth evolutionary stage', ISIL had met three of the four elements of statehood, within the definition provided by the Montevideo Convention adopted by the League of Nations in 1933: the Caliphate now occupied a defined territory (and had proven capable of defending it); it maintained a permanent population within its borders; and provided government and essential services to its constituents. The only missing element was international recognition and the capacity to enter into relations with other nation-states.

In addition to these four major evolutionary stages, a fifth evolution has been the group's sophisticated use of social media, which has been one of the cornerstones of ISIL's success, providing it greater resilience when compared to other groups. After first describing the pivotal role of social media—critical to ISIL's future prospects—the article will examine other elements considered important for the group's future prospects, including remote and self-radicalisation, maintenance of its territorial claim, and its response to the Western containment strategy.

Future prospects

ISIL's future prospects will continue to be dependent on social media, with the group potentially able to recruit more foreign fighters and inspire more 'remote radicals'. In a report tabled to the Australian Parliament in 2015, the Australian Security Intelligence Organisation (ASIO) reported that ISIL generates extensive media coverage with radio bulletins (in five languages), four photographic reports, three high-definition videos every day, and high-quality monthly magazines and movies.[43] Further, ASIO reported that ISIL had leveraged this unprecedented media presence (in terms of breadth and volume of content) to attract over 120 Australians to join ISIL as foreign fighters in the Middle East, with a further 160 actively supporting from Australia.

While the use of social media is not its exclusive province, ISIL has proven to be one of the most adroit users, quickly adopting what has been described by Yannick Veilleux-Lepage in 2016 as a paradigmatic shift, in that ISIL uses the medium to encourage self/remote radicalisation which, when aligned with parallel activities, inspires lone-wolf actors in support of ISIL.[44] In this regard, he contends ISIL no longer directs or controls attacks (as its predecessors did) but rather inspires and enables lone actors to take action.

This self/remote radicalisation methodology offers a glimpse into ISIL's future prospects, as it has reputedly inspired attacks both domestically and internationally. Domestically, in the last two years, three ISIL-inspired attacks have been successful, targeting police in two separate attacks in Victoria and NSW, and civilians in the Lindt Café siege in Sydney.[45] Additionally, ASIO further thwarted attempts in Sydney, Melbourne and Brisbane, and has reported a rising number of passports being revoked annually. Internationally, attacks in Paris, Belgium and Tunisia reinforce this potential future threat.

Moreover, as suggested in Jason Logue's 2015 article 'Propaganda of the deed' and Andrew Watkin's 2016 'Losing territory and lashing out', it is likely that ISIL activities and attacks will increase in an effort to divert attention from the group's losses in a particular area.[46] This suggests that, in future, spectacular attacks and violent executions should be interpreted as an indicator of desperation rather than strength.

This article asserts that ISIL's key strength is its media operations, and posits that it is likely to retain significant capability into the near future. The information domain reflects the flaws in the aforementioned disaggregation strategy, in that the absence of a unifying (Western) strategic narrative has created an uncontested space in which ISIL has been allowed to dominate. Degrading ISIL's social media capabilities through effective social cohesion messaging will require an 'integrated, coordinated, and synchronized approach' to counter the spread of ISIL propaganda'.[47] To effectively counter ISIL's message, authorities will need to work with Muslim communities, not against them, in the manner suggested by NSW's recently-conducted 'Countering Violent Extremism' project in western Sydney.[48]

The second area that will influence ISIL's prospects is its ability to maintain its territory, both in the central Caliphate and through its broader territorial claims of the group's *wilayat* (devolution of power) system of provinces in Libya, Algeria, Egypt, Yemen and Saudi Arabia. While ISIL has shown the ability to retain territory militarily, in the long term its conventional forces may be insufficient to defend its declared territory. Moreover, having adopted a nation-building approach within its territory (echoing in some parts the US counterinsurgency doctrine described earlier), ISIL will have a long-term obligation to provide these essential services in order to be seen as providing legitimate government to its population.

ISIL is already struggling to deal with many contentious issues within its territory, such as taxes, kidnapping, slavery, extreme justice and religious persecution of minority groups, which will continue to have implications for the community support for the shadow government, particularly if containment measures continue to reduce ISIL's revenue streams. Potentially, responses that target ISIL's legitimacy—both militarily and through other instruments—could push ISIL 'back to its roots as a rural insurgency operating largely outside the cities'.[49]

Finally, the role played by Western strategy itself is an important consideration in ISIL's prospects. This article will specify three elements as particularly relevant: not over-reacting to ISIL activities, thereby (counter-productively) enhancing ISIL's claims to legitimacy through over-securitisation of Muslims; enhancing the containment strategy; and finally, selecting the end-state desired.

ISIL has demonstrated a keen ability not only to promote sectarian violence but also to embrace a methodology designed to 'terrorise, mobilize and polarize' people towards it, as the lesser evil.[50] ISIL's successful social media and operations have thus provided an appealing concept to disenfranchised citizens, who become attracted to ISIL's sense of purpose which leads, in a sense, towards the mass-mobilisations described in Eric Hoffer's *The true believer: thoughts on the nature of mass movements* (1951), where ISIL relies on both 'pull' and 'push' recruiting techniques.

The allure of ISIL recruiting can be mitigated by authorities and mainstream media deliberately avoiding 'inflaming' ISIL activities and offering compelling counter-narratives that reduce the propagation of ISIL's message.[51] Similarly, the 'push' component can be avoided by not over-securitising Muslim communities and conforming to ISIL's objectives.

The current Western strategy of containment, as described earlier, comprises mainly airstrike and 'advise and assist' mentoring teams as the predominant methods to reduce ISIL's territory and render it incapable of administering its territory—essentially allowing it to 'fail under its own weight'.[52] One consequence of this prolonged strategy has been mass migration from Syria and Turkey into Europe which has potentially provided additional opportunities for ISIL members to infiltrate into Europe but also wider disenfranchisement in the Muslim communities, with an ever-present risk of the securitising of these communities, leading to further distrust of government and security agencies.[53]

Describing an alternative strategy is beyond the scope of this article. However, given the group's learning and adaptation over the past decade, it is assessed that ISIL's successes will continue to ebb and flow into the future although, overall, it will likely continue to prove relatively resilient to containment measures.

Having described these response options and ISIL's possible reactions and prospects, it is argued that before a widening of the campaign is contemplated, a number of factors must be considered. The most important would certainly

be a frank assessment of the desired political end-state sought, which may simply be, as argued by Thomas Ricks in 2015, an 'Iraq that is mostly free from extremists, is not a puppet of Iran, and an adequate [Western] partner with some marginally acceptable form of democracy'.[54] Without such clarity, ISIL will continue to prosper in the uncontested spaces (both physical and informational) in which it operates.

Conclusion

ISIL's emergence and evolution over the past ten years is largely a consequence of the broader war on terrorism, failure of the Arab Spring revolution and the alienation of Sunni populations in Iraq. The organisation is relatively unique in the sense that it has asserted and maintained territorial claim, which has been reinforced by a skilful and extensive media operation. These key actions have allowed the group to achieve disproportionate influence—to the degree that disenfranchised members of society have joined ISIS as foreign fighters or through so-called 'self-radicalisation' to carry out attacks in local communities.

This article has focused on three key elements of ISIL: its emergence as a terrorist group; its evolution and its assessed prospects into the future. The article has described ISIL's fortunes as ebbing and flowing but assesses that, in general, the group has proven to be resilient, capable of learning and adapting quickly, and is likely to maintain a competitive advantage over other groups for a considerable period. Notwithstanding the difficulty of predicting these challenges, the article has considered specific and broad implications for Australian security policy in framing response options for the Australian government to reconcile the challenges.

Historically, Australia's unique geography and its economic and security arrangements have protected it from a variety of security threats, terrorism included. However, the increasingly connected and globalised nature of society presents new threat vectors which nation-states, transnational criminal organisations and terrorist groups can exploit. This analysis of ISIL finds that while ISIL is not assessed as an existential threat to Australian strategic interests, the group will continue to present significant tactical and operational challenges to Australia.

Lieutenant Colonel Mark Smith is an Infantry officer with over 20 years' service. He is currently the Commanding Officer of both the 25th/49th Battalion, Royal Queensland Regiment and Battle Group Cannan—the Reinforcing Battle Group generated by 11 Brigade and 13 Brigade. He has a wide variety of regimental postings and his operational deployments include Timor Leste, Afghanistan and Vanuatu.

Lieutenant Colonel Smith has completed a Masters in Military and Defence Studies and a Masters of Business Administration. In addition, he holds a Bachelor of Legal and Professional Studies, and credentials in business, government, management, policing, security and risk management. He graduated from the Australian Command and Staff College (Joint) in 2013 and was the recipient of the Principal's Prize. In his civilian career, he is a Senior Sergeant with the Queensland Police Service, posted as a Senior Strategy Officer. He is also a member of the Department of Foreign Affairs and Trade's Australian Civilian Corps.

References

1   Although the group is known by a number of different names (including Daesh, Islamic State, Islamic State of Iraq and Syria, Islamic State of Iraq and the Levant), ISIL will be adopted as the group's primary name for consistency throughout this article. Any direct quotes from other authors will conform to the naming convention they adopt. See also David Kilcullen, *Blood year: Islamic State and the failures of the war on terror*, Hurst & Co.: London, 2016, p. 4.

2   Australian Government, *2016 Defence White Paper*, Department of Defence: Canberra, 2016, p. 47.

3   Australian Goverment, 'Listed terrorist organisations: Islamic State', *National Security* [website], available at <https://www.nationalsecurity.gov.au/Listedterroristorganisations/Pages/IslamicState.aspx> accessed 10 March 2016.

4   Literally, 'the organisation of Al Qaida in the land of two rivers', that is, Mesopotamia.

5   Hew Strachan, *The direction of war: contempory strategy in historial perspective*, Cambridge University Press: New York, 2013, p. 21.

6   Muhammad Al-Yaqoubi, 'Refuting ISIS: a rebuttal of its religious and ideological foundations', *Sacred Knowledge*, 2015, pp. xvii-xviii.

7   Carl von Clausewitz, *On war*, edited by Michael Howard and Peter Paret, Princeton University Press: Princeton, 1976, Book 1, Chapter 4.

8   Jessica Stern and J.M. Berger, *ISIS: the state of terror*, Harper Collins: London, 2015, pp. 14-5.

9   Craig Whitlock, 'Al-Zarqawi's biography', *The Washington Post,* 8 June 2006.

10 A.S. Hashim, 'The Islamic State: from al-Qaeda affiliate to Caliphate', *Middle East Policy*, Vol. 21, No. 4, 2014;

also A.W. Terrill, 'Understanding the strengths and vulnerabilities of ISIS', *Parameters*, Vol. 44, No. 3, 2014.

11 Mary Halbeck, *Knowing the enemy: jihadist ideology and the war on terror*, Yale University Press: New Haven, 2006, pp. 22-5.

12 Devin R. Springer, James L. Regens and David N. Edger, *Islamic radicalism and global jihad*, Georgetown University Press: Washington DC, 2009, p. 57.

13 A.Y. Zelin, *The war between ISIS and al-Qaeda for supremacy of the global jihadist movement*, Washington Institute for Near East Policy: Washington DC, 2014, pp. 1-2.

14 Springer, Regens and Edger, *Islamic radicalism and global jihad*, p. 21.

15 Hashim, 'The Islamic State'.

16 Springer, Regens and Edger, *Islamic radicalism and global jihad*, pp. 176-7.

17 Hashim, 'The Islamic State'.

18 David Kilcullen, *The accidental guerilla: fighting small wars in the midst of a big one*, Scribe Publications: Melbourne, 2009, p. 263.

19 David J. Kilcullen, 'Blood year: terror and the Islamic State,' *Quarterly Essay*, Issue 58, 2015, pp. 4-11.

20 Kilcullen, 'Blood year', p. 19.

21 Andrew Phillips, 'How al Qaeda lost Iraq', *Australian Journal of International Affairs*, Vol. 63, No. 1, 2009.

22 J. Cantwell and G. Bearup, *Exit wounds: one Australian's war on terror*, Melbourne University Press: Melbourne, 2013, p. 210.

23 Stephen Negus, 'Call for Sunni state in Iraq', *Financial Times*, 15 October 2006.

24 Zelin, *The war between ISIS and al-Qaeda for supremacy of the global jihadist movement*.

25 Kilcullen, *The accidental guerilla*, pp. 115-80.

26 Phillips, 'How al Qaeda lost Iraq'.

27 David Kilcullen, 'The deadly efficiency of ISIS and how it grew on the global stage', *The Guardian*, 12 March 2016.

28 Abdel Bari Atwan, *After bin Laden: Al Qaeda, the next generation*, The New Press: New York, 2012, pp. 38-57 and 212.

29 Alissa J. Rubin and Damien Cave, 'In a force for Iraqi calm, seeds of conflict', *The New York Times*, 23 December 2007.

30 Quoted in Thom Shanker, 'Al Qaeda leaders in Iraq neutralized, US says', *New York Times*, 4 June 2010.

31 Terrence McCoy, 'How the Islamic State evolved in an American prison', *The Washington Post*, 4 November 2014.

32 Richard Barrett, *The Islamic State*, The Soufan Group: New York, 2014.

33 Atwan, *After Bin Laden*, pp. 39-79.

34 H. Kissinger, *World order*, Penguin Publishing Group: New York, 2015, pp. 126-7.

35 Kilcullen, 'Blood year', pp. 61-3.

36 Stern and Berger, *ISIS*, p. 152.

37 K. Katzman, C.M. Blanchard, C.E. Humud, R. Margesson and M.C. Weed, *The 'Islamic State' crisis and US policy*, Congressional Research Service: Washington DC, 2015, p. 9.

38 Hashim, 'The Islamic State'.

39 Atwan, *After Bin Laden*, p. 17.

40 M. Styszynski, 'ISIS and Al Qaeda: expanding the jihadist discourse', *Counter Terrorist Trends and Analysis*, Vol. 6, No. 8, 2014, pp. 9-14

41 Stern and Berger, *ISIS*, p. 114.

42 Phillips, 'How al Qaeda lost Iraq'; also Stern and Berger, *ISIS*, p. 46.

43 Australian Security Intelligence Organisation (ASIO), *ASIO report to Parliament 2014-2015*, Commonwealth Publishing Service: Canberra, 2015.

44 Yannick Veilleux-Lepage, 'Paradigmatic shifts in jihadism in cyberspace: the emerging role of unaffiliated sympathizers in Islamic State's social media strategy', *Journal of Terrorism Research*, Vol. 7, No. 1, January 2016.

45 ASIO, *ASIO report to Parliament 2014-2015*, p. 45.

46 Jason Logue, 'Propaganda of the deed: how insurgents are seizing the initiative in the information environment', *The Strategy Bridge* [website], 2015, available at <https://medium.com/@JasFourTwo/propaganda-of-the-deed-808fdfd4b6bc#.vnwigj2si> accessed 21 March 2017; also Andrew Watkins, 'Losing territory and lashing out: the Islamic State and international terror', *Combating Terrorism Center – Sentinel*, Vol. 9, No. 3, March 2016, available at <https://www.ctc.usma.edu/posts/march-2016> accessed 22 March 2017.

47 Veilleux-Lepage, 'Paradigmatic shifts in jihadism in cyberspace', p. 46.

48 Roslyn Richardson, 'Fighting fire with fire: target audience responses to online anti-violence campaigns', *Australian Strategic Policy Institute* [website], 2014, available at <https://www.aspi.org.au/publications/fighting-fire-with-fire-target-audience-responses-to-online-anti-violence-campaigns/Fight_fire_short_paper.pdf> accessed 22 March 2017.

49 Michael Knights, 'ISIL's political-military power in Iraq', *Combating Terrorism Center* [blog], 27 August 2014, available at <https://www.ctc.usma.edu/posts/isils-political-military-power-in-iraq> accessed 21 March 2017.

50 Jason Burke, 'Islamic State "goes global" with Paris attacks', *The Observer*, 14 November 2015.

51 Lauren Williams, 'Islamic State propaganda and the mainstream media', *Lowy Institute* [website], 29 Feburary 2016, available at <https://www.lowyinstitute.org/publications/islamic-state-propaganda-and-mainstream-media> accessed 21 March 2017.

52 Mara Revkin and William McCants, 'Experts weigh in: is ISIS good at governing?', *Brookings Institute* [website], 20 November 2015, available at <https://www.brookings.edu/blog/markaz/2015/11/20/experts-weigh-in-is-isis-good-at-governing/> accessed 21 March 2017.

53 Springer, Regens and Edger, *Islamic radicalism and global jihad*, pp. 27-39 and 201.

54 Thomas E. Ricks, 'To destroy ISIS in Iraq, start with the desired end state and work backwards', *Foreign Policy*, 26 May 2015.

The experiences of Australian military spouses on overseas postings: a qualitative study

Dr Narelle Biedermann, James Cook University

Military families encounter numerous relocations and absences due to deployments in support of the military member's career, which has been widely demonstrated to have an impact on the psychosocial well-being of military spouses.[1] The impact of the stressors associated with military relocations and deployments is like a pebble dropped into a pond, where the ripples extend out far beyond the drop zone.

Indeed, Saltzman *et al* suggest everything that comes with military service—the good *and* the bad—is a family matter.[2] Support from the family is critical to the success of the military member.[3] One area lacking in the literature concerns the experiences of spouses of members of the ADF, particularly in relation to their experiences with postings. The purpose of this study was to explore the experiences of Australian men and women who accompany their military spouse on an overseas posting using a qualitative research methodology.

This research project is unique in Australia. While the experiences of members of the ADF, and indeed international militaries, are frequently examined in research undertaken from within the ADF, as well as by external researchers, using both quantitative and qualitative approaches, the experiences of families are often neglected. It is recognised that military spouses live a life that is both uncertain and exciting.[4] Also often acknowledged is their capacity to cope and adjust to uncertainties, and their ability to 'keep the home fires burning' during extended periods of separation while their military partner is deployed or absent from the family residence.[5]

Australian research to date has focused on the experience of spouses during military deployments, all of which found that prolonged separations associated with deployments are profoundly stressful life events that can have a negative effect on health and wellbeing.[6] Internationally, research exploring the experiences of military spouses during deployments reports

that it often is an extremely stressful and distressing period.[7] Additionally, some international research has been conducted into the experience and impact of military separation on children.[8]

Through the conduct of a literature search, the author found no evidence of research in Australia on the experience and impact of overseas postings on spouses. One comparable study from the UK, using a descriptive qualitative design, examined the experiences of 13 British military spouses and concluded that the experience is largely dependent on the spouse's personality, resilience and support networks.[9] However, the UK study was limited insofar as all but two of the participants were spouses of serving officers, which may not be representative of the experiences of spouses of others. Furthermore, some participants were still on their overseas posting at the time, which may have affected their reflections of the experience. Nonetheless, it provided a solid framework on which to build this current study.

The ADF supports its personnel and their families through the Defence Community Organisation (DCO). The official DCO website provides information and guidance for aspects of Defence life that affects families, including postings.[10] Unfortunately, this information is specific to postings within Australia. Preparations for overseas postings occur often only through word-of-mouth from others that have gone before or who are currently overseas, and varying levels of support from staff in overseas posting cells.

Method

A qualitative approach was utilised to evaluate data generated through an asynchronous virtual focus group. As the author sought to understand a human experience, qualitative methods were employed to allow the data to speak for itself, enabling a better understanding of the phenomenon, and acting as a guide for further research and reflection.

The author's Institutional Human Ethics Board approved the study, which included methods to secure the protection of human subjects. To protect the privacy of participants and their ADF spouse, no names or other identifying features have been used throughout this paper.

To be eligible to participate, participants must have accompanied their ADF spouse on an overseas posting for a minimum of one year, and have been back in Australia for at least six months. A secret Facebook page was set up and those who agreed to participate were given access to this page. Facebook was chosen as the 'location' for the study group as this social media platform is frequently used as a support system for military spouses, particularly for maintaining contact with family and friends during overseas postings.

Procedures

Participants were recruited through private and secret Facebook groups that are only open to Australian military spouses and partners. Spouses who contacted the researcher in response to the researcher's advertisement were provided with an information sheet that gave more detail about the project, as well as their role and rights as participants.

In total, 23 spouses participated in the project, whose partners represented all three branches of the ADF, comprising 12 from Army, 9 from RAAF and 2 from RAN. All participants were female, as no male spouses responded to the invitation.

Data collection occurred over the course of one month, which was analysed using a thematic approach in which codes were derived from the raw data in an inductive analysis.[11] To ensure credibility in the analysis, the participants' own words have been used to illustrate the themes in this paper.

Results

Participants unanimously reported that overseas postings require numerous physical, psychosocial and cognitive adjustments—some of which were unexpected. However, nearly all reported that the posting was a highlight of their married lives. Four key themes were identified, relating to sacrifices for the good of the family; adjustments to a new environment; seeking support; and personality and resilience. Numerous sub-themes emerged from these themes, which are presented in Table 1.

Key theme	Sub theme
Sacrifices for the good of the family	• The 'good military wife' • Adjustments to family way of life • Impacts on health and relationships • Impacts on career
Adjustments to a new environment	• Adaptation to new culture – military and host nation • Culture shock • Coping mechanisms • Influence of rank on experience
Support	• Informal support networks • External support networks
Personality and resilience	• Preparation of self • Approach to problems • Past experiences

Table 1: Key themes and sub-themes

Theme 1: sacrifices for the good of the family

A predominant theme centred on sacrifice, and the regard participants placed on their family above themselves. Several sub-themes emerged as descriptors of the sacrifices made for the good of the family, namely the 'good military wife'; changes to family way of life; impacts on health and relationships; and impacts on career and identity.

According to the participants, sacrifice that comes with life as a military wife, especially during an overseas posting, is expected and accepted. Being a spouse of a serving member means they must relinquish control regularly to the needs of the ADF—be it at posting time where they have no control over the location where their spouse, and therefore, their family are sent, or when their spouse might deploy or go away for an extended period.

One such sacrifice includes a sense of duty to the spouse in such a way that it mirrors the sacrifice the service member makes in his or her service to the country. Most participants described themselves as a 'good military wife', insofar as their role as an overt supportive partner in their

husband's career was an important part of their identity. The posting may not have been best for the spouse or the children but because it was important for their husband's career, they fully supported the posting. Comments included:

> I knew how much he wanted this posting, and being the good military wife I am, I was genuinely happy for him. I just needed to have a couple of cries … to feel better.

Another sacrifice comes from changes to the family way of life and its configuration in the pursuit of an overseas posting. For example, several participants described the sadness of having to leave their beloved family pets behind:

> Having no children, our dog was our baby and that was the hardest thing to leave her behind…. [U]nfortunately, she passed away while I was [overseas].

Overseas postings brought about some particular challenges for blended families, in which there were step-children and shared custody considerations. This was described as being significantly more traumatic than anticipated,

and while Skype enabled regular face-to-face communication with their children back in Australia, it was not the same as having them come to stay during school holidays and weekends.

Some participants were forced to make certain sacrifices to their health and diet throughout their overseas posting because of climatic, cultural and environmental limitations. In some cases, the climate presented an unexpected obstacle in maintaining their health and fitness. Burdened by months of extreme winters in North American and UK postings, an exercise regime was not as easy to sustain as they were accustomed to in Australia:

> The cold and snow stopped us dead in our tracks and we struggled with that the whole time. My children went from being outside adventurers to couch potatoes. We all came back 15kgs heavier!

Other participants indicated that access to healthy and nutritious food in their location proved difficult:

> We found it a challenge to try to maintain a healthy diet like we were accustomed to at home … a lot of heavily sugared [and] processed food was more accessible over fresh produce. We did the best we could to eat healthy, but it was almost impossible or terribly expensive.

An advantage to the sacrifices made to take the overseas postings was that it had a generally positive impact on their relationship with their spouse, and on their family relationships as a whole. Being away from the normal day-to-day life in Australia provided them with opportunities to travel and see the world, which in turn, brought them closer together as a family unit:

> Our relationship was strengthened. We saw a lot more of each other and really got some quality family time.

Because their spouse was home a lot more than he normally was in Australia, simple joys such as family dinners and participation with their children's school and sporting activities were savoured. Others found having their spouse home every night required a period of adjustment, especially for those whose partner had just returned from a deployment immediately prior to their posting:

> We had the added pressure of having [my husband] just return from a 6-month deployment to Iraq, so we were still reacquainting as we moved overseas. It was hard getting to know him again under such stressful circumstances because everything is magnified when they come home from a deployment and everything is stressful when you have to move, so throw them both together in the mix, well, it was ugly. But we knew we'd survive it because we'd survived everything else up until then.

Several participants indicated their overseas postings had a negative effect on their marriage, to the point it led to the dissolution of the marriage. Infidelity was an issue for a number of participants, although this was only observed by those posted to Asian nations. It was suggested that exposure to temptations not normally as readily available in Australia was too much for some spouses, leading to adultery and marriage breakdown. Other participants noted that they were aware that infidelity was an issue in some marriages of ADF families in same location.

The majority of participants who were working prior to their overseas posting reported that they were forced to resign from their job in order to take the posting. Most were philosophical, suggesting this was a sacrifice worth making for the experience:

> As with every posting, I hated giving up my job! I have always struggled to maintain a sense of self-worth when I don't work outside the home ... but our [overseas] posting also meant I could afford not to work, and take some 'me time' for the first time ever! I enjoyed having preschool kids at home part of the day (as opposed to babies when I was last a stay-at-home mum). I also liked being able to go to school events without having to stress about time off work. Lots of spa days, time at the gym ... luxury 'me time' I could never afford in Australia.

Despite the upside of having more time for themselves, several participants noted it was challenging to adjust to being 'dependent' on their spouse financially, suggesting this loss of income influenced their attitude towards money and that this loss of self negatively impacted their sense of identity:

> I lost a bit of my identity. I felt bad for not being able to contribute financially to the family … [and I] felt a bit guilty when I went shopping.

Theme 2: adjustments to a new environment

Four themes emerged as descriptors of adjustments to the new environment or host country: adaptation to a new culture (military and host nation); culture shock; coping mechanisms; and influence of rank on experience.

Participants described themselves as adaptable and quick to adjust to new posting locations and the ADF lifestyle. However, the adjustments required to adjust to their new host country were challenging for all in some way. Language barriers, isolation, cultural nuances, and even climate presented new challenges. It is important to highlight that the participants described having to adapt to two very different cultures—the host nation, and the military their spouse was now serving alongside.

Participants described feeling welcome and 'at home' when they were embraced by the host nation military. Invitations to family events and military-sponsored social activities helped the transition for all family members. Participants posted to North America unanimously agreed they were made to feel very welcome by the host nation military community. Adapting to the host nation proved more difficult in Asia where there was an expectation that Australian families would employ domestic help, such as a housekeeper, and observe the host nation's behaviours associated with their religion, social norms and social class. One spouse described the stressors of arriving in a new country, and quickly finding herself alone:

> [It was] my first time being away from family … [and] having to rely on my new military family was hard for me. We went from the hotel to our house on the Monday and then my husband went to work and I was left in the house on my own with all these amah [local women employed as maids] coming up to the door looking for a job. [In the end], I closed the door, burst into tears [and] wanted to go home.

Culture shock, a well-known term used to describe the early experiences of an immersion in an unfamiliar culture, occurred across the spectrum of all participants, regardless of their posting location. For most, the shock hit the moment they disembarked from their flight, and continued for weeks, as they dealt with smells, traffic, climate, social norms and idiosyncrasies that are not typically found in traveller's guidebooks. In the case of those spouses in English-speaking countries, this was unexpected because they had simply assumed it would be just like living in Australia:

> My culture shock came as a complete surprise. I just made the presumption that going to North America would be an easy transition.

Finding a way to adjust to culture shock was very important, as participants were conscious this was their family's new life for the next year or so:

> [I could not just] wallow in self-pity at not having a clue what was going on. [Rather, I needed to] hook in and do whatever it took to acclimatise. I had to go outside my comfort zone, but I just had to do it.

Theme 3: seeking support

Support for military families in Australia came in a variety of formal, Defence-sponsored or supported organisations, and informal networks external to Defence. These organisations recognise social support networks as crucial for well-being and adjustment.[12] Participants suggested support systems for families posted overseas were not always as easy to locate and often required perseverance to find something that worked for them. Two themes emerged as descriptors of the kinds of support mechanisms observed: informal support networks; and external support networks.

On arrival in their new host country, the prevalence of support networks varied. Some participants described being provided with formal support networks by their predecessor or other families in the location, or even by the very strong support networks that existed in the host nation military. This often included simple gestures such as filling the fridge and pantry with staples, escorting new families around their new community, introducing them to locals who were willing to provide support, helping with enrolments in schools, and setting up utilities and bank accounts. This kind of practical support was most effective in aiding their transition.

Higher-level support, such as that coming from the Australian Embassy or the Defence

Dr Narelle Biedermann, James Cook University

community back in Australia, was found to be less effective across all host nations when compared to the systems in place for Australian-based families. This was particularly the case in locations where there were no other Australian families. Several spouses described the burden of isolation and loneliness that comes with being away from the Australian accent.

> No formal support for us. Informal, half-assed handover from our predecessor who then left us to our own devices. I recall bawling when on day 10, I got a phone call from a lady at the Australian Embassy to touch base … they were happy tears just to have a conversation with someone with an Australian accent who understood how isolated I felt.

The search for informal support was described as being extremely important, particularly for a sense of companionship and support that comes with friendships. In some cases, it was more difficult to find informal support, especially among those who were childless or had young children who did not attend schools. Often, they had to actively seek out networks. Some joined quilt making clubs or family welfare clubs, or volunteered at a military charity store, finding support there. Others seized on the friendliness of neighbours and joined in neighbourhood activities. One spouse highlighted the significance of those informal networks in avoiding social isolation during her posting:

> I spent a lot of time by myself with two small kids. [My husband] went overseas a lot for work. I don't actually remember him being around a lot. I learnt to do everything myself and not expect help as I knew I wouldn't get any. Fortunately, I made great friends with my neighbour across the road and they became my family. Without them, I wouldn't have survived.

Theme 4: personality and resilience

Participants suggested resilience and a positive attitude are key personality traits that could have a significant impact on adjusting to life in an overseas posting. Resilient traits, such as optimism, have been found as key in enabling individuals and families to adapt to stressful events.[13] According to participants, it takes a certain kind of woman to be a military wife. Not everyone will be able to tolerate the demands,

uncertainties and constant changes that come with postings, absences and deployments.

Participants insisted that overseas postings are more complicated than a regular Australian-based posting and, as such, require a different attitude. There were numerous examples of resilience found in the data. Three themes emerged as descriptors of personality and resilience: preparation of self; approach to problems; and past experiences.

Among those who found their overseas posting enjoyable, there was a degree of preparation of themselves and their families. Some sought out language training so they could at least master some key phrases on arrival. Others studied the cultural nuances and sought out information that would make their transition smooth.

Before they even left Australia, most participants tried to establish a relationship with their predecessor to start asking questions and seeking advice on important issues such as schools, housing and health care. Having access to this type of information was instrumental in the transition of the family because it gave them a situational awareness of what to expect. All indicated they used the Internet to research the town they were going to, and to help establish some early networks with school and social communities.

Participants predominantly displayed a robust 'get on with it' attitude in their approach to the overseas posting and problems as they arose. Over the course of their lives as military spouses, most have learned to be incredibly self-sufficient and 'problem solve' rather than 'problem dwell', and generally approach postings with an inspiring efficiency and resilience:

> I still remember finding out about our posting - it was a huge week in our lives!! Basically, we found out we were expecting our first baby, a deployment, and the posting all in the same week! I had to do all the planning as I was on my own, and pregnant. It was tough, but very exciting all at the same time! We had our baby girl ([which coincided with] husband coming home on [deployment leave]). [Then] he went back to Iraq for 8 weeks, came home and a week later we packed up and moved overseas! How did I do it? I just did!

Past experiences aided participants immensely. There was a relationship between those participants who enjoyed the experience and those who had done a number of previous postings with their partner around Australia. Those women who were new to military life tended to have more negative perceptions of their posting experience and described more negative issues. With experience came wisdom and reason, because they had encountered stressors associated with numerous military postings before and knew that everything would fall into place in the end. Among those who found the experience positive, an optimistic attitude was evident in the way they described events and situations:

> I think the thing to note is that by accepting an overseas posting, you're agreeing to a bigger change than normal. I know when I post internally here in Australia what to do when I get sick, the parameters of seeing a dentist, what's required with a school enrolment. When we were overseas, there was so much information on top of the normal challenges that I understood I needed to be prepared for but not fully aware of the extent. So buying a car wasn't as easy as just buying a car. Getting a phone wasn't as easy as walking into a shop and buying a phone. Everything is harder, but you can't let it cripple you or you'd never go.

Discussion

In providing responses to many questions, participants indicated there was an explicit need for sacrifice in order for the family to survive and function 'normally' while supporting their spouse. Some sacrifices were made by the entire family: leaving pets behind, saying goodbye to family members (some of whom were elderly or ill and might not be alive by the end of the posting), and giving up freedoms and 'normal' life events such as sports or hobbies.

Other sacrifices were clearly made by the wife in support of her husband's posting and career. These sacrifices are often unacknowledged and unappreciated. Nonetheless, these participants were happy to make them. Those who were most at peace with their sacrifices were most likely to describe their posting as a highlight of their lives. In this way, their resilience is amplified by their acceptance of their sacrifice.

The participants were adamant that not everyone is able to make these sacrifices, or indeed live with the consequence of them once made. In their eyes, only those who are resilient enough to handle whatever is thrown at them will survive this lifestyle and the constant sense of loss that comes with frequent relocations and absences. One spouse acutely captured the overall sense of resilience:

> I married my husband accepting his career choices and all the ups and downs that come with it [like] me changing jobs, friends [and] houses every few years. It's just what you have to do. I have met many spouses who act as though the ADF shouldn't be allowed to tell them where to move, or why their husbands have duty on a certain day. They forget that it's all part and parcel of an important job.

Limitations and suggestions for further research

The picture provided by this research is incomplete. For example, the experiences of male spouses are absent, as no males volunteered to participate. This is a significantly smaller population within the ADF but their voices are still important. Additionally, the experience of spouses who have been posted to other international destinations where ADF members serve might have provided a more complete illustration of the experience for spouses.

To improve generalisability, researchers may wish to replicate the current study with a larger, more diverse sample that includes male spouses and a wider cross-section of posting locations (for example, Canada, Europe and New Zealand). Additionally, greater understanding could be gleaned by the inclusion of more spouses who endure a third-country deployment and the effect this has on their well-being.

Finally, this study did not explore the experiences of children who accompany their family on an overseas posting, and perhaps a study of these experiences may assist educators, health care professionals and Defence family and community organisations in understanding the unique needs of children before they are posted overseas and on their return to Australia.

Conclusion

The aim of this study was not to produce generalisable or quantifiable research findings. The meaning of the diverse experiences of spouses would not have been done justice through a reduction to quantifiable data. Rather, the aim of this study has been to provide insights and understanding of a unique phenomenon: to say, 'this is what it was like to have accompanied my military spouse on an overseas posting; to pack up my home and my family; to give up my job, my social and family support; and set up "home" in another country'.

The ADF maintains its own diverse cultural, demographic and personal constructs. The impact of these constructs extends beyond the serving member to their entire family. The current study reveals common themes that spouses who accompany their husband on a military overseas posting may experience. Most significantly, the relationship between the acceptance of sacrifices made for the good of their husband and their family, and resilience and adaptation is evident.

For military spouses, life leading up to and during an overseas posting presents a unique journey, and it is one that benefits greatly from supportive relationships, knowledge and preparation, and a willingness to do whatever it takes to lead their family through the journey. Given what we understand about the idiosyncratic challenges faced by military families, it is vital that those who work in community organisations that support the ADF and its members be culturally competent to meet the unique needs of these families during these times of transition.

Dr Narelle Biedermann served in the Royal Australian Army Medical Corps and the Royal Australian Army Nursing Corps between 1990 and 1998. She has published two books; the first, 'Tears on my pillow: Australian nurses in the Vietnam War', was based on her PhD dissertation, and the second, 'Modern military heroes: untold stories of courage and gallantry', has recently been republished.

Dr Biedermann was employed as an analyst at the Centre for Army Lessons, Land Warfare Development Centre, between 2006 and 2011. She holds a Bachelor of Nursing Science (Honours), Graduate Certificate of Nursing Science (Clinical Teaching), Master of Defence Studies, and a Doctor of Philosophy. She is currently employed as a Senior Lecturer, Academic Lead: Blended Learning, and Master of Nursing course convener at James Cook University, Townsville.

References

1 Sarah O. Meadows *et al*, *Family resilience in the military: definitions, models and policy*, RAND Corporation: Santa Monica, 2015; Catherine E. Runge, Michael Waller, Alison MacKenzie and Annabel C.L. McGuire, 'Spouses of military members; experiences and insights: qualitative analysis of responses to open-ended question in a survey of health and wellbeing', *PLoS ONE*, Vol. 10, No. 2, 2014, abstract available at <doi:10.1371/journal. pone.0118433> accessed 1 July 2017; Patricia Lester *et al*, 'The long war and parental combat deployment: effects on military children and at-home spouses', *Journal of the American Academy of Child Psychiatry*, Vol. 49, No. 4, 2010, pp. 310-20, abstract available at <doi:10.1016/j. jaac.2012.01.016> accessed 1 July 2017; Fawziyah A. Al-Turkeit and Jude U. Ohaeri, 'Post-traumatic stress disorder among wives of Kuwait veterans of the first Gulf War', *Journal of Anxiety Disorders*, Vol. 22, No. 1, 2008, pp. 18-31, abstract available at <doi:10.1016/j. janxdis.2007.01.011> accessed 1 July 2017.

2 William Saltzman *et al*, 'Mechanisms of risk and resilience in military families: theoretical and empirical basis of a family-focused resilience enhancement program', *Clinical Child and Family Psychology Review*, Vol. 14, No. 3, 2011, p. 213, abstract available at <doi: 10.1007/s10567-011-0096-1> accessed 1 July 2017.

3 Nansook Park, 'Military children and families: strengths and challenges during peace and war', *American Psychologist,* Vol. 66, No. 1, 2011, p. 65, abstract available at <doi:10.1037/a0021249> accessed 1 July 2017.

4 Tracy Eubanks, 'Life as a military spouse', *Urologic Nursing*, Vol. 33, No. 2, 2013, p. 97.

5 Gillian Blakely, Catherine Hennessy, Man Cheung Chung and Heather Skirton, 'A systematic review of the impact of foreign postings on accompanying spouses of military personnel', *Nursing and Health Sciences*, Vol. 14, 2012, p. 121, abstract available at <doi:10.1111 /j.1442-2018.2011.00659.x> accessed 1 July 2017.

6 Samantha Atkins, *A picture of Australian Defence Force families 2009: results from the first survey of Australian Defence Force families,* Directorate of Strategic Personnel Policy Research: Canberra, 2009; Annabel McGuire *et al, Timor-Leste family study: technical report.* Centre for Military and Veterans' Health, The University of Queensland: Brisbane, 2012; Runge, 'Spouses of military members'.

7 Manon Andres, *Behind family lines: a longitudinal study into family members' adaptations to military-induced separations*, International Sociological Association: Gothenburg, Sweden, 2010; H. Thomas de Burgh, Claire J. White, Nicola T. Fear and Amy C. Iversen, 'The impact of deployment to Iraq or Afghanistan on partners

and wives of military personnel', *International Review of Psychiatry*, Vol. 23, No. 2, 2010, p. 192, abstract available at <doi:10.3109/09540261.2011.560144> accessed 1 July 2017; Sara Green, Paula S. Nurius and Patricia Lester, 'Spouse psychological well-being: a keystone to military family health', *Journal of Human Behavior in the Social Environment*, Vol. 23, No. 6, 2013, p. 753, abstract available at <doi:10.1080/10911359.2013.795068> accessed 1 July 2017; Diane L. Padden, Rebecca A. Connors and Janice G. Agazio, 'Stress, coping, and well-being in military spouses during deployment separation', *Western Journal of Nursing Research,* Vol. 33, 2011, p. 247, abstract available at <doi:10.1177/0193945910371319> accessed 1 July 2017; Kendra N. Lowe *et al*, 'Impact of military deployments on family relationships', *Journal of Family Studies*, Vol. 18, No. 1, 2012, pp. 17-27; Tara L. Werner and Charlene S. Shannon, 'Doing more with less: women's leisure during their partners' military deployment', *Leisure Sciences*, Vol. 35, 2013, p. 63, abstract available at <doi:10.1080/01490400.2013.739897> accessed 1 July 2017.

8   Anita Chandra *et al*, 'Children on the homefront: the experience of children from military families', *Pediatrics*, Vol. 125, No. 1, 2010, p. 16, abstract available at doi:10.1542/peds.2009-1180 accessed 1 July 2017; Elizabeth A. Kaczmarek and Anne M. Sibbel, 'The psychosocial well-being of children from Australian military and fly-in/fly-out (FIFO) mining families', *Community, Work & Family,* Vol. 11, No. 3, 2008, p. 297, abstract available at <doi:10.1080/13668800801890129> accessed 1 July 2017; Lester, 'The long war and parental combat deployment', p. 316; Gail H. Manos, 'War and the military

family', *Journal of the American Academy of Child and Adolescent Psychiatry*, Vol. 49, No. 4, 2010, p. 297, abstract available at <doi:10.1016/j.jaac.2010.01.005> accessed 1 July 2017; Alexander C. McFarlane, 'Military deployment: the impact on children and family adjustment and the need for care', *Current Opinions in Psychiatry*, Vol. 22, 2009, p. 369, abstract available at <doi:10.1097/YCO.0b013e32832c9064> accessed 1 July 2017.

9   Gillian Blakely, Catherine Hennessy, Man Cheung Chung and Heather Skirton, 'Adaption and adjustment of military spouses to overseas postings: an online forum study', *Nursing and Health Sciences*, Vol. 16, 2014, p. 387, abstract available at <doi:10.1111/nhs.12122> accessed 1 July 2017.

10 Defence Community Organisation (DCO), 'About us', *DCO* [website], 2017, available at <http://www.defence.gov.au/DCO/About/Default.asp> accessed 17 February 2017.

11 Elizabeth H. Bradley, Leslie A. Curry and Kelly J. Devers, 'Qualitative data analysis for health services research: developing taxonomy, themes, and theory', *Health Services Research*, Vol. 42, No. 4, 2007, p. 1758, abstract available at <doi:10.1111/j.1475-6773.2006.00684.x> accessed 1 July 2017.

12 DCO, 'About us'.

13 Michael Ungar, 'Varied patterns of family resilience in challenging contexts', *Journal of Marital and Family Therapy*, Vol. 42, No. 1, 2015, p. 19, abstract available at <doi:10.1111/jmft.12124> accessed 1 July 2017.

Upping our game: near-future intelligence support within the 'disaggregated battlespace'

Captain Kevin Jolley, Australian Army

In recent decades, the civilian sector has surpassed the military in many areas of innovation and research. Once the domain of government-financed military agencies, an increasing proportion of innovation now derives from private 'tech giants' with the imagination and budget to drive the advancement of technology. The Internet has also facilitated greater technological awareness in the broader community, providing non-specialist users with unprecedented information on new technologies and emerging developments.

Notwithstanding their increasingly broad civilian development and application, the scope and rate of technological advances have and will continue to shape the conduct of modern military operations and improve their command and control, as well as the provision of logistics. This article offers an insight into how such developments will likely shape the future conduct of warfare within a 'disaggregated battlespace', which includes the trend of a 'gradualist approach' to

avoid triggering intervention, as well as the corresponding requirements of intelligence professionals.

The effect of long-range platforms/precision weapons

Recent advances in unmanned aerial vehicles (UAVs) have captured the imagination across both civil and military domains. The agile and cost-effective nature of UAVs makes their military application ideal, particularly for less wealthy nations and even non-state groups. Certainly, their employment in recent conflicts as a surveillance and reconnaissance tool, along with their ability to deliver precision kinetic effects, has done much to influence and shape those conflicts. It has also influenced and shaped the public's perception of modern warfare.

In the foreseeable future, UAVs could be used to attack key targets, including major naval

platforms, with 'swarms of multi-mission UAVs … [preceded by] waves of decoy drones, exhausting air-to-air and ship-to-air missiles'.[1] 'Swarming' is a military threat that challenges missile-defence orthodoxy, with no obvious counter-technology at present. UAVs also offer the ability to economically deliver precision effects at a much lower risk than manned aircraft. Furthermore, UAVs offer a potential force-projection capability, a key requirement in the increasingly technological battlespace where militaries typically seek to create distance between the battlespace and their key national interests.

There has also been rapid development in the evolvement of precision stand-off weapons that complement force projection. Ground-based, air-to-ground and naval long-range missiles pose an escalating threat. During a recent joint exercise, the US aircraft carrier group within the scenario was essentially held hostage by the fictitious threat posed by a long-range, shore-based anti-ship missile system.[2] The threat severely degraded the aircraft carrier group's influence during the conduct of the joint combat scenario, demonstrating the asymmetrical impact that a relatively low-cost, long-range weapon could have on the most expensive and capable military equipment in the world.

In a recent article on the future battlefield, US Army Chief of Staff General Mark Milley was cited as saying that 'land-based forces … [would] have to penetrate denied areas to facilitate air and naval forces'.[3] Milley envisaged an anti-access/area-denial (A2/AD) zone with ground forces facing everything from 'rifles and tanks to electronic jammers, computer viruses, and long-range missiles striking targets on the land, in the air and even at sea'. US Department of Defense Deputy Secretary Bob Work has similarly referred to the 'spread of long-range precision missiles, linked by wireless networks to long-range sensors—such as drones and satellites—that provide targeting data'.[4] This appreciation of long-range force projection is addressed in the US Army's latest warfighting concept, known as the Multi-Domain Battle, where battle will be contested not just in air, sea and land domains but also in the informational and cyber realms.[5]

The 'disaggregated battlespace'

The rapid evolution of technology will arguably influence three key areas in the future conduct of warfare: logistics, command, and communications. Milley has warned that we 'are on the cusp of a fundamental change in the character of ground warfare'. Identifying the increasing threat of precision long-range weapons, he contends that units will not be able to remain static for long periods of time, asserting that 'if you stay in one place longer than two or three hours, you will be dead'.[6]

An adversary's logistics chain has always been a highly desirable target. In future, logistics within the battlespace will need to become more internalised, utilising technology to maintain combat power, while traditional logistic systems will need to be hardened and made more resilient to survive precision weapons aimed at fuel supplies and lines of communication.

Technological solutions could include combat units fabricating spare parts using 3D printing, and purifying their own drinking water, to remove the need for echelon support.[7] Further internalisation could include 3D printing of food and ammunition, and using solar power and electrical technology to reduce the dependency on liquid fossil fuels. Unmanned aerial, ground and submersible systems could also provide a much less targetable method of resupply, in almost all terrain and weather conditions, by reducing the risk of interdiction through precision targeting.

The conduct of operations will also change significantly as units become semi-autonomous through disaggregation to ensure survival and mission success. Commanders will need to remain fluid with their actions as the pace of the battlespace changes. Long planning sessions will need to be replaced by quicker decision cycles, not least because forces with slow response times will be particularly vulnerable to targeting by precision weapons.

The technological threat posed by advanced electronic warfare means that units will increasingly become regularly isolated, in communication terms, from peer and commanding units.[8] As such, 'actions on' will need to evolve from reliance on tactics, techniques and procedures

(TTPs) to carefully considered plans based on an appreciation of multiple scenarios or eventualities. Instead of planning for immediate and subsequent objectives, tactical and operational commanders will need to provide greater mission command and, like a game of chess, allow for the planning of three or four actions ahead to negate disruptions from electronic attack. The character of warfare will become more rapid and chaotic in 'disaggregated warfare', with initiative and adaptability more important than ever.

At the same time, the evolution of battlefield communications offers to provide greater awareness and control than ever before. The prevalence of private communications networks and satellite coverage rivals and surpasses military assets in many areas. Threat groups can utilise encrypted messaging services on private devices connected to civilian networks to instantly notify peers and superiors of friendly troop movements, locations and dispositions. Contemporary violent extremist organisations have migrated to encrypted communications that are extremely difficult, if not impossible, to interdict.

The majority of the world's population possesses hand-held devices that can provide voice, video and data links across most populated and rural areas. This plethora of sensors offers an enormous advantage in understanding the battlespace, as well as enabling those who are willing to take advantage of it. These technologies potentially offer the ability for Australian forces to communicate far more easily and effectively than with the current military communications systems. Hence, consideration should be given to enabling Australian soldiers with handheld devices (either their own or issued) to provide instant C2 in areas where civilian networks are available. This is a key area where the military has been slow to utilise the exceedingly efficient and capable technologies available within the private sector.

The 'gradualist approach'

The conduct of warfare evolves continuously, with occasional disruption and occasional periods of rapid development. Over the last few decades, a new trend has emerged. 'Gradualism' has long been associated as a political and

social extension of a particular ideology, much like Islamism seeks to convert the world's population to Islam through a graduated approach. However, some major powers have recently been using a far more sinuous and graduated approach in pursuit of geopolitical objectives, in stark contrast to the US invasions during the Gulf Wars. The Russian invasion and annexation of Crimea in early 2014 was achieved with relatively little resistance through a graduated approach using a combination of a proxy insurgent force complemented by special and conventional forces to seize and hold the peninsula.

Key to this were the political and social claims of traditional ownership and the gradual approach to supporting anti-government forces in Ukraine, as well as masking the tactical insertion of Russian troops through effective information operations. This non-linear combination of conventional and unconventional elements has been referred to as the 'Gerasimov doctrine', emanating from General Gerasimov, current Chief of the Russian General Staff.[9] In this manner, Russia was able to invade and subsume a sovereign state's territory, achieving both tactical and strategic surprise while avoiding interruption by the international community through effective deception and inherent deterrence.

This is similar to China's gradualist infiltration into the South China Sea. The Chinese approach is supported by claims to traditional ownership, with China's so-called 'nine-dash line' providing the social and political justification for its actions. In doing so, the Chinese have usurped the territorial and maritime-related resource claims of a number of other states. As a result, China now has multiple runways in the region capable of supporting military aircraft, anti-aircraft installations, regular marine patrols and stationed military personnel. The use of a gradualist approach over some decades has enabled the Chinese to force project far into the South China Sea. Both the Russian and Chinese campaigns have been supported by highly effective psychological operations, clouding the figurative waters through claims of traditional ownership and numbing the effect of military force projection through gradual force build-up.

In terms of non-conventional threats, Islamic State has certainly adopted the disaggregated battlespace approach. Its calling for

home-grown extremists to wage war in their own countries is well known. It has empowered its followers through the provision of guidance and information, enabling initiative and adaptability to replace consistent and supportive direction. Combating this is quite difficult, as the problem is manifested in an extreme ideology rather than a specific organisation or state. This is another feature of near-future warfare, with extreme ideologies adopting disaggregated approaches to stretch security services, either in pursuit of their own ideals or as proxy for a sovereign state.

What this means for intelligence professionals

The above elements are representative of the changing face of warfare and the future of conflict within the next 20 years. For intelligence professionals, a number of critical changes must be implemented to ensure relevance is maintained. Intelligence-driven operations will continue to be the most effective approach, as reactive operations will cede initiative to an adversary. Timeliness will become the most critical principle. As the pace of change quickens, so too the decision cycle and the intelligence that supports it. Dissemination methods, too often neglected or forgotten in the rush to produce fully synchronised collection plans and reports, will become critical. Intelligence not available to a commander and combatant is at risk of being irrelevant.

Dissemination becomes key

For dissemination, timeliness has always been the critical factor. Methods of delivery must become shorter. Formations and units will no longer have the time to listen to lengthy intelligence briefs. Intelligence officers should give thought to producing short podcasts of information; small reports that can be messaged through encrypted messaging services, and short videos that provide intelligence briefs complete with supporting terrain pictures, threat TTP clips and geospatial imagery.

With such an approach, a soldier on the ground can receive the same intelligence briefing as the divisional commander. All aspects within the intelligence cycle should be reviewed for efficiencies, while maintaining the integrity of analytical processes. Absorption of the product within minimal timeframes to the widest audience possible must be considered a key tenet. Consideration should also be given to the new manner of absorption by short bursts of information or video feed—which is what we are growing accustomed to every day through social media use.

Aggregation and 'big data'

Atmospherics will become increasingly useful and critical to gaining an understanding of the battlespace and its current fluidity. Aggregation of the enormous amounts of 'big data' will enable analysts to conduct better trend analysis than ever before. This term is used by many but with little understanding of what constitutes 'big data' and its rather large management requirements.

The data basing of such information is critical, one that is available to the joint environment and able to be accessed through various battlefield management systems. The removal of tactical and operational barriers to intelligence transfer will serve to create greater economy of effort among the joint and special operations analysts. The focus of these efforts will shift to supporting precision weapons, both in the friendly targeting cycle and in the likely capabilities of threat weapons. Commanders will quickly need to know where long-range weapons can affect them, and whether their long-range weapons can achieve a similar effect. Allocating priority and relevance tagging to data will be critical.

As warfare fluidity increases and commanders begin to consider third- and fourth-line objectives as a matter of course, intelligence officers must support this hypothetical planning. Wargaming must become a far more critical component of the planning process—and less about intelligence and operations officers competing to outdo each other with threat capability recall. The scope of possible threat reactions will become more relevant, to provide greater insight to branch planning. Simulations can provide a highly efficient manner to test threat reactions, and are an effective technological solution to support a higher pace.

Captain Kevin Jolley, Australian Army

Information effects more relevant than ever

The disaggregation of the battle space provides both threat and opportunity. The threat will recognise the ability of friendly elements to force project with precision, and will take steps to mitigate accordingly. This will require a fundamental shift in the targeting approach by intelligence professionals. Clausewitz's model discusses a force's freedom of action, strength and will to fight as derivatives of its centre of gravity.[10]

However, in a disaggregated battlespace where identifying a unit and its strength (deployed capabilities) may become far more difficult—and stand-off distances render aspects of terrain less useful—perhaps the only option will be to focus on undermining an adversary's will to fight. If traditional operations cannot be conducted because of stand-off distances caused by long-range weapons, then comprehensive information actions can continue to target the enemy. The adversary's psyche will become the new high-value target.

Empowering decision-makers

High-level political decisions will need to be supported with operational and tactical intelligence. The growing tendency of large powers to use a form of gradualism to achieve their objectives means that historical 'triggers' or 'red lines' become blurred. A key example of this lack of red line action was the Obama Administration's response to the Assad regime's use of chemical weapons in Syria in 2012. Intelligence professionals must identify and report the signs of gradualism, using tactical and operational sources, to achieve strategic understanding and subsequent action.

Finally, intelligence professionals must be prepared to adapt existing analytical frameworks in response to changing threats. Doctrine must not become a refuge of the unimaginative. An extremist ideology cannot be analysed using the current intelligence preparation framework. Due consideration should be given to understand the full spectrum of the problem, including the underlying ideology and supporting aspects such as narcotics and global arms trades. This will allow for a comprehensive analysis, and continue to provide awareness and warning for commanders.

Conclusion

The purpose of this article has been to provide an appreciation of the changing style and advancement of warfare over the next 20 years. Key to this is the technological advancement of the private sector and the flow-on effects for military application. The battlespace will become faster and more fluid, with long-range precision changing the fundamentals of tactical and operational manoeuvre. Mobility will be the key to survival and, in turn, the enemy will become increasingly harder to undermine. Information operations will become more important than ever as a means of continuously targeting the threat.

Furthermore, the style of warfare is changing, with states opting to adopt a gradualist approach to avoid triggering third-party intervention. Extremist ideologies are seizing technology to disaggregate their struggle, and overwhelm and stretch security services. For intelligence professionals, keeping up with decreasing decision cycles will be critical to maintain intelligence-driven operations. Our own methods must change to meet these challenges, to ensure that we continue to provide timely and appropriate advice to Australian commanders.

Captain Kevin Jolley graduated from the Australian Defence Force Academy in 2009, and the Royal Military College, Duntroon in 2010. He completed two tours of Afghanistan in 2013 and 2014. He is currently posted to the 1st Intelligence Battalion.

References

1 J. Lehner, 'Rise of the machines: the inevitable vanguard of Australian military operations', *Bridges Review* (internal to Defence), 2015.

2 H. Kazianis, 'Is China's "carrier killer" really a threat to the US Navy?', available at <https://www.youtube.com/watch?v=wDxghSKerkw> accessed 3 May 2017.

3 Cited in S.J. Freedberg, 'Miserable, disobedient & victorious: Gen Milley's future US soldier', *Breaking Defense* [website], 5 October 2016, available at <http://breakingdefense.com/2016/10/miserable-disobedient-victorious-gen-milleys-future-us-soldier/> accessed 3 May 2017.

4 Cited in Freedberg, 'Miserable, disobedient & victorious'.

5 US Defense News, 'New Multi-Domain Battle concept to drive change in Army's future', *Defense News* [website], undated, available at <http://defensenews-alert.blogspot.com.au/2016/10/new-multi-domain-battle-concept-to.html> accessed 3 May 2017.

6 Cited in Freedberg, 'Miserable, disobedient & victorious'.

7 Freedberg, 'Miserable, disobedient & victorious'.

8 Freedberg, 'Miserable, disobedient & victorious'.

9 V.R. Morris, 'Grading Gerasimov: evaluating Russian nonlinear war through modern Chinese doctrine', *Small Wars Journal*, 17 September 2015, available at <http://smallwarsjournal.com/jrnl/art/grading-gerasimov-evaluating-russian-nonlinear-war-through-modern-chinese-doctrine> accessed 3 May 2017.

10 M. Evans, 'Centre of gravity analysis in joint military planning and design: implications and recommendations for the ADF', *Security Challenges*, Vol. 8, No. 2, 2012, p. 81, available at <https://www.regionalsecurity.org.au/Resources/Files/vol8no2Evans.pdf> accessed 3 May 2017.

Debiasing the military appreciation process

Dr Jim Sheffield, Victoria University of Wellington
Colonel Roger Margetts, ONZM, New Zealand Army
Lieutenant Colonel Gordon Milward, ONZM, New Zealand Army

> It ain't what you don't know that gets you into trouble. It's what you know for sure that just ain't so! (attributed, perhaps incorrectly, to Mark Twain)

Prior to the Iraq War, the Chairman of the US Joint Chiefs of Staff, Colin Powell, received advice about 'weapons of mass destruction' that turned out to be incorrect. He subsequently formulated three rules for his intelligence staff:

> Tell me what you know. Tell me what you don't know. And then, based on what you really know and what you really don't know, tell me what you think is most likely to happen. (Powell, 2004)

Each of the rules encapsulates a distinct perspective or mode of thinking. In particular, the first two rules capture Mark Twain's observation that what we know may not be so. Confidence in what we know comes fast and easy but must be balanced by the slow and difficult search for gaps in knowledge. The bias to confirm what we already know is strong. Even the

hint of disconfirming evidence may cause negative emotion and 'loss aversion'. Group norms may favour conformity over creative and critical thinking. A bias for information quantity may create complexity that obscures lack of information quality and the need for action.

In their article titled 'Thinking more rationally: cognitive biases and the joint military appreciation process', published in this *Journal* in 2015, Nigel Dobson-Keeffe and Warren Coaker asserted that '[t]here is little evidence that the Joint Military Appreciation Process (JMAP), as used by the ADF, considers the effects of these cognitive biases, despite their potential to affect operational decisions'. The authors then examined the JMAP to determine its vulnerability to bias, identifying *what* biases are important, and *where* they may have greatest impact.

However, we believe that complexity is a common reason why military decision-makers are unaware of the processes by which they make sense of the world, their own capabilities and

desires, and the interaction between them. We have focused, therefore, not on cognitive error as a deviation from a single, normatively correct response but on the confusions inherent in military decision-making. We collaborated with senior staff in the New Zealand Army to reflect critically on *why* the military appreciation process is important, and *how* it may be improved by a 'de-biasing' program.

Literature review

System 1 and system 2 thinking

The Military Appreciation Process (MAP) employed by the New Zealand Army is a structured decision-making process for operational planning primarily by individuals (where 'groupthink' bias may not be important). It is not dissimilar to the JMAP and other operational planning processes used by allied nations. Hoskin (2009) argues that the JMAP is generally very effective but could be improved by the better application of human factors, such as the personal role of

the commander, intuition and creativity. In a similar vein, Smith (2011) argues that operational art and strategy are dynamic and contingent practices, and that expertise in the face of ambiguity requires an adaptive mental stance or cognitive dual-process capability.

Bloxam (2012) asserts that 'in the last few decades there has been a gradual synthesis of the literature towards a dual-process model of cognition which is simple, but not simplistic, elegant and also very accessible'. While the terminology and application domains vary, there is consensus on the core concepts (see, for example, Evans, 2008; Kahneman, 2011). Evans & Stanovich (2013) state that:

> Our preferred theoretical approach is one in which rapid autonomous processes (Type 1) are assumed to yield default responses unless intervened on by distinctive higher order reasoning processes (Type 2). What defines the difference is that Type 2 processing supports hypothetical thinking and loads heavily on working memory.

These characteristics are illustrated at Table 1.

Property	System 1 thinking	System 2 thinking
Action	Reflexive, skilled	Deliberate, rule-based
Automaticity	High	Low
Awareness	Low	High
Context important	High	Low
Cost	Low	High
Effort	Minimal	Considerable
Errors	Common	Few
Hard-wired	Maybe	No
Predictive power	Low	High
Reasoning style	Intuitive Heuristic Associative Concrete	Analytical Normative Deductive Abstract
Reliability	Low, variable	High, consistent
Scientific rigour	Low	High
Speed	Fast	Slow
Vulnerability to bias	Yes	Less so
Working memory	Not involved	Involved

Table 1: Characteristics of system 1 and system 2 thinking (adapted from Bloxham, 2012)
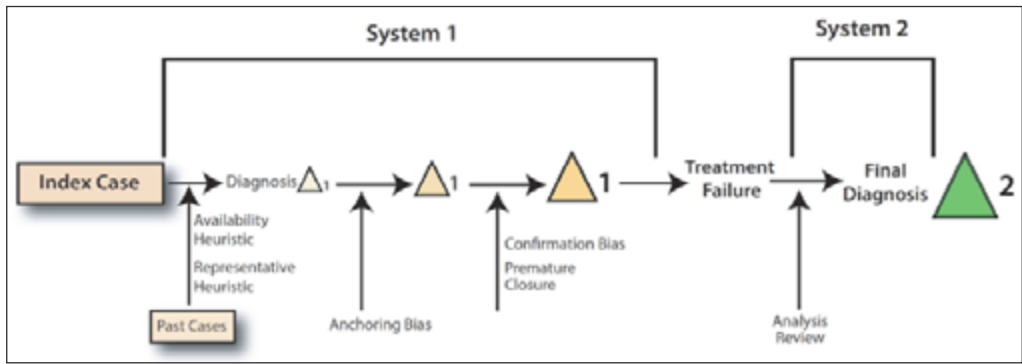
Figure 1: A common clinical sequence of events (source: Bloxham, 2012)

Health

A key application domain of the cognitive dual-process model is health. Bloxham (2012) describes:

> A common clinical sequence of events whereby the index case has an initial wrong diagnosis induced by its similarity to a more common or recently seen condition (availability heuristic), and which also appears to be a typical example of its class (representative heuristic). This initial diagnosis is then reinforced by several other well established heuristics (anchoring bias, confirmation bias and premature closure) which can all be contained under the scope of System 1. Treatment failure then forces a switch to System 2, which is more analytical in nature and may include the formal consideration of the combined probabilities of the various individual signs, symptoms and investigations pertaining to the case [as outlined at Figure 1].

Bloxham (2012) observes that both system 1 and system 2 thinking play an essential role in rational decision-making and that attention should be focused on the triggers or stimuli in the internal or external environment that promote or inhibit these two systems (Figure 2 and Table 2 refer).

Croskerry (2009) observes that the dual-process theory supports simplified models that can be readily taught to learners across a wide range of disciplines. In particular, he contends that

> An understanding of the model allows for more focused *metacognition*, that is, the decision maker can identify which system they are

currently using and determine the appropriateness and the relative benefits of remaining in that mode versus switching to the other.
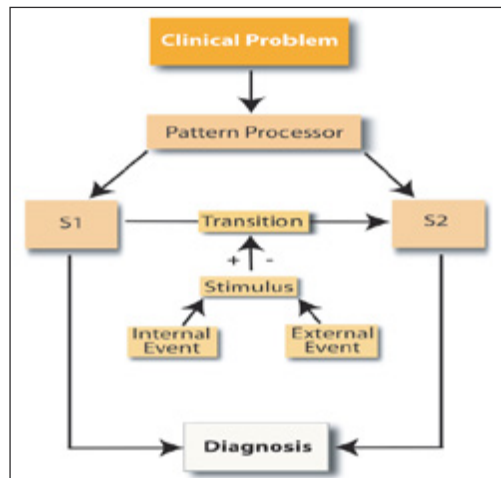
Figure 2. Algorithm for possible pathways between clinical problem and diagnosis (source: Bloxham, 2012)

Lambe, O'Reilly, Kelly & Curristan (2016) conducted a systematic survey of dual-process cognitive interventions to enhance diagnostic reasoning of medical trainees and doctors. While many of the studies found some effect of interventions, guided reflection interventions emerged as the most consistently successful. It was also concluded that cognitive forcing strategies improved accuracy and confidence judgments.

	Positive	Negative
Internal events	Cognitive expertise Experience Simulation practice Statistical training Personality	Stress Poor health Fatigue Personality
External events	Situation awareness 3rd party action 2nd options Ambient conditions Conflicting data	Distractions Workload Ambient conditions

Table 2: Transition stimuli (adapted from Bloxham, 2012)

Military

A second key application domain of the cognitive dual-process model is the military. All military decision-making articles addressed, implicitly or explicitly, fast (system 1) and slow (system 2) thinking, and the importance of the transition between them (see, for example, Rolison, Evans, Dennis & Walsh, 2012). Aspects of the MAP aligned with system 1 are illustrated in Table 3.

1. Ill-defined goals and ill-structured tasks

2. Uncertainty, ambiguity, and missing data

3. Shifting and competing goals

4. Dynamic and continually changing conditions

5. Action-feedback loops (real-time reactions to changed conditions)

6. Time stress

7. High stakes

8. Multiple players

9. Organisational goals and norms

10. Experienced decision makers

Table 3: Aspects of the MAP aligned with system 1 thinking (source: Klein & Klinger, 1991)

Neuroscience is providing empirical evidence for the biology associated with the dual-process model, demonstrated in first-person accounts of combat experiences (Sheffield & Margetts, 2016). In debiasing, guided reflection about visceral experiences, and about emotions such as fear, would appear particularly useful.

In the Rand Corporation's Project Airforce, Davis, Kulick & Egner (2005) recommended that '[d]ecision support should appeal to both the rational-analytic and the intuitive capabilities of the decisionmaker'. The authors contrasted the logic of storytelling (reduced conceptual uncertainty) and the logic of statistics (reduced empirical uncertainty), and stated that 'the particular balance should depend on characteristics of the decision, the decision environment, and the decisionmaker'. The confirmation bias was a key barrier in moving from system 1 to system 2 thinking, with Cook & Smallman (2008) concluding that:

> Domain experts exhibited confirmation bias in a realistic intelligence analysis task and apparently conflated evidence supportiveness with importance. Graphical evidence layout promoted more balanced and less biased evidence selection.

Wickens et al. (2010) found that when integrating intelligence information, anchoring on old (and less relevant) information sources (cues) was reduced by simple instructions to pay more attention to recent (more reliable) cues. Herdener

et al. (2016) found that when operators made trajectory predictions from graphical displays, they were able to update incorrect anchors (means) but were very poor at processing statistical information about uncertainty (variance).

In a report entitled 'Training critical thinking for the battlefield', Cohen et al. (2000) state that '[a] very short period of training has been consistently found to significantly affect both … variables related to critical thinking processes and … participants' decisions in a military scenario'. Morewedge et al. (2015) report that a single training intervention with an instructional video or game produced large and persistent reductions in decision bias. Games which provided personalised feedback and practice produced larger effects than videos.

Models of the JMAP and MAP

The Dobson-Keeffe & Coaker (2015) representation of the inter-operable JMAP highlights that biases in collecting information (information, availability, pattern recognition) are important in three clusters of steps (labelled analysing data, deciding and acting). All four processes are marked by time pressures and conceptual uncertainty, so that cognitive processing is primarily experiential (Klein & Klinger, 1991; Slovic

et al., 2004) or System 1 (Bloxham, 2012). The model makes predictions about which cluster (as opposed to which step) each bias will impact the most (Figure 3).

The current research builds on similarities between the battlespace intelligence operations of the ADF's inter-operable JMAP and the New Zealand Army's MAP. The Dobson-Keeffe & Coaker (2015) allocation of biases to the clusters of steps in the JMAP serves as a reference model, or initial best-practice theoretical model, in allocating biases to the clusters of steps in the MAP.

Our representation of the MAP highlights that biases in analysing information (confirmation, my side, illusory correlation, over-confidence) are important in three clusters of steps (labelled problem definition, design, and implementation). As the MAP is primarily viewed as an individual process, we have chosen to drop from our analysis the group-think bias. To sharpen the analysis, we have made predictions about which step (as opposed to which cluster of steps) each bias will impact the most. We envision a training program in which cognitive biases studied in the context of process flows serve as the occasion for possible transition between system 1 and system 2 (Figure 4).
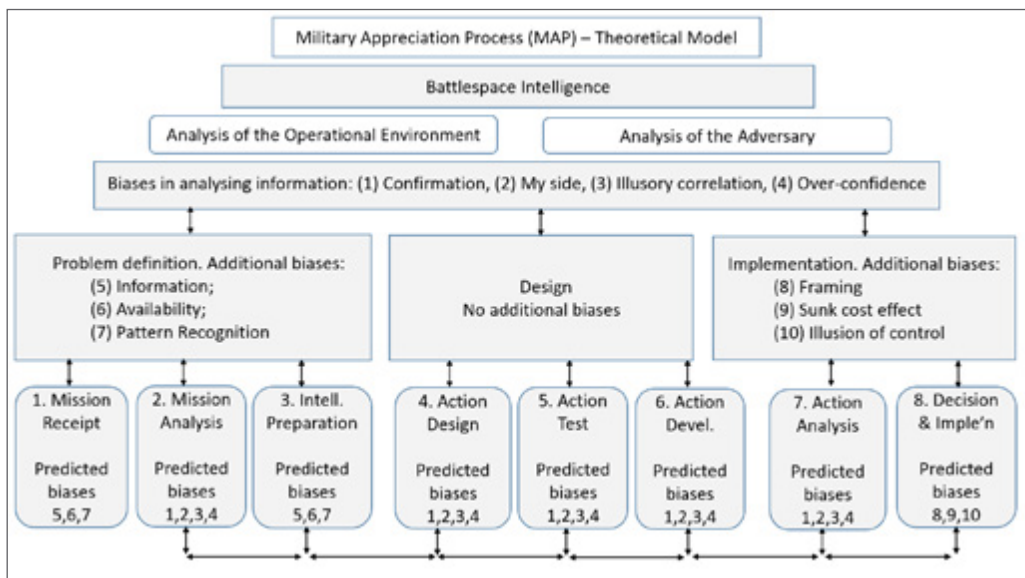

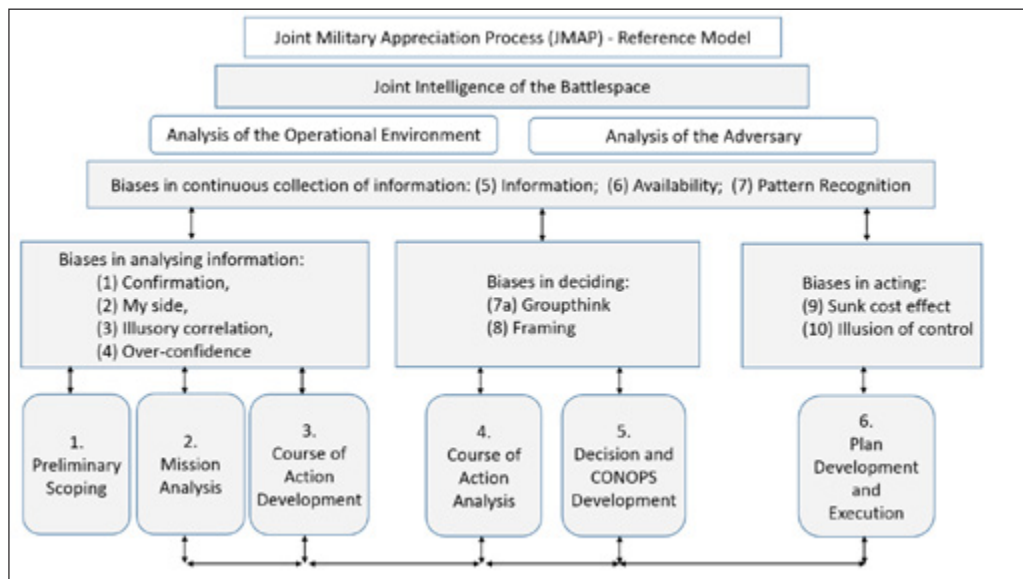Figure 3: JMAP reference model (adapted from Dobson-Keeffe & Coaker, 2015)

Figure 4: MAP theoretical model

Summary

In summary, the need for an appropriate balance between fast (system 1) and slow (system 2) thinking plays an important integrating role in the current behavioural decision-making literature. We reviewed applications and training programs in health and the military. Guided reflection, educational interventions, checklists, and cognitive forcing strategies were important tools. A single training intervention with an instructional game or video produced large and persistent reductions in decision bias.

A process model of the MAP was developed and predictions made about the biases important to each step. We argue that a training program focused on decision processes with embedded 'metacognitive moments' that serve as the occasion for possible transitions between system 1 and system 2 will enable more rational thinking in the New Zealand Army.

Methodology

The empirical research focuses on gaps between participant narratives and explores how a convergence of meaning can be fostered through a training program. Empirical data was gathered from an in-depth, qualitative case study of training for battlespace intelligence. Our informants (senior staff in the New Zealand Army) participated in a three-step research process (interviews, card sort and checklist).

Interviews

Semi-structured interviews guided the participants' critical reflections on the purpose of the MAP, and its strengths and weaknesses, and how it could be improved (Margetts, 2016a).

Card sort

A card-sort exercise and a 'talk aloud' protocol guided reflection on bias, and the likely impact on the eight steps in the MAP (Figure 5). Each bias in the Dobson-Keeffe & Coaker (2015) study was placed on an index card, with name and description on one side, and military application on the other. Observations were noted about the participants' verbalisations, and their deliberations as they assigned biases to the steps. A bias could be allocated to more than one step, and not all biases had to be allocated. During this process, participants were encouraged to 'think aloud' about their experiences.

The allocation of biases to steps of the MAP was analysed against the criteria in three reference models:

1. The *theoretical model* created by transferring allocations to steps in the JMAP (Figure 3) to the steps in the MAP that arguably had a similar function (Figure 4).

2. An *empirical model* based on consensus on card-sort allocations.

3. A *best-fit model* based on an opportunistic choice of either the empirical or theoretical models.

For each model, patterns of participant bias assignments were analysed via 11 parameters of fit at four levels (including step and cluster) of abstraction.

Results

Interviews

Nine participants were involved in the interviews and card-sort activity, all with substantial military experience, to ensure they reflected the beliefs and opinions of individuals well qualified to understand and use the MAP. They also included a 'key informant', who had been central in the development of the MAP.

Why the MAP is important

> The purpose of the MAP is to assist individuals in groups to plan and make decisions in a variety of demanding situations ranging from simple to complex, low stress to high stress and non-conflict right through to high-end conflict. It achieves this by aiding commanders and staff to think through what may happen and thereby be better prepared to effectively mitigate risks or exploit opportunities as they occur. The MAP is kind of doing two things; it's assisting planning before execution and then assisting decision making during the execution of the plan. Whether the critical situation is time sensitive or not, whether it's simple or complex, or whether you feel your life is threatened or not, it's a tool with great utility. (key informant)

A strong theme was that the MAP 'provides structure to the decision-making process' and 'breaks down complexity'. Positive comments such as 'a method of interpreting complexity' and 'making sense of all the complexity' recurred consistently. Negative comments included 'leads people down rabbit holes' and

'not packaged user friendly'. Such respondents expressed reservations over the 'time compression issues' and preferences for 'simpler tools'.

Overall, the usefulness of the MAP in managing complexity in critical situations was assessed at 4 on a 5-point scale (1=not at all useful; 5=extremely useful).

Strengths and weaknesses of the MAP

> In the military context, we are often faced with a complex and dynamic situation that ideally requires slow thinking to solve, but in reality we have to react to using fast thinking. In these circumstances the MAP is very good at focusing a Commander and staff on determining when a decision has to be made by, and what type of planning approach is to be used. The MAP enables you to balance in the time available, the use of slow thinking analysis and fast thinking intuition. If you've got plenty of time you can run the full deliberate process and weight analysis over intuition—thereby avoiding the pit fall of using bias prone fast thinking to solve complex problems when you don't have to. This exposes a potential weakness in military culture—because we are so used to using short term fast thinking in conflict situations we may tend to automatically apply this style of decision making to all situations. (key informant)

An emergent theme around weaknesses was seen in comments such as 'at worst is inflexible and less responsive' and 'not supportive of quick, instinctive decision making'. It seems the deliberate nature of the process and the discipline it provides is also a drawback as it 'limits divergent thinking'. Another theme centered on the frustration shared by students and instructors, such as it is 'hard to teach—overwhelming for them and how to get into the detail they don't understand'.

Common and recurring problems

> It takes about six weeks for experienced military people to get up to speed on the process and then be able to intelligently focus on the situation. Learning or rather absorbing military culture, jargon and the lessons from operational experience is a socialisation process that you can't speed up and takes between two to four years, in my opinion.

I think there's a real danger of reinforcing only fast thinking as our default planning and decision making style. I think initially when you're learning the process we need to take the time-sensitivity out so that people have the opportunity to practise slow thinking. There's a real tension here, under pressure people just whip out the first answer that comes to mind which makes people even more prone to their bias. We could be inadvertently conditioning our officers to being decisive, unimaginative and bias prone decision-makers. (key informant)

For those new to the Army, the MAP is confounding as seen in the comment that 'the new and inexperienced face a military culture … [and] a language they don't understand'. Others capture a theme whereby the MAP 'requires significant practice to master', and again with the comment that 'complexity and no prior experience [can] only be remedied by repetition of use'.

Goals for the training program

When using the MAP as an individual, challenging yourself to be a little bit creative in each of those steps that I talked about, and being aware of your own bias, is critical. Having some sort of mini process to be creative and avoiding being prone to bias, or whatever your frame of reference is, will be helpful.

At those points we should use some sort of tool or process that prompts us to think outside the box and avoid our instinctive and normal way of viewing things. That would help offset the danger of bias and lack of creativity. The key points of the MAP process that challenge your thinking become even more critical. So a smart checklist that mitigated bias at those critical points in the MAP that required assumptions and/or deductive reasoning would be very useful. (key informant)

A strong theme was that a checklist would promote a common awareness among instructors and junior officers of the impact of bias: '[a checklist would be] incredibly helpful [given we are] prone to bias, especially in initial use of the MAP'. Participants saw it as 'definitely beneficial as an instructor' as it gave 'instructors [their] own understanding of bias'. A checklist was good 'both ways—good for the student and instructors'. Overall, the usefulness of a debiasing checklist was assessed at 4.3 on a 5-point scale.

Interestingly, after experiencing the card-sort activity, some participants revised their rating upwards. No-one scored the checklist lower than 4. It appears that the card sort served to guide reflection and increase the flow of comments. A checklist would provide a focus when debriefing or correcting student performance. Also '[I'm a] big fan of that and good way to operate' as it allows students to 'look, think and act'. This appears to recognise that instructors and students would be able to share a common description and presentation of a bias, where it was likely to occur, and how to address it systematically.

Summary

Participants valued the MAP as a tool for managing complexity in critical situations. While it served many useful purposes, major issues remained, including irreducible complexity, insufficient training, the need for creativity, and a culture of time compression. There was 'real danger of reinforcing only fast thinking as our default planning and decision making style'. Participants strongly believed that a debiasing checklist would address outstanding issues, reduce the impact of time compression, and promote balanced thinking. Participants strongly believed that a checklist and related debiasing procedures held positive benefit.

Card sort

Some indicative results of the card sort are presented in Figure 5. At the overall or MAP level, 182 assignments were made, with 81 assignments to the problem definition cluster, 59 to the design cluster, and 42 to the implementation cluster.

Some steps attracted more biases than others. For example, step 3 attracted 48 assignments, and the consensus was that biases 1, 2, 6, 7, and 10 (listed in Figure 5) were important. In contrast, step 1 attracted 7 assignments and there was a consensus that only bias 5 was important. The consensus allocation of biases differed in interesting ways from the reference model. For example, the consensus that biases 1, 2, and 10 have greatest impact at step 3 is at odds with the theoretical model, which requires that bias 1 and 2 be assigned to step 2, and bias 10 be assigned to step 8.
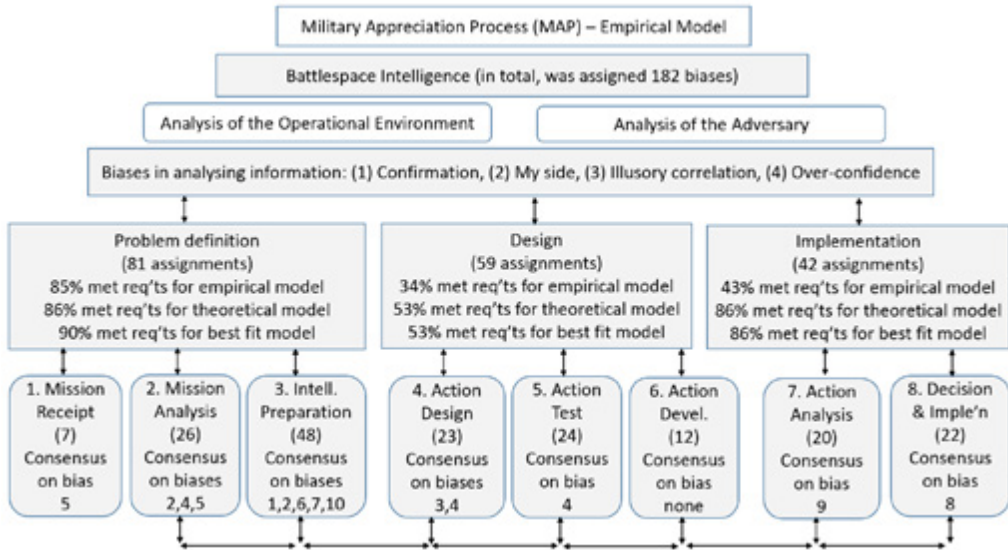
Figure 5: MAP empirical model (based on results of card sort)

Checklist

A debiasing checklist based on a cluster level analysis was developed as part of a 32-page curriculum pack. It was presented to the training staff and senior lecturers responsible for training the 2017 cohort of 30-40 junior officers. The training program, which included experiential exercises in metacognition and focused on guided reflection, was well received. The instructors also reported that teaching debiasing provided for their own reflection on the MAP, and the biases important to each step.

Summary

Empirical research employed a three-step methodology. Interpretive interviews with key decision-makers revealed that divergent beliefs existed and were associated with differing responses to time compression. Participation in a card-sort exercise induced MAP instructors and a key informant to believe that debiasing process flows would alleviate some of the frustrations occasioned by time compression.

Discussion

Two narratives were central to the interviews with participants, namely that 'we could be inadvertently conditioning our officers to being decisive, unimaginative and bias prone decision-makers'; and that 'a checklist would be good both for the students and instructors'. Participants strongly believed that a debiasing program would improve the MAP by mitigating the impact of time compression, and enabling a more appropriate balance of system 1 and system 2 thinking.

In the card sort, instructors' cognitive explorations of the MAP were guided by multiple models, parameters, and levels of abstraction. The result was an empirical consensus allocation of biases that differed in interesting ways from the predictions of the theoretical model, indicating that further insights and accommodations are possible. Do the theoretical and empirical models identify real differences? Do our predictions at which step a bias is important make sense? What do those familiar with both the JMAP and the MAP think? Continuing discussions and exercises among ADF and New Zealand Army staff are expected to produce further insights and accommodation around interpretation.

Our analysis of decision processes in health and the MAP focused on individual decision-making. In health applications, the process model is somewhat linear, moving from diagnosis to treatment. Biases associated with system 1 tended to be located in the diagnosis cluster of steps, and biases associated with system 2

in the treatment design and implementation clusters. The JMAP and MAP process models have steps and clusters that are richly inter-connected, and highlight the continual need for information collecting and information analysis. This suggests that system 1 and system 2 thinking may be important in multiple steps and/or clusters. The checklist located the biases associated with information analysis (confirmation, my-side, illusory correlation, over-confidence) in all three clusters (problem definition, design, and implementation) of the MAP.

In summary, empirical research focused on participant narratives and fostered convergence of meaning through a training program that was seen as good both for students and instructors.

Conclusion

Our research with senior staff in the New Zealand Army identified that the root cause of different perceptions about the MAP was unresolved dilemmas about time compression. Convergence of sense and meaning was fostered by a training program that engaged MAP instructors, a key informant, and the current cohort of junior officers in guided reflection, a think-aloud protocol, card sorts, reference models, a checklist for debiasing the MAP, and metacognitive exercises.

The training program had a key takeaway message that was consistent with research within the sense-making paradigm and, we believe, is applicable to many project-based organisations:

> Don't beat yourself up (about bias) as we need to make assumptions to survive everyday life. As you eat you assume that the food is not poisoned, although you have no evidence. As you drive through a green light, you assume the cross traffic will remain stopped, although you have no proof. The key is to have an awareness of our assumptions and realise that sometimes our intuition can hurt us and lead to a bad assumption gap. Whether consciously or subconsciously, once you make an assumption, the gap between what you think and the reality can get further and further apart. (Margetts, 2016b, p. 6)

This message was perhaps one reason why the checklist was perceived as good 'both ways'. Acknowledgement of bias had become an occasion for creativity and an accepted way of

enabling more rational thinking in the New Zealand Army. Previous research indicates that similar one-shot, relatively brief training programs were also received with some enthusiasm and had lasting effect. The research therefore illustrates a practical and cost-effective approach to developing debiasing training programs.

A focus on cognitive dual-process capability (system 1 *and* system 2) and the transitions between them has enabled the design of a practical debiasing program. This program integrated many biases under a single theoretical perspective and empirical process model. Future research will explore related applications in the context of the New Zealand Army, and allied forces including the ADF.

Dr Jim Sheffield is Director of Case Competitions at Victoria University of Wellington, and Senior Lecturer, School of Management, where he teaches problem solving and decision making to MBA students. He first researched heuristics and biases at the University of Arizona in the 1980s. His doctoral work in group support systems led to the creation of a Decision Support Centre at the University of Auckland. Major action research initiatives include the development of economic strategy, science policy and comprehensive regional planning. He has over 100 publications.

Colonel Roger Margetts is presently serving in Iraq as Director of Training for the Iraqi Security Forces. He has served in the New Zealand Defence Force since 1989, including command roles in the 1st Infantry Battalion, the 1st NZSAS Regiment and the Land Operations Training Centre. Roger has served extensively in the Middle East through multiple tours in Kuwait, Afghanistan and Iraq. Key staff leader roles include Head of Capability Management Teams and Instructor Counter Insurgency at the Australian Command and Staff College. Roger has a MBA from Victoria University of Wellington, and a Bachelor of Arts degree in Psychology from Massey University.

Lieutenant Colonel Gordon Milward is the Program Principal Lead Capability at the New Zealand Defence Force's (NZDF) Institute for Leader Development. He has commanded the 2/1st Infantry Battalion, the 3rd Land Force Group, the NZ Army Training Group and the NZDF Land Component. Other roles have been Chief of Staff Operations in East Timor, Chief of the Observer Group Golan in the Middle East, and the NZ Defence Advisor to PNG, Solomon Islands and Vanuatu. In 1996-97, while on the Directing Staff of the Australian Army Command and Staff College, he developed and trialled the planning and decision-making

process that became the Australian Army's Military Appreciation Process, the genesis of the current Joint Military Appreciation Process.

References

Bloxham, C. (2012), 'Thinking about thinking', *Darlington and County Durham Medical Journal*, Vol. 6, No. 2, pp. 5-13.

Cohen, M.S., B.B. Thompson, L. Adelman, T.A. Bresnick, L. Shastri and S.L. Riedel (2000), *Training critical thinking for the battlefield*, Cognitive Technologies Inc.: Arlington.

Cook, M.B., and H.S. Smallman (2008), 'Human factors of the confirmation bias in intelligence analysis: decision support from graphical evidence landscapes', *Human Factors*, Vol. 50, No. 5, pp. 745-54.

Croskerry, P. (2009), 'Clinical cognition and diagnostic error: applications of a dual process model of reasoning', *Advances in Health Science Education*, Issue No. 14, pp. 27-35.

Davis, P.K., J. Kulick and M. Egner (2005), *Implications of modern decision science for military decision-support systems*, RAND Corporation: Santa Monica.

Dobson-Keeffe, N., and W. Coaker (2015), 'Thinking more rationally: cognitive biases and the joint military appreciation process', *Australian Defence Force Journal,* Issue No. 197, pp. 5-16.

Evans, J., and K. Stanovich (2013), 'Dual-process theories of higher cognition: advancing the debate', *Perspectives on Psychological Science*, Vol. 8, No. 3, pp. 223-41.

Evans, J. (2008), 'Dual-processing accounts of reasoning, judgment, and social cognitio', *Annual Review of Psychology*, Issue No. 59, pp. 255-78.

Herdener, N., C.D. Wickens, B.A. Clegg and C.A.P. Smith (2016), 'Anchoring and adjustment with spatial uncertainty in trajectory prediction', Proceedings of the Human Factors and Ergonomics Society 2016 Annual Meeting, pp. 1605-9.

Hoskin, R. (2009), *The ghost in the machine: better application of human factors to enhance the military appreciation process*, Land Warfare Studies Centre: Canberra.

Kahneman, D. (2011), *Thinking, fast and slow*, Farrar, Straus and Giroux: New York.

Klein, G., and D. Klinger (1991), 'Naturalistic decision making', *Human Systems IAC Gateway*, Vol. XI, No. 3, pp. 16-9.

Lambe, K.A., G. O'Reilly, B.D. Kelly and S. Curristan (2016), 'Dual-process cognitive interventions to enhance diagnostic reasoning: a systematic survey', *BMJ Quality & Safety,* Issue No. 25, pp. 808-20.

Margetts, R. (2016a), 'Thinking about thinking: insights for junior officers in the New Zealand Defence Force', unpublished MBA research report, Victoria University of Wellington.

Margetts, R. (2016b), 'ACS MAP bias awareness package: student bias checklist & supporting material', New Zealand Defence Force.

Morewedge, C.K, H. Yoon, I. Scopelliti, C.W. Symborski, J.H. Korris and Karim S. Kassam (2015), 'Debiasing decisions: improved decision making with a single training intervention', *Policy Insights from the Behavioral and Brain Sciences*, Vol. 2. No. 1, pp. 129-40.

Powell, Colin, 'Intelligence reform', Opening Remarks before the Senate Governmental Affairs Committee Washington, DC, 13 September 2004', *Federation of American Scientists* [website], available at <https://fas.org/irp/congress/2004_hr/091304powell.html> accessed 18 April 2017.

Rolison, J.J., J. Evans, I. Dennis and C.R. Walsh (2012), 'Dual-processes in learning and judgment: evidence from the multiple cue probability learning paradigm', *Organizational Behavior and Human Decision Processes*, Issue No. 118, pp. 189-202.

Sheffield, J., and R. Margetts (2016), 'The soldier: my decisive moment in Afghanistan', *Emergence: Complexity and Organization*, Vol. 18, No. 1, pp. 1-12.

Slovic, P., M.L. Finucane, E. Peters and D.G. MacGregor (2004), 'Risk as analysis and risk as feelings: some thoughts about affect, reason, and rationality', *Risk Analysis*, Vol. 24, No. 2, pp. 311-22.

Smith, C.R. (2011), *Design and planning of campaigns and operations in the twenty-first century*, Land Warfare Studies Centre: Canberra.

Wickens, C.D., S.L. Ketels, A.F. Healy, C.J. Buck-Gengler and Lyle E. Bourne Jr., (2010), 'The anchoring heuristic in intelligence integration: a bias in need of de-biasing', Proceedings of the Human Factors and Ergonomics Society 54th Annual Meeting, pp. 2324-8.

Social and political acumen: a vital but neglected professional skill set

Brigadier Nicholas Jans, OAM (rtd), formerly Australian Army

We had run up against a wall in dealing with a particular agency in Defence. We initially got bogged down with the thought that 'they are wrong', and it was frustrating that our 'logical arguments' didn't work. This especially often happens when dealing with gatekeepers: those who control access to key decision-makers elsewhere in the organisation. But we persisted. Not getting our argument across would be very costly; and we also needed to maintain the long-term relationship. We moved from an approach that was based on verbal arguments to demonstrations of how these would work, using examples and dealing with questions. All the time, we were reassuring them of our experience in this area, and gently guiding them through the arguments while biting our tongues. Eventually—inch by inch—we turned their thinking around towards our views and goals.

<div align="right">An O7 officer interviewed for this study</div>

As the case above illustrates, work in the Australian Defence bureaucracy is subtly but significantly different to the structured and focused activities that comprise the majority of appointments in the first half of the average professional's career. Issues are often complex, with long-term implications across a range of political, professional, economic and societal factors. They involve multiple stakeholders, many of whom have distinct agendas, perspectives and priorities. All this equates to a career environment that often seems a world away from the well-ordered routines and relationships of the ship, the regiment or the squadron.

Those who perform well in such an environment tend to be skilled in a competency set known as social and political acumen (SPA). SPA comprises the skills needed for situations involving multiple stakeholders with diverse and sometimes competing interests, in order to find about and make sense of the environment,

and to achieve sufficient alignment of interests and/or consent in order to achieve outcomes.[1] Its importance is indicated by its inclusion and primacy in the appraisal form used for senior military officers (AC740: Executive and Senior Executive Officer Appraisal and Development Report for Military Officers), where it is one of four core professional competencies listed for the annual evaluation of O6 and O7.[2]

However, there are crucial impediments to sound professional understanding and practice of SPA. AC740 is surprisingly vague about the nature of SPA and its component behaviours (beyond the terms 'political', 'diplomatic', 'networker' and 'liaising'), and the competency set receives little explicit coverage in either formal professional military education or mentoring.[3]

The study reported herein is an important first step in finding out more about SPA and its practice, in an exploration of the skills involved, the main weaknesses and vulnerabilities in its performance, and options for lifting individual and collective performance.[4]

The study

The study focused on those in the mid-senior career stage. Invitations were emailed to all 212 uniformed O6 and O7 officers working in the Canberra Defence bureaucracy. Responses were received from 67 officers, 33 of whom were interviewed (these were essentially those who responded first). Sample details are shown in Table 1.[5]

Interviews explored the extent to which O6 and O7 were aware of and practised SPA, and the benefits and challenges involved in doing so. The questionnaire (a modification of the instrument used in recent ground-breaking research of public servants in several Commonwealth

countries) was sent to interviewees in advance.[6] About one in three prepared responses prior to the interview. Almost all interviews were conducted by telephone, with transcripts sent to interviewees within 48 hours for checking.[7]

Findings

The report presents findings in terms of four broad aspects of SPA:

- 'What': the concept and practice of SPA as perceived by those at the middle-senior career levels;
- 'Why': the reasons why officers at the O6 and O7 level need to be skilled in SPA;
- 'How': details of SPA practice; and
- 'So-what: the implications of the findings of this study for improving understanding and professional practice.

The 'what'

The large majority of interviewees regarded SPA as a core key skill set, typically describing SPA in terms such as 'vital', 'critical', 'fundamental', 'very important' or 'core to what I do'. Their comments included:[8]

> SPA applies to virtually everything that I do—I can't think of an activity where it does not. Perhaps the extent of its use varies but its importance does not. Whereas work at earlier career levels is essentially focused inwards and downwards, that is not the case here.

> SPA is about understanding how certain courses of action will be seen by government and other stakeholders, who to get onside, which ducks to get in a row, what do they care about, who do they trust most (and related to that last point, how I can line those people up to support my needs), which networks to tap and manage given a particular

	O6	O7	Total		Men	Women
Navy	6	5	**11**		8	3
Army	6	4	**10**		8	2
Air Force	7	5	**12**		10	2
Total	**19**	**14**	**33**		**26**	**7**

Table 1: SPA study sample

need and context, and which networks need refreshment, given that every January we find that the turnover from last year's network has been about 50%.

Interviewees showed a ready acceptance of the need to go beyond collaboration into compromise, trade-off, and acceptance of significant modification (at least temporarily) to their own goals in the interests of the larger good. This larger good is often expressed in terms of organisational outcomes (that is, advancing the broader agenda) or of maintaining an important relationship. These often go well beyond simple compromise into quasi-creative solutions that improve on and are more generally acceptable than original proposals. Hence, comments included:

> Getting the right result is more important than being right…. [and] The aim is to find win-win solutions consistent with other issues on one's agenda.

Importantly, interviewees also saw the clear logic in coupling the 'social' with the 'political' in terms of discerning what is going on, what is important, who has a stake, and the points of potential agreement and leverage; and making sense of bigger picture issues and how local agendas fit or could better fit with these.

However, being savvy does not equate to being skilled, and most were quick to concede their SPA limitations and those of their colleagues:

> I'm probably not as skilled at networking and liaising as I need to be; either that or I don't give sufficient attention to them.

> A lot of what we do is very simple, but commonsense is not always applied. People get stuck in the process, rather than trying to understand the issues.

The 'why'

SPA is important for mid-to-senior officers for at least four main reasons. Firstly, many policy initiatives and projects at this level are complex, and most of those at this level understand that such initiatives have to fit the ADF as a whole rather than just the contemporary needs of a single Service:

> Understanding the nature of the playing field helps you understand where your current

thinking fits with that of others, and how it might be possible to reshape your thinking so that it aligns with rather than is contrary to that of others.

Secondly, while we might like to think of ourselves as logical beings, the reality is that our perceptions of and reactions to our world are subject to a variety of psychological influences. For example, we tend to give attention to evidence from sources we have learned to trust or to whom we give credence for other reasons. Within the military, this tendency is reinforced by the value placed on qualities that are often difficult to describe and analyse (such as status, experience, reputation, etc).[9]

A third reason why SPA is important at this level is because of subtle but significant shifts in the nature of leadership. In contrast to the more direct engagement of earlier career roles, middle-level and senior leadership depends much more on indirect control and influence, and on being a facilitator of the work of others, as opposed to 'leading from the front':

> Pre O6, you are doing things; you are doing 'the right work'. At higher levels, however, your main function is to help a range of others to do their work. In order to be able to do this, you need to understand the nature of their work and the context in which it is done. SPA is fundamental to this understanding.

The final reason why officers at this level need SPA skill is that the basis for authority in the bureaucracy is significantly different to that which applies in ship and units. Implicit authority in the ADF tends to be characterised by a 'knower code', that is, 'Do as I say because of who I am', with authority legitimised by rank, experience, status and function. In contrast, the APS is characterised by a 'knowledge code', that is, 'do as I say because I know'.[10] Implicit authority in the Defence bureaucracy is a shifting amalgam of the two, with many military professionals generally not even realising this, let alone adjusting to it.

> You need to understand what motivates different people and therefore how you shape and package an issue according to its target. It is applicable even in dealing with one's own staff.

> One of the most challenging aspects is to find the right words to show the other party that I

am indeed trying to see things from their perspective, and am trying to look at both sides.

In short, the ability to get something accepted by a number of stakeholders depends very much on understanding their perspectives and on forging an emotional connection between them. Although it might sound manipulative—and, in many areas of commercial practice, it clearly is—much depends on the spirit and purpose by which the connection is being made. This is where integrity and authenticity, underpinned by professional ethics, are important:

> It depends in part on building useful networks, but that is just the start. You then need social skills (active listening, self-awareness, body language, and the like). Very importantly, it depends also on the kind of person you present as. If you don't present as authentic, it is not surprising if you are not completely trusted.

The 'how'

SPA activities comprise six main complementary dimensions, grouped in three categories:[11]

Foundational:

- *Use personal skills.* Be self-aware in regard to one's own motives and behaviours; be open-minded and curious; exercise self-control.

- *Use interpersonal skills.* Interact constructively with others; get support or buy-in from people over whom one has no direct authority.

Functional:

- *Build relationships and networks.* Build robust relationships and networks across intra- and inter-organisational boundaries to support sense-making and influencing.

- *Read people and situations.* Analyse and discern the dynamics that can occur when stakeholders and agendas come together; gain and use knowledge of institutions, processes and social systems to understand what is happening or what might happen.

Strategic:

- *Build alignment and alliances.* Build alignment from different interests, goals and motives by forging differences in outlook or emphasis into collaborative alliances and actions.

- *Think and act strategically.* Think and act strategically in relation to power dynamics and organisational attributes that can be managed to improve effectiveness and efficiency purpose, and consider these in the context of longer-term issues and second- and third-order effects.

Table 2 gives examples of the behaviours associated with each of these dimensions.[12]

The 'so-what'

The final section discusses how SPA practice can be improved. It proposes a number of actions, ranging across the developmental, the structural, and the symbolic.

Developmental

Developmental activities that directly shape SPA could include:

- Giving SPA greater emphasis in major professional military education activities, particularly the important year-long courses at the Australian Defence College;

- Encouraging mentoring by raising awareness, providing refresher training, emphasising the benefits for mentors as well as mentorees, etc;

- Developing the skill progressively in a series of short on-site courses; and

- Running common-interest groups or 'learning circles', facilitated by a moderator, in which small groups of officers meet regularly to discuss and exchange ideas on SPA and other leadership practices.

The advantage of including SPA in the longer professional military education programs is that would allow experienced officers to exchange ideas with peers, and give them time to examine and learn about the practice of SPA within the broader professional and strategic context:

> I didn't really need SPA in the early stages of my career, but the higher you go, the greater the ambiguity of the environment and issues, and thus the greater the need. You get better, and you learn from reflecting on your social interactions and political judgements. I once was given some great advice: 'Every day you will go home and reflect on what you said, how

Category	Dimension	Example behaviours
Foundational	*Use personal skills*	Be proactive while aware of own values, motives and behaviours. Be humble about what one does not know, open to the views of others, and curious about others' views.
	Use interpersonal skills	Establish rapport and make people feel valued, by active listening, inclusive language, verbal reinforcement, sharing credit, frequent contact, etc. Use 'tough' skills when necessary: negotiate; stand up to pressures from others; handle conflict to achieve constructive outcomes, etc.
Functional	*Build relationships and networks*	Develop and cultivate multiple and overlapping networks to support intelligence gathering, indirect influencing, alliance building, etc. Understand others' perspective and help them to understand yours; get support and buy-in from those over whom you have no direct authority.
	Read people and situations	Use professional and tacit knowledge of institutions and social systems to understand what is or what might happen. Analyse or intuit likely standpoints of various interest groups in advance.
Strategic	*Build alignment and alliances*	Seek out, develop and cultivate alliances and partnerships, and bring difficult issues into the open. Develop agreed frames of reference or mental models to help forge differences into collaborative action.
	Think and act strategically	Understand and manage core organisational power dynamics and how these might shape, or can be managed so as to shape, long-term capacity and direction. Scan the broad environment – internal, external, political, societal, organisational – to analyse or intuit the 'so-what?' and possible second- and third-order effects of key factors and situations.

Table 2: SPA skills framework

it went over, and what it meant in terms of your leadership effect'. For 'leadership', read 'SPA'.

The advantage of the mentoring option is its long term, progressive facility, in an environment in which the mentoree would feel safe to be candid and to ask the 'dumb questions'. The advantage of the short-course option is that it enables the officer to put this learning into practice while the material is still fresh in the mind.

The learning circles option shares these advantages and more. As was shown earlier, O6/O7 officers collectively possesses a sophisticated understanding of SPA, so they would learn much from each other, while simultaneously establishing and expanding their networks. And this option would also be the cheapest and easiest to enact. Underlying all these is the principle of 'practice, practice, practice': as one officer remarked, 'intuition is a function of experience'.

Structural

Structural activities for SPA are those that indirectly shape the skill set by providing task aids, professional guidance and prompts, and incentives for certain ways of behaving. These could include:

- Using a SPA checklist and SPA behaviour scales from the component activities in the SPA skills framework for both personal guidance and for self- and supervisor assessment;

- Making SPA more prominent in professional leadership models and incorporating SPA-related elements into these models; and

- Giving SPA greater emphasis in annual performance reviews for O5 and in major professional military education activities such as those at the Australian Defence College.

The first structural activity option—developing and using a SPA checklist, etc—would be straightforward and would have significant practical benefit. Individuals and mentor-mentoree pairs could use the information gathered thereby to identify strengths, weaknesses and corrective action.

Symbolic

Symbolic activities for SPA include giving greater weight to SPA expertise in career decision-making and by increasing official recognition of SPA performance (such as in honours and awards lists). Symbolic activities would raise the profile of the skill set and of those who are seen as expert practitioners, and give further incentives for those at all levels to focus on its practice.

Several officers expressed the view that career decisions are unfairly skewed towards those who thrust themselves forward and continue 'leading from the front' in a traditional manner:

> Most are not as good as they think they are; many are not good listeners; and they are not comfortable with counter views. And many are too inclined to 'busyness', and thus have inadequate time to reflect on how and why things are going as they are and to plan how to do something about changing this.

Those who are more inclined to 'lead from the shadows' tend to be overlooked, ironically because of their very success in doing so. And another irony, as one interviewee pointed out is that:

> While extroverts are more likely to be noticed, introverts have an advantage. X was a particular example. He used to say very little in a meeting but he was able to sum up brilliantly at the end.

SPA can also be enhanced symbolically when senior officers demonstrate appropriate behaviour:

> Senior officers must play their part in setting the tone and establishing the right environment. We recently saw a period in which the three personnel O7s collaborated: this established an appropriate tone at the top, and this flowed through to their more junior colleagues.

Encouragingly, most O6/O7 officers see their senior colleagues as good SPA role models, with many citing 3- and 4-stars as excellent examples of SPA:

> Most of those I deal with are well skilled. They are aware of different ways to get something done, and are prepared to actually do that something. In essence, they are well versed in greasing the wheels without being conniving; and they know different ways that work and are better at identifying and articulating these.

> Just as importantly, they had well-stablished reputations for integrity/character. This allows them to set a positive leadership example of authenticity and to be respected. This in turn gives the credibility to call it as they see it; and this adds further to the reputation and lustre.

However, others see it as:

> ... patchy; with many coming up through a comparatively narrow career path, and finding themselves in their first joint job as a Brigadier. As a consequence, they struggle.

Conclusions

SPA emerges as an intriguing 'sleeper' dimension of military professional leadership. Encouragingly, most O6 and O7 seem to have at least a good working understanding of what is involved but very few (especially the O6) appreciate the full dimensions of the skill set, particularly in terms of low-key and behind-the-scenes indirect influence that often is done so subtly that it is scarcely noticed.

However, almost all see themselves as having at least some significant deficiencies in their ability to practice SPA. They pointed to the deficiencies in ADF leadership doctrine, in terms of its coverage of such an important but subtle skill set; to its inadequate coverage in Service leadership thinking and models and in professional military education programs; and to the related lack of mentoring and other somewhat indirect aspects of development and education.

Incidentally, very few interviewees spoke of using SPA for the purpose of personal gain, with a number expressing their aversion for doing so. However, SPA can be useful for seeking out appropriate mentoring opportunities.

Enhancement of SPA skill for mid-to-senior officers is likely to result in significant improvements in personal and organisational efficiency and effectiveness. And for an individual, focusing on SPA might well turn out to one of the best things that individuals could do for their careers in both the short and the longer term.[13]

Brigadier Jans served in the Australian Regular Army in field artillery, training and personnel policy development. Since his retirement from full-time service in 1985, he has consulted to the ADF, the US Navy and a range of Australian and international civilian organisations on leadership and strategic human resource management. He has a PhD in organisational behaviour. He has lectured at the University of Canberra, is on the editorial board of the international journal 'Armed Forces & Society', and currently holds a visiting fellowship at the School of Business, University of NSW in Canberra.

References

1   Adapted from Jean Hartley, John Alford, Owen Hughes and Sophie Yates, *Leading with political astuteness: a study of public managers in Australia, New Zealand and the United Kingdom*, ANZSOG and CM: Melbourne, 2013, p. 3. Important ideas were also gleaned from the conceptual development of the 'boundaryless career' and the distinctions between 'know-how' and 'know-whom, know-why and know-so what': see R.J. Defillippi and M.B. Arthur, 'The boundaryless career: a competency-based perspective', *Journal of Organizational Behavior*, Issue 15, 1994, pp. 307-24.

2   The Service ranks at O6 and O7 are, respectively, CAPT/COL/GPCAPT and CDRE/BRIG/ACDRE.

3   Similarly, while Defence SES officers are expected to perform against the SES capability framework, including 'political nous', the capability framework gives little detail of what the latter entails.

4   Ethics approval was granted by DPR-LREP 014/15 AB3861781 of 17 March 2015.

5   The sample may possibly be biased, with those who volunteered perhaps largely comprising those who are already comfortable with and engaged in SPA. However, this is unlikely to be a significant limitation, given that the invitation to participate was answered by nearly one in three from a group of very busy people (which would be regarded in scholarly circles as a good result). A sample of 33 is comparatively large for an analysis based on in-depth interviewing and detailed analysis of responses.

6   The questionnaire is available by request from the author: nicholas.jans@gmail.com

7   The study has a significant potential limitation in that it is possible that those who volunteered largely comprised those who are already comfortable with and engaged in SPA. However, this limitation may not be significant. The invitation to participate was answered by nearly one in three from a group of very busy people (and would be regarded in scholarly circles as being a good result). Moreover, a sample of 33 is comparatively large for an analysis based on in-depth interviewing and detailed analysis of responses.

8   Quotes from interviews are presented in this and following sections. A host of relevant information could have been included but was omitted because of space limitations. For further details, see Nicholas Jans, *Supporting, influencing, leading: getting things done through social and political acumen*, Centre for Defence and Strategic Studies: Canberra, 2015.

9   N.A. Jans, 'New values, old basics: how leadership shapes support for inclusion', *Australian Defence College* [website], September 2014, available at <http://www.defence.gov.au/ADC/Publications/Commanders/2014/New_values_old_basics_how_leadership-shapes_support_for_inclusion.pdf> accessed 11 July 2017.

10 Elizabeth Thomson, *Battling with words: a study of language, diversity and social inclusion in the Australian Department of Defence*, Department of Defence: Canberra, 2014, p. xii. I have paraphrased Thomson's concept of the ADF code slightly. Her concept is 'Do as I say because I am who I am'.

11 Five of these closely match those identified in recent research on Commonwealth senior public servants: see Hartley, *Leading with political astuteness*; and Gerald R. Ferris, Darren C. Treadway, Robert W. Kolodinsky, Wayne A. Hochwarter, Charles J. Kacmar, Ceasar Douglas and Dwight D. Frink, 'Development and validation of the political skill inventory, *Journal of Management*, Issue 31, 2005, pp. 126-52. The additional dimension was 'build relationships and networks', which emerges as the pivotal and most frequently mentioned activity set.

12 For a broader discussion, see Jans, 'Supporting, influencing, leading'.

13 For examples of how 3- and 4-star officers depend on social and political acumen, see Nicholas Jans, Stephen Mugford, Jamie Cullens and Judy Frazer-Jans, 'The Chiefs: a study of strategic leadership', *Australian Defence College* [website], 2013, pp. 20 and 57, available at <http://www.defence.gov.au/adc/publications/chiefs/thechiefs.pdf> accessed 27 June 2017.

Primary health care in the ADF

Commander Neil Westphalen, Royal Australian Navy Reserve

An earlier article by the author asserted that high rates of preventable workplace illness and injury indicate the need to improve the management of the occupational and environmental hazards associated with ADF workplaces, with emphasis on prevention rather than treatment.[1] This article expands with respect to providing primary health care for ADF members.

Primary health care in Australia

In 2014, the Australian health care system had 98,807 medical practitioners in more than 80 specialties, including 32,050 general practitioners.[2] The latter included 21,576 Fellows and trainees of the Royal Australian College of General Practitioners, and 1630 Fellows and trainees of the Australian College of Rural and Remote Medicine. The remaining 8844 general practitioners did not have fellowships but were vocationally registered by Medicare to provide primary health care services. By comparison, in 2014 the Australasian Faculty of Occupational and Environmental Medicine represented only 492 Australian physicians and trainees.

Definitions

The definitions of 'primary health care' used in Australia are rather complex. The Australian Institute of Health and Welfare defines primary health care as 'typically the first health service visited by patients with a health concern…. It includes most health services not provided by hospitals, and involves:

- A range of activities, such as health promotion, prevention, early intervention, treatment of acute conditions and management of chronic conditions;

- Various health professionals, such as general practitioners, dentists, nurses, Aboriginal health workers, local pharmacists and other allied health professionals; and

- Services delivered in numerous settings, such as general practices, community health centres, allied health practices including physiotherapy and dietetic practices, and more recently via telecommunications technologies such as health advice telephone services, video consultations and remote monitoring of health metrics through electronic devices'.[3]

The College of Rural and Remote Medicine's position paper, 'Defining the specialty of general practice', refers to the 1991 international consensus description of general practice as follows:

> The general practitioner or family physician is the physician who is primarily responsible for providing comprehensive care to every individual seeking medical care and arranging for other health personnel to provide services when necessary.
>
> The general practitioner/family physician functions as a generalist who accepts everyone seeking care, whereas other health providers limit access to their services on the basis of age, sex or diagnosis. The general practitioner/family physician cares for the individual in the context of the family, and the family in the context of the community, irrespective of race, religion, culture or social class. He is clinically competent to provide the greater part of their care after taking into account their cultural, socio-economic and psychological background. In addition, he takes personal responsibility for providing comprehensive and continuing care for his patients.
>
> The general practitioner/family physician exercises his/her professional role by providing care, either directly or through the services of others according to their health needs and resources available within the community he/she serves.[4]

The Royal Australian College of General Practitioners' website describes general practice as providing 'person-centred, continuing, comprehensive and coordinated whole person health care to individuals and families in their communities'.[5] It also indicates that, as a relationship-based specialist medical discipline, general practitioner clinicians are defined by the characteristics of their discipline, which are person-centredness; continuity of care; comprehensiveness; whole person care; diagnostic and therapeutic skill; coordination and clinical teamwork; continuing quality improvement; professional, clinical and ethical standards; leadership, advocacy and equity; and continuing evolution of the discipline.

Implications

Some general practice attributes, per the Royal Australian College of General Practitioners' website in particular, facilitate the baseline clinical skills required to provide primary care for deployed ADF members and to undertake humanitarian aid/disaster-relief operations.[6] These attributes include providing comprehensive whole-person diagnostic and therapeutic care to individual patients within a clinical, multi-disciplinary environment (usually but not always in a lead role).

However, the attributes that are less consistent with respect to primary care for ADF members pertain to person-centredness (particularly with respect to the duty-of-care obligations of their patient's chain of command), continuity of care (with particular reference to their patient's geographic mobility) and primarily providing care for a working-age population that has an increasing but still small proportion of female members.[7]

Furthermore, neither the College of Rural and Remote Medicine nor the Royal Australian College of General Practitioners refers to a role for general practitioners with respect to assessing the effects of workplace hazards on their patient's health or vice versa (that is, assessing their patient's medical suitability for employment). The author's earlier paper described some of the limitations of general practitioners regarding their capacity to undertake these tasks.

On the other hand, military and civilian occupational and environmental physicians can complement their general practitioner colleagues regarding the primary care diagnosis and treatment of workplace-related musculoskeletal and mental health disorders, managing workplace-based rehabilitation, and assessing medical suitability for employment and deployment.

Reasons for presentation	Number	%	Rate per 100,000	5% LCL[b]	95% UCL[c]
Prescription[a]	13,131	8.7	13.3	12.6	14.0
Checkup[a]	13,015	8.6	13.2	12.6	13.8
Test results[a]	9342	6.2	9.5	9.0	9.9
Cough[c]	6187	4.1	6.3	5.8	6.7
Back complaint[a,c]	3347	2.2	3.4	3.2	3.6
Vaccinations[a,d]	3324	2.2	3.4	3.1	3.6
Administration procedure[a]	3252	2.1	3.3	3.1	3.5
Throat complaint[c]	2836	1.9	2.9	2.6	3.1
Rash[a]	2678	1.8	2.7	2.5	2.9
Blood test[a]	2283	1.5	2.3	2.2	2.5
Depression[c,d]	2224	1.5	2.3	2.1	2.4
Abdominal pain[a]	2101	1.4	2.1	2.0	2.3
Upper respiratory tract infection[c,d]	2077	1.4	2.1	1.8	2.4
Fever	1826	1.2	1.8	1.7	2.0
Headache[a]	1635	1.1	1.7	1.5	1.8
Skin complaint[c]	1577	1.0	1.6	1.5	1.7
Hypertension/high blood pressure[a,d]	1505	1.0	1.5	1.3	1.7
Knee complaint[c]	1505	1.0	1.5	1.4	1.6
Observation/education/advice/diet[a]	1499	1.0	1.5	1.4	1.7
Anxiety[a,c]	1465	1.0	1.5	1.4	1.6
Weakness/tiredness	1464	1.0	1.5	1.4	1.6
Other referrals not elsewhere classified	1458	1.0	1.5	1.4	1.6
Sneezing/nasal congestion[c]	1281	0.8	1.3	1.1	1.5
Shoulder complaint[c]	1259	0.8	1.3	1.2	1.4
Diabetes[a,d]	1251	0.8	1.3	1.1	1.4
Diarrhoea	1238	0.8	1.3	1.1	1.3
Ear pain/earache	1220	0.8	1.2	1.1	1.3
Sleep disturbance	1162	0.8	1.2	1.1	1.3
Vertigo/dizziness	1086	0.7	1.1	1.0	1.2
Foot/toe complaint[c]	1086	0.7	1.1	1.0	1.2
Subtotal	**89,287**	**58.9**	-	-	-
Total Reasons for Presentation	**151,636**	**100.0**	**153.6**	**151.8**	**155.4**

Table 1: Top 30 reasons to present to civilian general practitioners, 2013-148

ADF non-deployed primary health care

The earlier paper noted that, anecdotally, only 20-40 per cent of ADF primary care presentations are for conditions typically seen in an equivalent Australian civilian population. In support of this contention, Table 1 describes the top 30 reasons for civilian patients to see a general practitioner in 2013-14.

Notes:

a. Includes multiple diagnoses.
b. LCL = lower confidence level; UCL = upper confidence level. The smaller the interval between LCL and UCL, the more likely the rate per 100,000 presentations figure is truly representative.
c. Most common ADF clinical conditions in 2007-8 and 2008-9.[9]
d. Most common civilian clinical conditions.[10]

Furthermore, Table 2 shows that in 2013-14, only 2.4 per 100 patient presentations to civilian general practitioners were for work-related reasons, making up only 1.5 per cent of all reasons to see a general practitioner.

Notes:

a. LCL/UCL as for Table 1.
b. Includes general check-ups, administrative procedures, cuts/lacerations, and other skin injuries.

Notwithstanding the lack of data regarding ADF primary care presentations, Tables 1 and 2 confirm the substantial differences between the ADF and civilian populations. In short, compared to their civilian colleagues, ADF general practitioners see proportionally far more musculoskeletal and mental health disorders, most of which

are either work-related or affect the ability of the patient to work.

Furthermore, these figures do not include non-primary-care ADF general practitioner presentations such as health assessments ('medicals') or Medical Employment Classification Reviews, both of which are occupational and environmental health functions. These presentations arguably consume 30-40 per cent of the average military general practitioner's workload, or about the same as their actual clinical workload.[12]

General practitioners and occupational and environmental health

The earlier paper refers to the extensive media commentary that demonstrates the need to improve how the ADF manages occupational and environmental hazards in its base settings. It also noted that thus far there has been no requirement for 'garrison' health services to facilitate local Command compliance with the *Work Health and Safety Act 2011.* This limitation, combined with a lack of occupational and environmental physicians within Joint Health Command, currently restricts 'garrison' rehabilitation and other clinical occupational and environmental health services to that provided by general practitioners and other non-occupational and environmental health providers.

Yet a review of the College of Rural and Remote Medicine's website confirms the absence of any internal occupational and environmental medicine courses. Furthermore, the only occupational and environmental health-related references in the Royal Australian College of General Practitioners' '2016 Core Skills Unit' of its 'Curriculum for Australian general practice' are two lines indicating that general practitioners are

Work-related reason	Number	Per cent of total	Rate per 100	5% LCL[a]	95% UCL[a]	Work-related as % of all
Musculoskeletal	1291	56.9	1.3	1.2	1.5	7.3
Psychological	299	13.2	0.3	0.3	0.4	2.3
Other work-related[b]	878	29.9	0.7	0.6	0.8	0.6
Totals	**2268**	**100**	**2.4**	**2.2**	**2.5**	**1.5**

Table 2: Most common work-related reasons to present to civilian general practitioners, 2013-14[11]

only expected to undertake an education and promotion role with respect to early return-to-work after work-related injuries or illness, and identifying opportunities to prevent injury and disease in at-risk individuals.[13]

The Royal Australian College of General Practitioners' curriculum offers 'contextual units' in military medicine and occupational medicine.[14] Other contextual units of less direct relevance to the ADF include travel medicine, individuals with disabilities, musculoskeletal and sports medicine, adult medicine, men's health, women's health, psychological health, abuse and violence, and addiction medicine. However, all these units consist of 2-3 page summaries, each only describing the relevance of the topic in a general practitioner setting, with very limited further references regarding the actual skills required.

The Royal Australian College of General Practitioners has a Military Medicine Working Group, which is developing a post-fellowship Diploma of Military Medicine that includes modules in public health, and occupational and environmental health. However, neither of the relevant Faculties of Public Health or Occupational and Environmental Medicine have so far been involved in their development.[15]

Furthermore, the Australian and New Zealand Society of Occupational Medicine Inc. is a professional society for those who practise or have an interest in occupational health. It seeks to advance the knowledge, practice and standing of occupational health by providing opportunities for professional development, networking and partnerships.[16] However, 'garrison' services have not yet mandated employing general practitioners from this or other occupational health organisations.

Civilian general practitioner training, therefore, provides a comprehensive basis for the *clinical* primary care of individual ADF members. However, it does not provide the full range of *non*-clinical primary care and other occupational and environmental health skills and expertise required for the ADF workforce. This further supports the author's earlier assertion that it takes up to 12 months for new full-time general practitioners to understand how to assess medical suitability for ADF employment and

deployment, even without considering any other military occupational and environmental health functions.

ADF medical officer career implications

Defence requires all uniformed, Australian Public Service and contract civilian medical practitioners to comply with the registration standards of the Medical Board of Australia. Service medical officers currently have a four-level career structure, linked to remuneration, as follows:

- ML1: new entry medical officers who have not yet met all the requirements to be operationally deployable under remote supervision, pending further medical studies and Service training courses. All permanent medical officers are expected to initially undertake primary health care roles before diversifying into other streams. In practice, however, ADF medical officer recruiting is almost exclusively premised on an eventual civilian general practitioner career.

- ML2: medical officers who are deployable with remote supervision. Although it is intended that medical officers begin specialising into either clinical or management staff/force protection streams at this point, the aforementioned initial recruiting practices mean that exceptionally few are choosing the latter.

- ML3: primary health care medical officers, with either a Royal Australian College of General Practitioners or College of Rural and Remote Medicine fellowship. Most medical officers choose to leave the ADF at this point, which generally coincides with the end of their return-of-service obligation.

- ML4: medical officers who have achieved a qualification listed as a specialist medical qualification by the Medical Board of Australia, other than general practitioner. Among other specialties, it includes management/staff/force protection specialties, such as medical administration, public health, and occupational and environmental medicine. However, in November 2016, there were only two permanent ADF occupational and

environmental physician trainees, while public health and medical administration trainee numbers were probably comparable.[17]

An under-recognised medical officer retention factor pertains to the lack of diversity with respect to the clinical conditions experienced by the ADF workforce. Treating a succession of musculoskeletal and mental health disorders every day is unlikely to facilitate retaining Service or civilian general practitioner medical officers who prefer more clinical variety.

Consideration should therefore be given to recruiting and training more Service and civilian medical officers with an interest in an occupational and environmental medicine career. It is likely that they would not only maintain an interest in workforce primary health care but also accept that their eventual career progression to non-clinical roles is more consistent with their occupational and environmental medicine aspirations compared to their general practitioner peers. These 'garrison' occupational and environmental physicians would also facilitate local Command compliance with the *Work Health and Safety Act*.

Conclusion

With ADF personnel arguably exposed to the most diverse range of occupational and environmental hazards of any Australian workforce, high rates of preventable workplace illness and injury indicate the need to improve the management of occupational and environmental health hazards, with better emphasis on prevention rather than treatment.

This suggests that the ADF's health services should be premised on an occupational and environmental health paradigm, with revised fundamental inputs to capability that would lead to a genuinely holistic and sustainable workforce-based ADF health service delivery model by 2030.

Although general practitioners would still maintain an essential primary health care role within such a paradigm, they lack the skills and expertise to provide the full range of clinical and other occupational and environmental health services required for a young, fit, geographically mobile

and predominantly male (although this is changing) ADF workforce.

However, occupational and environmental physicians have the skills and expertise to provide primary health care for workplace-related musculoskeletal and mental health injuries, as well as managing workplace-based rehabilitation, and assessing medical suitability for employment and deployment. Such a delivery model would entail recruiting and training more Service and civilian medical officers who are interested in an occupational and environmental physician career.

Dr Neil Westphalen graduated from Adelaide University in 1985, and joined the RAN in 1987. He is a RAN Staff Course graduate, and a Fellow of both the Royal Australian College of General Practitioners and the Australasian Faculty of Occupational and Environmental Medicine. He also has a Diploma of Aviation Medicine and a Master of Public Health, and was admitted as a Foundation Fellow of the new Australasian College of Aerospace Medicine in 2012.

His seagoing service includes HMA Ships Swan, Stalwart, Success, Sydney, Perth and Choules. Deployments include Operations DAMASK VII, RIMPAC 96, TANAGER, RELEX II, GEMSBOK, TALISMAN SABRE 07, RENDERSAFE 14 and KAKADU 16. His service ashore includes clinical roles at Cerberus, Penguin, Kuttabul, Albatross and Stirling, and staff positions at Headquarters Australian Theatre, Joint Health Command, Director Navy Occupational and Environmental Health, Director of Navy Health, and Fleet Medical Officer (the latter from January 2013 to January 2016). Commander Westphalen transferred to the Active Reserve in July 2016.

References

1   N. Westphalen, 'Occupational and environmental medicine in the Australian Defence Force', *Australian Defence Force Journal*, Issue 200, November-December 2016, pp. 49-58, available at <http://www.adfjournal.adc.edu.au/UserFiles/issues/200%202016%20Nov_Dec.pdf> accessed 21 April 2017.

2   Department of Health, 'General practice statistics', *Department of Health* [website], available at <http://www.health.gov.au/internet/main/publishing.nsf/content/General+Practice+Statistics-1> accessed 21 April 2017.

3   Australian Institute of Health and Welfare, 'Australia's Health 2014', *Australian Institute of Health and Welfare* [website], p. 241, available at <http://www.aihw.gov.au/WorkArea/DownloadAsset.aspx?id=60129548150> accessed 21 April 2017.

4   Australian College of Rural and Remote Medicine, 'Defining the specialty of general practice', *Australian College of Rural and Remote Medicine* [website], available at <http://acrrm.org.au/docs/default-source/documents/about-the-college/position-statement-defining-the-specialty-of-general-practice.pdf> accessed 21 April 2017.

5   Royal Australian College of General Practitioners, 'Becoming a general practitioner in Australia: what is general practice?', *Royal Australian College of General Practitioners* [website], available at <http://www.racgp.org.au/becomingagp/what-is-a-gp/what-is-general-practice> accessed 21 April 2017.

6   Examples where clinical primary care services have been essential to ADF humanitarian aid/disaster-relief operations include HABITAT (1991 aid to the Kurd population after the 1st Gulf War), TAMAR (1994-5 response to the Rwandan genocide), SUMATRA ASSIST (2004 tsunami), PAKISTAN ASSIST (2005 earthquake), PACIFIC ASSIST (2015 cyclone) and FIJI ASSIST (2016 cyclone). Primary care services are also intrinsic to the Exercise PACIFIC PARTNERSHIP series of humanitarian aid deployments, held in conjunction with the US and other partner nations since 2006.

7   Westphalen, 'Occupational and environmental medicine in the Australian Defence Force'.

8   Sydney University Family Medicine Research Centre, 'General practice activity in Australia 2014-15', *Sydney University Family Medicine Research Centre* [website], available at <https://ses.library.usyd.edu.au/bitstream/2123/13765/4/9781743324530_ONLINE.pdf> accessed 21 April 2017.

9   Australian Institute of Health and Welfare, 'Australia's health 2010', *Australian Institute of Health and Welfare* [website], available at <http://www.aihw.gov.au/WorkArea/DownloadAsset.aspx?id=6442452962> accessed 21 April 2017.

10 Georga Cooke, Lisa Valenti, Paul Glasziou and Helena Britt, 'Common general practice presentations and publication frequency', *Australian Family Physician*, Vol. 42, Nos. 1/2, January/February 2013, pp. 65-8.

11 Sydney University Family Medicine Research Centre, 'General practice activity in Australia 2014-15'.

12 Westphalen, 'Occupational and environmental medicine in the Australian Defence Force'.

13 Royal Australian College of General Practitioners, 'Curriculum for Australian general practice: CS16 Core Skills Unit CS1.2: General practitioners use effective health education to promote health and wellbeing to empower patients', *Royal Australian College of General Practitioners* [website], available at <http://www.racgp.org.au/Education/Curriculum/CS16/CS1.2.1//promote-health-and-wellbeing> accessed 21 April 2017.

14 Royal Australian College of General Practitioners, 'Contextual Unit MM16 Military Medicine', *Royal Australian College of General Practitioners* [website], available at <http://www.racgp.org.au/download/Documents/Curriculum/2016/MM16-Military-medicine.pdf>; and Royal Australian College of General Practitioners, 'Contextual Unit OM16 Occupational Medicine', *Royal Australian College of General Practitioners* [website], available at <http://www.racgp.org.au/download/Documents/Curriculum/2016/Presentations-OM16-Occupational-medicine.pdf> both accessed 21 April 2017.

15 Personal communication at 2016 Australasian Military Medicine Conference.

16 Australian and New Zealand Society of Occupational Medicine Inc. [website], available at <http://www.anzsom.org.au/about/about-anzsom> accessed 21 April 2017.

17 Personal communication with AFOEM [Australasian Faculty of Occupational and Environmental Medicine] Defence Director of Training, 25 November 2016.

Cultural competence and linguistic capability in ADF human-intelligence source operations

Captain S, Australian Army

Cultural competence is a set of congruent behaviours, attitudes, and policies that come together in a system, agency or among professionals and enable that system, agency or those professions to work effectively in cross-cultural situations.

T.L. Cross *et al*, *Towards a culturally competent system of care*, National Institute of Justice: Washington DC, 1989

For some time, a range of government and non-government organisations have been acknowledging the importance of 'cultural competence' or 'cultural proficiency' in their service delivery and practitioner training. This has been particularly prominent in healthcare and social services, as well as law enforcement and the criminal justice system.

This article will argue that elements of cultural competence and related aspects such as effective linguist capability are integral to human intelligence in general, and military-related source

operations in particular. The article will then suggest how this can be better incorporated into both specialist and continuation training, and how linguist support to the capability can be enhanced to avoid cultural 'fouls' and missed collection opportunities.

As source operations are a human-intelligence discipline, it is explicit that human interaction is central to the capability. Throughout the selection, training, certification and employment of a military source operator (an individual trained to exploit information from a human source, most usually in an operational theatre), interpersonal skills are assessed and scrutinised. Psychological testing and observation of interpersonal interaction are used to ensure the right person has been chosen for a role which is critically dependent on understanding what is going on in the head of the person opposite them.

During the training of potential source operators, considerable scrutiny is placed on the exact

wording used during interaction with simulated sources. However, at present, almost all this scrutiny is conducted in a cultural and linguistic vacuum. With the exception of a short period of training in the use of an interpreter, all current training in the ADF is conducted between Australians and in English. This is continued during unit training, where training activities are almost exclusively conducted in a domestic context, with a simulated local source network.

Compare this to the actual conduct of source operations by the ADF. Almost exclusively, the gathering of human intelligence in an overseas theatre will be from sources who are foreign nationals, who either do not speak English or speak it as a second, third or fourth language. Less visible than the linguistic barrier will be their difference in world view. Understanding the motivation of a source is a critical component to effective human-intelligence operations. And, needless to say, the world view of a 42-year old father of three from Brisbane is substantially different to a counterpart from Kandahar, Dili, Mogadishu or Aleppo. Everything from sense of humour to honour, duty, loyalty and loss of face is subtly (or not so subtly) different when influenced by such factors as religion, educational levels, exposure to violence, and longstanding cultural norms.

At present, considerable effort is put into training to ensure that military source operators have the skills to pull the right strings when engaging with Australian role players. However, little preparation is given for re-tuning this skill-set to a source who may be Pashtun, Dinka, Arab or Melanesian. This cultural gap is currently addressed only by means of several pre-deployment 'culture briefs', which are largely untailored to source operations. Once in theatre, source operators learn 'on the job' and their most effective training in the local culture tends to be via the mistakes and missed opportunities of the first few months of their deployment. This is hardly ideal. Imagine a team of medical professionals deploying to an area with specific tropical diseases in the expectation that they would learn 'on the job'—so that after mistakes on the first dozen or so patients, they would begin effective treatment!

What is even more damaging and can delay the adaptive process for source operators is that they often have insufficient appreciation

of how significantly different the subtleties of human interaction are from culture to culture. In other words, they typically are unprepared for how people from different cultures respond to questions from others—and often in different ways about different things for different reasons. Psychologists are divided as to the extent of the impact of culture on such fundamental aspects of human interaction. But it is clear that the cultural gap can be huge.

Recent experience in Afghanistan starkly demonstrates this gap. When an Australian is offended by a comment or joke made by another soldier, their response—unlike what has happened several times with an Afghan soldier—would never be to kill the person he days earlier had considered a good friend. Shame, honour and personal goals can all be significantly different to what a 'Westerner' might expect. Hence, source operators need firstly to be aware that all preconceptions and templated solutions need to be reassessed for each deployment. Secondly, they need specific preparation for that environment so they are among the most culturally attuned personnel deployed. This is often the case by the end of their deployment. But it should be the case at the beginning as well, where lost collection opportunities and cultural 'fouls' tend to occur, as illustrated at Figure 1.
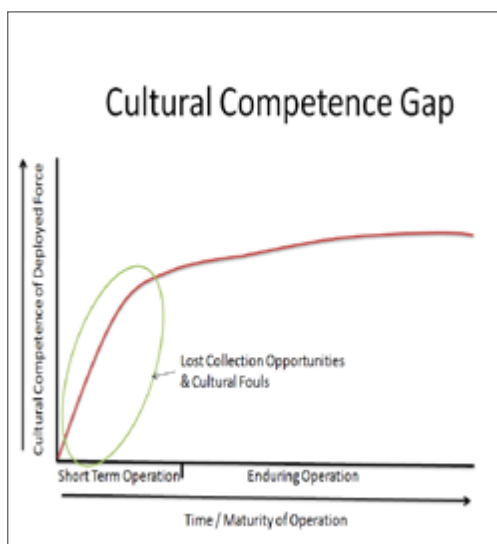

Figure 1: The propensity for lost opportunities and cultural 'fouls' to occur early in deployments

In addition to the issues of what is going on inside a source's head is the reality of what is coming out of their mouth. As mentioned earlier, source operator training gives particular attention to the exact language used by a source, scrutinising the language for ambiguity or lost meaning. Yet the availability and quality of interpreters on deployment can be so poor that the most basic question can readily be mangled into something with quite different implications.

Two major issues impact the availability of good linguist support. First is the need to have linguists or interpreters who are security vetted for the nature of the conversations being held. Second is the availability of linguist support in the specific language being used, including the correct dialect for that region and ethnic group. In an ideal world, a human-intelligence team would deploy with sufficient personnel trained in the local language, and to a standard high enough to replicate local language skills. In practice, this is highly unrealistic, even in regions in which Australia has been militarily involved for decades. As a Pashto linguist, the author can attest to the extreme challenges in teaching military personnel to speak a language which is so regional that even a native speaker from one province can barely understand someone from another.

The challenges in vetting local nationals to a sufficient standard are obvious in countries suffering prolonged instability, limited records and high levels of insurgent intimidation. The result is that field human-intelligence teams are typically forced to rely on limited numbers of contracted linguists provided by commercial companies, which usually source native speakers from diaspora populations in the Western world. Because of their lives in the West, these individuals can be vetted to a reasonable degree. Understandably also, these individuals are in high demand, and so are both expensive and few in numbers. The result is fatigued interpreters, notwithstanding that they often have extensive knowledge of a source network due to their high workload.

Nevertheless, these same interpreters, who tick the key boxes of vetting and language ability, may lack the necessary temperament or character. In human-intelligence operations, more than any other military activity, an interpreter must be in full unity with the individual they are working

for. In many cases, contracted interpreters are an excellent asset and are both hard working and capable. However, this is far from guaranteed. Complex conversational plans, concealed essential elements of friendly information and unspoken signals require a high level of synergy. A fatigued, arrogant or disinterested contracted interpreter, motivated only by a high wage, is unlikely to deliver this close cooperation.

So how does a small, specialised capability increase cultural competence and build a linguist support system which can assist with as yet unforeseen future operations?

Training cultural competence

Military source operator training needs to incorporate two distinct elements to achieve cultural competence. The first is to teach a generic understanding of the differences between cultures and the challenges this can produce in source operations. At present, this is usually delivered in an ad hoc manner via vignettes from the experiences of individual instructors. However, it should be formalised into a dedicated component of source operator training. It could, for example, be delivered as part of a pre-course study pack which required trainees to read historical cases of successful (and failed) source operations and the complexity of cross-cultural communication.

It could also be reinforced during training by amending slightly some role player parts to include certain cultural issues and requirements. For example, one serial could include an otherwise placid source taking offence over something very minor which then requires the trainee to apologise and identify how to rebuild rapport. This could be continued during further training, and elaborated with external presentations and study on relevant religious and cultural beliefs in likely areas for deployment. If the related security sensitivities could be addressed, it would also be invaluable to conduct training exercises in friendly countries to better incorporate and expose source operators to cultural differences.

A second element would be the delivery of effective pre-deployment cultural training to make human-intelligence team members among the most culturally attuned personnel on the deployment. This would need to include,

as a minimum, a study pack on generic cultural issues in that region, external lectures or engagement opportunities with diaspora communities in Australia (with suitable pretext), and a tailored reading list and appropriate funding to obtain study materials and books. By engaging with academic experts as well as appropriate analysts within Defence, a combination of experts could be utilised to brief and inform teams prior to deployment. This is every bit as relevant as reading into the reporting currently being produced in a respective theatre of operations, as it would provide the broader context in which that specific reporting is being produced.

Building adaptable linguist support

More complex would be the provision of appropriate and agile linguist support. The best way to achieve this is also one of the most difficult, that is, by developing military linguist resources tailored to human-intelligence operations. As it is not viable to maintain a large cadre of full-time linguists covering every possible language required, some risk must be taken in predicting which languages will be required. This prediction should look up to a decade into the future, which presents obvious problems in an unpredictable world.

However, it should be possible to produce a list of around half a dozen languages which reflect Australia's strategic collection priorities and anticipated areas of involvement. These languages should then form the basis for a two-tier approach to linguist capability. Following the example of the 2nd Commando Regiment, every source operator should be supported to develop their own basic language skills. This would require three things: direction, funding and specific time allocation for study.

Based on individual aptitude and operational requirements, each potential operator would be given a language to develop. They would then need to be adequately resourced by being provided access to high quality self-paced learning programs, such as the Rosetta Stone on-line language learning software which has been used so successfully by the British military. In addition, places on courses such as those offered by the

University of Queensland, or bespoke intensive courses using the Defence School of Languages could assist to deepen linguist ability.

Finally, dedicated periods of time would need to be ring-fenced to support learning, with operators held accountable for progressing their study in the allocated time. If, as a result of such training, Australia was able to deploy just two source operators to a new operational theatre with a basic understanding of the local language, it would prove of significant benefit to the quality of the human intelligence subsequently produced. The importance of language as a rapport-building tool is immeasurable. Even a limited vocabulary would allow the first rotation of intelligence-collection personnel to understand the local situation more quickly. It would also allow deployed source operators to quality-check their interpreters.

The suggested second tier of linguist support would be a cadre of dedicated ADF linguists possessing a high degree of fluency in one or more of the target languages. Existing linguists could be captured on a database for use by human-intelligence collection elements both on operations and in training (noting that language skills are already recorded on personnel records). In order to ensure these linguists were optimised to support such operations, a short course could be created to ensure they had a basic understanding of human-intelligence processes, requirements and considerations.

The inclusion of dedicated ADF linguists on exercises would also serve the double purpose of enhancing their ability to support source operations and provide training to source operators in working through interpreters. However, what would greatly enhance this capability is the targeted recruiting of a reservist linguist capability. Currently, linguist reservist capability is significantly undermanned and consists primarily of ex-Regular personnel. These unfilled Reserve positions could be filled with linguist support personnel recruited via University Regiments from students studying appropriate foreign languages. By advertising the financial benefits of having languages recognised in the ADF, appropriate candidates might also be enticed to join the Intelligence Corps and sit within the ADF's human-intelligence capability.

These suggested changes to both cultural training and linguist capability are small and relatively cheap by comparison to the cost of other intelligence-collection capabilities. They would, however, be significant in enabling an increase in the quality of human-intelligence reporting in the crucial early period of an ADF operation. The biggest barrier to their effective implementation is the current limitation in manpower and training time available within the ADF's human-intelligence capability. It would be necessary, therefore, to balance the importance of understanding (both literally and figuratively) the human terrain and the importance of other training that the ADF's human-intelligence resources are currently committed to.

As the world continues to be both unpredictable and volatile, it will remain vital for ADF commanders to appreciate the importance and complexities of human terrain as an aid to decision making. Human intelligence-related cultural and linguistic competence will continue to be a key factor in understanding complex environments across a range of operations from short-term humanitarian support to longer-term warlike operations.

Captain S has been an Intelligence Officer for over ten years and has served on multiple deployments to Afghanistan and Iraq. These have included a variety of human-intelligence related roles, including command of a Field HUMINT Team and as a Pashto-speaking Human Terrain Officer. He has also deployed in support of Special Operations elements, as well as a considerable period involved in mentoring and advising local partner forces. He has participated in numerous exercises in Europe and the US, as well as bilateral activities in Southeast Asia. He has a Masters degree in Conflict, Development and Security.

Review essay

Douglas MacArthur: American warrior

Reviewed by Emeritus Professor
David Horner, AM,
Australian National University

When General Douglas MacArthur arrived in Melbourne on 21 March 1942, Australia was at its lowest ebb. On 23 January, Japanese forces had seized Rabaul in New Britain and a thousand Australians had been captured. On 15 February, the Japanese had captured Singapore and a further 15,000 Australian troops had become prisoners-of-war. The Japanese advance seemed relentless. On 19 February, Japanese aircraft bombed Darwin and, over the following month, Australian forces in Java, Timor and Ambon surrendered. The Japanese landed on mainland New Guinea on 8 March. With the three divisions of the Australian Imperial Force still overseas, and with its small, weak navy and air force, Australia seemed open to Japanese invasion.

And then MacArthur arrived, to be welcomed by an excited crowd of between 4000 and 6000 Australians as his train pulled into Melbourne. A few days earlier, the US and Australian Governments had announced that MacArthur would be supreme commander of an Allied command, the Southwest Pacific Area, which would encompass Australia and the islands to the north. The *Brisbane Courier* observed that MacArthur's arrival 'was stirring news, the best news Australians have had for many a day'. Frank Forde, Deputy Prime Minister and Minister for the Army, who met MacArthur on the railway platform, commented that faced by the 'greatest catastrophe that could have happened', the country looked to America.

Five days later, MacArthur flew to Canberra to attend a dinner hosted by Prime Minister John Curtin and to meet the bipartisan Advisory War Council. As they left the meeting, MacArthur threw his arm over the Prime Minister's shoulder, promising him that 'we two, you and I, will see this thing through together…. You take care of the rear and I will handle the front'. From then, through to 1945, MacArthur became the dominant figure in Australia's conduct of the Second World War. Indeed, few figures who have spent

less than three years in this country have had such an impact on Australian life.

The publication of this latest biography of MacArthur by the American popular historian Arthur Herman provides an opportunity to reflect on the enduring importance of MacArthur to the defence of Australia in the Second World and to Australia's approach to the American alliance and to coalition warfare over the subsequent 70 years. Before considering these issues, however, one might reasonably ask whether there is anything more to say about MacArthur that has not already been said in the more than 50 biographies that have already appeared.

Herman argues that most of them fall into two categories: those by 'unrelenting critics' and those of 'unashamed adulation'. There are also general biographies, such as those by William Manchester (1978) and Geoffrey Perret (1996), as well as scholarly biographies such as the three-volume series by D. Clayton James. But Herman claims that 'it is time for a biography of MacArthur that gives this larger-than-life figure his full due by peeling back the layers of myth, both pro and con, and revealing the marrow of the man and his career'. Herman's sympathetic biography largely achieves its aim. Drawing on a large range of sources and recent scholarship, he provides an engaging and nicely paced account of MacArthur's life, examining both his personality and his military achievements.

One of the most interesting themes is MacArthur's interest in Pacific affairs and the way this was shaped by his father Arthur, a hero of the US Civil War and a long-serving officer in the US Army. As early as 1883, when Douglas was just three, Captain Arthur MacArthur had written a 44-page memorandum in which he argued that the US should seek to establish a vast commercial network in Asia. He thought it was inevitable that Russia and the US would meet in Asia. As Herman suggests, it was as if Arthur MacArthur 'could see in a crystal ball his son's and his army's agonies on the Korean Peninsula almost seventy years later'.

Commanding US forces in the Philippines at the beginning of the 20th century, Arthur MacArthur developed attitudes to Asian independence which were to colour his son's views. These were reinforced when, as a young officer, Douglas

(who had already served in the Philippines himself) accompanied his father on an eight-month tour of the key Asian countries and colonies. In all, Douglas MacArthur was to live for almost 13 years in the Philippines during war and peace. Then, from 1945 to 1951, he commanded the allied forces in Japan, during which he laid the foundation for a democratic Japan. With this background, as Herman reminds us, MacArthur warned John F. Kennedy not to get involved in Vietnam, adding that '[a]nyone who starts a land war in Asia ought to have his head examined'.

There was much more to the MacArthur story than his involvement with Asia. By the time he arrived in Australia in March 1942, he already had a long and distinguished military career. In the First World War, he was chief of staff of a division and commanded a brigade in action, winning many decorations for bravery. He was then Superintendent of the US Military Academy. By 1930, he was Chief of Staff of the US Army, serving under Presidents Hoover and Roosevelt, with whom he had significant differences. Later, he became military adviser to the Philippines government, during which time he retired from the American Army. He was recalled in July 1941 to command the US Army Forces in the Far East.

His command in the Philippines, once Japan entered the war in December 1941, was not successful. His air force was destroyed on the ground by Japanese air attacks, and his troops, who withdrew to the Bataan peninsula, were shortly to face a disaster exceeded only by that of the British at Singapore. He should have been relieved of his command, and it was perhaps only for political reasons that Roosevelt ordered him to Australia. His defeat in the Philippines rankled deeply within him.

MacArthur believed that it was his destiny to lead the Allies to victory in the Pacific, having vowed to the people of the Philippines, 'I shall return'. His US air commander in Australia in 1942, Lieutenant General George Brett, described him as 'a brilliant, temperamental egoist; a handsome man, who can be as charming as anyone who ever lived, or harshly indifferent to the needs and desires of those around him'.

MacArthur was a man of personal contradictions. As US Army Chief of Staff, he had kept a Eurasian mistress, while his mother, ignorant

of this arrangement, helped him with official entertainment. MacArthur bribed the mistress to leave town, for fear of his mother's wrath. He married for the second time while in the Philippines, and arrived in Australia with his wife, young son and amah. In January 1942, in the midst of his defensive campaign in the Philippines, the Filipino President Quezon secretly awarded him $500,000 (probably about $8 million today) as 'recompense and reward' from the Philippines people. Herman argues that MacArthur accepted the payment only because he never expected to live to spend it.

Yet for all his faults, MacArthur gained the confidence of the Australian Government, which hoped that his appointment would ensure American support. He harassed Washington for more troops and slowly put together his new command. General Sir Thomas Blamey was the sole Australian to be appointed as one of MacArthur's three immediate subordinates—he was given command of the Allied Land Forces. Australia provided most of the ground troops while the US provided the majority of the ships and aircraft, although the numbers were still relatively small. This was the time of the Battle of the Coral Sea. We need to remember that the US helped defend Australia in 1942 when Britain was unable to do so and Australia's forces were too weak by themselves to stop the Japanese advance.

Herman's account of MacArthur in Australia and his role in the New Guinea campaigns of 1942-43—the period of most interest to Australian readers —is the weakest part of his book. While living in Australia, first in Melbourne and then in Brisbane, MacArthur became the focus of public attention. His demands were fulfilled, his press communiqués provided the main source of military information, and Australian and American forces responded to his directions.

The campaign in Papua between July 1942 and January 1943 did not show MacArthur at his best. Questioning the fighting qualities of the poorly supplied Australian troops fighting on the Kokoda Trail, he asked Curtin to send Blamey to Port Moresby to take personal command. The Australians had in fact fought well but Blamey felt obliged to relieve the local Australian commander and, faced with MacArthur's demands for more speed, Blamey relieved two other

senior officers. For the final stages of the campaign, MacArthur moved to Port Moresby and, in dramatic fashion, told his American corps commander Lieutenant General Robert Eichelberger: 'If you don't take Buna, I want to hear that you are buried there!'. Eichelberger survived but many Australian and American soldiers died because of the need for a rapid victory.

By contrast with the Papuan campaign, the New Guinea offensives of 1943 were a brilliant orchestration of Australian and American sea, land and air forces. Australia provided the bulk of the ground forces until April 1944, after which the Americans bore the brunt of the fighting. As the Americans approached the Philippines, MacArthur promised Curtin that Australians would take part in the islands' recapture but that never came to pass. MacArthur was unwilling to allow the Australians to play a major role in the recovery of American territory.

In late 1944, MacArthur directed Blamey to use more forces to garrison the Japanese-held areas of New Britain, Bougainville and New Guinea than the Australian commander thought necessary. He also ordered Australian troops to land at Tarakan and at Brunei Bay, Borneo, in May and June 1945. Blamey opposed the final landing at Balikpapan in July but MacArthur insisted and the Australian Government acquiesced. In the emergency of 1942, Australia had little alternative but to accept Macarthur's leadership. But, by 1944, Australia should have realised that America's, or perhaps MacArthur's policies, were not necessarily the best for Australia.

Australia drew two important lessons from this experience. First, at the strategic level, there is no certainty that US and Australian interests are the same. In the future, Australia would need to work hard to have any influence over alliance strategy and, even then, would be unlikely to succeed. Whether that lesson was fully heeded with regard to the Vietnam War or the 2003 invasion of Iraq is open to debate. The second lesson was to ensure that in coalition operations, Australian commanders had the capacity to withdraw Australian forces if proposed operations might unnecessarily endanger Australian lives or were not in accord with Australian government policy. Such command arrangements have been in place in all of Australia's subsequent coalition wars, from Korea to Afghanistan and Iraq.

Herman could not be expected to deal with these specific issues but he fails to come to grips with the shortcomings of MacArthur's military campaign in 1942-43. The Australian official historian, Gavin Long, made considered judgments about MacArthur's performance in his book *MacArthur as military commander*. Herman dismisses Long's arguments simply on the basis that Long was an 'unrelenting critic' of MacArthur.

There is, of course much more to Herman's book than the New Guinea campaign, a testimony to the length of MacArthur's career, which in a military sense reached its high point with the amphibious landing at Inchon in Korea in September 1950. The following April, MacArthur was relieved of his command by President Truman, bringing to an end a military career of almost 52 years in uniform.

For a book that a generally provides a well-rounded, modern and thought-provoking account of arguably America's greatest soldier, it is unfortunate that it is marred by numerous mistakes, ranging from the slipshod to the laughable. I can only mention a few. George Marshall was not Secretary of Defense when the Inchon landing was being planned but was appointed soon after the landing in September 1950 (page 4). The Emperor Franz Josef was the uncle not the father of Franz Ferdinand, whose assassination triggered the First World War (p. 75). Arthur MacArthur died almost 50 not 60 years after the battle of Missionary Ridge (p. 75). Japan joined the First World War in 1914 not 1915 (p. 149). France capitulated in June not July 1940 (p. 286). The US Army general in the Philippines was Jonathan Wainwright not James (p. 296) or even Joseph (p. 329). MacArthur's B17 bombers could fly 2000 not 200 miles (p. 298). The 'veteran salt' Commander Bulkeley, who commanded the PT boats which spirited MacArthur away from Corregidor, was actually 30-year-old Lieutenant Bulkeley in 1941 (p. 305).

The errors become more numerous once MacArthur reached Australia. MacArthur made his renowned statement 'I shall return' at the South Australian town of Terowie not Adelaide (p. 419). Blamey commanded the Australian corps not a division in the Western Desert (p. 428). Admiral Grace was actually Admiral Crace (p. 434). MacArthur's naval commander in May 1942, Admiral Leary, was an American not an Australian (p. 435). MacArthur fired Leary in September 1942, not Hart as the book claims (p. 463), so Leary's successor, Carpender, was not present for the Battle of the Coral Sea in May as the book states (p. 439). The Central Bureau, MacArthur's crucial signals intelligence unit, was in Henry Street, Brisbane not Melbourne (p. 436). Laughably, Wau is not an island but a town some 50 kilometres inland in New Guinea and the Japanese never captured it as the book claims (p. 465). New Georgia is a thousand miles from Salamaua, New Guinea not one hundred (p. 483). The Japanese base at Wewak was 500 miles north-west not south of Dobodura (p. 484). Australians will be infuriated to learn that, according to the book, it was American not Australian troops who landed east (not north-east) of Lae and captured the New Guinea town in September 1943. Returning to my earlier theme, if an American author cannot get Australian military operations right, then Australians need to be wary of American strategic decision-makers.

The errors continue in the later chapters. General Yamashita did not 'mastermind' the capture of Manila in 1942, he was in Malaya (p. 530). Inchon is west not east of Seoul, the Korean capital (pages 4 and 728); but don't bother checking on the map because it does not appear on it. For that matter, the maps are particularly weak. The map of Australia (p. 424) shows the towns of Onslow and Albany but not the capital, Canberra, nor Melbourne, where MacArthur had his headquarters. The battle map of New Guinea (p. 443), including the Lae landing I referred to earlier, bears no relationship to what actually happened. The British brigade in Korea, which included an Australian battalion, was not part of the US X Corps on the east coast of the peninsula (p. 773). The fighting in Korea ended in July not March 1953 (p. 837). Finally, my good friend the distinguished American historian Ed Drea would be surprised to learn that he is now called Kenneth (pages 612 and 852).

Book reviews
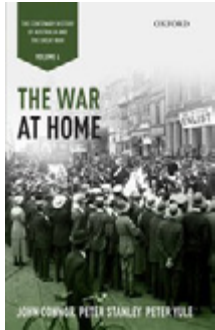
The war at home: the centenary history of Australia and the Great War, Volume 4

John Connor, Peter Stanley and Peter Yule
Oxford University Press: South Melbourne, 2015, 320 pages
ISBN: 978-0-1955-7678-8
$59.95

Reviewed by Colonel Gavin Keating, DSC, CSC, Australian Army

The war at home is part of Oxford University Press' recent *Centenary history of Australia and the Great War* series. Now is a timely opportunity, during a period when Australia remembers its participation in the Great War, for the current generation of historians to raise fresh questions and perspectives about this experience. As the late Jeffrey Grey, series editor, noted in his foreword, '[w]e are not telling a different story, but hopefully have told the story differently'.

The intent of this particular volume is to interpret the economic, political and social experiences of the Australians who remained at home during the conflict. In doing so, it seeks to address themes left untouched by Ernest Scott, who wrote *Australia during the war* as part of C.E.W. Beans' official history of the Great War. As Peter

Stanley highlights, the people who remained home (and the events and activities they participated in) 'have been largely overlooked in the war's historiography, which remains seriously skewed towards the drama of conflict'. While perhaps not as captivating as the chronology of past battles popular with some current writers, the book covers themes that arguably remain more relevant to modern Australia and its future.

Peter Yule's section on Australia's wartime economy notes that it was particularly vulnerable to the disruptions of global conflict. As a large resource exporter, with only an emerging industrial base, the country's economy was almost immediately influenced by disruptions to shipping commerce and the resulting shortages as Britain concentrated on maintaining its supply routes with closer parts of the Commonwealth. However, Australia's 'critically dangerous' export position was significantly stabilised in 1916, after Prime Minister W.M. (Billy) Hughes' visit to Britain, where he achieved spectacular success in negotiating a series of favourable trade deals with the British Government, particularly covering wheat and zinc.

In addressing the related shipping shortages, Hughes was able to apply pressure to the British allocation system by the secret purchase of 15 steamships, the existence of which was only revealed to his Imperial colleagues during a critical stage in his negotiations. Ironically, this success only served to reinforce Australia's role as a primary resource supplier to Britain, increasing the economy's vulnerability to the conditions that would later spark the Great Depression. Manufacturing stagnated during the war, in sharp contrast to Australia's experience during the Second World War. Australian industry provided only a small amount of the weapons and equipment required by the Australian Imperial Force. The weakness of the industrial base was best illustrated in the manufacture of artillery munitions. Despite concerted efforts early in the war, Australia produced only 15,000 shells of acceptable quality during the conflict—scarcely enough to supply more than a brief bombardment by Western Front standards.

Billy Hughes looms large in John Connor's section on Australian politics during the war. His relentless energy and iron will achieved considerable successes on the international stage but

divided his colleagues and substantially contributed to the split of the Australian Labor Party during the first of two conscription referendums. Connor describes these referendums as 'the most divisive events in Australian political history'. Both votes for conscription were narrowly defeated, with voter turnout for both higher than the 1917 federal election held in between. The causes of the defeats were complex but it is generally believed that voter class played a significant factor.

Hughes' machinations before the first vote, where he used the *War Precautions Act* to restrict anti-conscription coverage and attempted to use the same act to authorise polling officials to disqualify male voters who had not attended a compulsory call-up for military training just prior to the vote, showed him at his political worst. As Connor highlights, in light of the civil disturbances experienced in Canada and New Zealand after the successful introduction of conscription in those countries, it was perhaps best that Australia did not follow suit, regardless of the efficiency of such a system. Hughes' political manoeuvrings to remain Prime Minister in the face of considerable opposition after both referendums demonstrated the strength of his political cunning and ruthlessness. More positively, some of these same strengths helped Hughes to ensure Australia's strategic interests were addressed during his tenure on the Imperial War Cabinet in 1918 and subsequent participation in post-war peace negotiations.

In his section on society, Peter Stanley covers a range of different issues, many of which support the view of some commentators that the impact of the Great War on Australian society was 'essentially negative, reactionary and destructive of tolerance'. German Australians 'found that they swiftly became the subjects of a campaign of vilification unseen in Australian history, before or since'. The pressures of war hardened religious sectarianism, particularly given the prevailing majority Protestant view that Irish Australians were disloyal and did not support the war effort. The pressures of the conscription campaigns, and the rise of the Catholic Archbishop Daniel Mannix as a prominent opponent of conscription, only inflamed sectarian prejudices and moved them from purely religious matters into everyday life.

The *War Precautions Act*, passed without dissent in October 1914, gave the Government virtually unlimited powers over the Australian people, some of which were not always used wisely. The burden of sacrifice was not evenly spread across the country, creating new divisions in society and reinforcing older ones. While over 400,000 Australians volunteered to serve in the AIF, it is notable that two-thirds of eligible men did not enlist. Stanley notes that, contrary to popular belief, Australia's 60,000 war dead did not represent a higher proportion of the population than other nations (Australia's war dead represented 1.22% of the population, New Zealand 1.51%, Britain 1.6% and France 3.4%).

However, the grief associated with such casualties, the financial and psychological costs associated with caring for the 150,000 who were wounded (physically and mentally) and the lost human potential that these combined figures represented all impacted on the country in ways that were undoubtedly substantial but remain difficult to quantify. The arrival of Spanish influenza, brought into Australia by troops returning from the war, only heralded more suffering, with 12,000, mostly civilians, dying in 1919.

The authors generally conclude that the war severely damaged Australian society. Its impact on the economy left it 'anaemic and vulnerable'; politics became more bitter and 'torn by class rivalry, religious bigotry and the echoing taunts of the conscription campaigns'; and the 'optimistic, unified [and] progressive Australia that the world had so admired before' was arguably dead. Jeffrey Grey was somewhat more optimistic when assessing that '[t]he nation that emerged from [the war] was a more mature and aware entity, but that development came at a heavy human and social cost'. *The war at home* is a sobering reminder that the costs of world wars are borne by more than just their uniformed combatants, and last much longer than just the duration of hostilities—an important reminder as we remember those momentous events from over a century ago.

The AIF in battle: how the Australian Imperial Force fought 1914-1918

Jean Bou (ed.)
Melbourne University Press: Carlton, 2016,
328 pages
ISBN: 978-0-5228-6865-4
$49.99

Reviewed by Justin Chadwick

Jean Bou is one of Australia's eminent military historians, currently working at the Australian War Memorial. In *The AIF in battle*, he has brought together other military historians to contribute to this timely and important book that discusses and analyses key aspects of how the Australian Imperial Force (AIF) fought during World War 1.

Bou's introduction discusses the historiography of Australian military history and argues the need for a different approach. He notes that although much has been written on the actions of Australian troops during World War 1, particularly as part of centenary commemorations, most concentrate on specific battles, commanders or a particular Service. As Bou asserts, this 'amounts to a considerable edifice, but one that is somewhat fractured and spread out, in both space and time'.

This book attempts to investigate the AIF's evolution as a fighting force over the period of the war, demonstrating that the AIF that landed and fought at Gallipoli was a very different fighting force, with different equipment, tactics and command arrangements, from the one that was fighting at the end of 1918.

Each chapter of *The AIF in battle* looks at different aspects of the AIF. These include the infantry battalion, mounted warfare in Palestine, artillery on the Western Front, command, air power, mining operations, trench raiding, and concludes with three chapters on the AIF and its battles from 1916 to the hundred days of 1918.

What becomes apparent from these essays is that each explores the changes that the AIF went through. Some of these are well known, such as the difficult transitions in tactics that were costly in lives, particularly for the infantry. Less known are others such as the development of the Flying Corps, where many pilots and crew were killed by enemy fire or equipment failure.

Of particular interest is David Horner's discussion of higher command of the AIF and the degree to which Australian officers had to 'learn on the job'. Although some of the officers had experience commanding during the South African War, and some permanent officers had staff college qualifications, the majority had little higher-level command knowledge as Australia had never fielded a divisional command structure. This higher command discussion is lacking in many histories which tend to maintain the 'Bean tradition' where the Digger is the centrepiece of any conversation.

The AIF in battle is a timely and important book to add to the ever-expanding work on the AIF and its role during World War 1. Each chapter is well-written and informative, albeit a smattering of spelling errors detract from the reading. This book is important, given that so many of the centenary-related publications have been a reinforcement of existing narratives. *The AIF in battle* should serve as a touchstone for other historians to further progress a longitudinal approach to Australian military history by identifying the development of ideas and techniques over time.
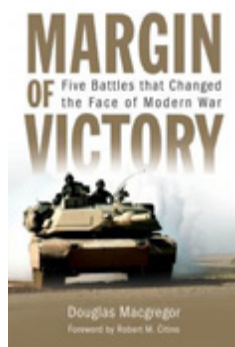
Margin of victory: five battles that changed the face of modern war

Douglas MacGregor
Naval Institute Press: Annapolis, 2016,
270 pages
ISBN: 978-1-6125-1996-8
US$34.95

Reviewed by John Donovan

Reading a book by retired US Army Colonel Douglas MacGregor is a challenging experience. It is not necessary, however, to agree fully with MacGregor to gain valuable insights from the research and analysis behind his proposals.

In this book, MacGregor studies five battles to glean lessons relevant to army reform in the 21st century. He differentiates between wars of decision, choice and observation, focusing particularly on wars of decision, and seeks reforms to ensure that the US is victorious in the first battle in such wars.

The first battle studied is Mons in 1914. MacGregor attributes British success during the retreat from Mons through Le Cateau largely to reforms implemented before 1912 by Richard Haldane, Secretary of State for War. Despite budget constraints, where priority was given to the Royal Navy, these reforms prepared the British Army (just) enough for a continental war. Resistance within the Army diminished the effect of the reforms but MacGregor notes that sufficient remained to provide a margin of victory when needed, despite deficiencies in British leadership.

The next study is on the Japanese capture of Shanghai in 1937. MacGregor introduces General Ugaki Kazushige, who in the 1920s attempted to move the Japanese Army from a focus on infantry numbers towards greater mobility and firepower. Reaction to Ugaki's proposals arose, however, and opposition was more successful, delaying many reforms until the 1940s. Shanghai was a battle between masses of infantry, with limited mobility and fire support. While Haldane had given the British Army a margin of victory in 1914, opposition to Ugaki's changes left the Japanese Army strong enough to prevail in individual battles but not able to win against China.

These first two case studies emphasise the need to implement reform before a war, as more immediate priorities might constrain implementation during one. In his next two case studies, MacGregor introduces command arrangements.

The third study, on the destruction of Germany's Army Group Centre in 1944, differentiates between German military reforms between the wars, which 'focused on marginal, tactical changes to … [a] … World War 1 army', and Soviet reforms implemented during the war, which focused on 'integrating and concentrating combat power … for strategic effect'. MacGregor also compares the polyglot German command system unfavourably with the integrated, joint Soviet system. The Soviet reforms were based on theoretical concepts developed in the 1930s but temporarily abandoned after Stalin's purge of the Red Army. They became the basis of the reconnaissance-strike complex of the 1980s.

The fourth study is on the Egyptian crossing of the Suez Canal during the 1973 Yom Kippur War. MacGregor compares Egyptian military reforms, implemented with deep understanding of Egyptian culture, with Israel, which learned incorrect lessons from earlier wars. The Egyptians specifically planned to counter known Israeli tactics. While the Israelis eventually prevailed by using manoeuvre, the victory was

costly, in part because Israeli supporting fire-power and infantry were not closely integrated with tanks. MacGregor considers that Israel's unified military command structure provided the necessary margin of victory.

MacGregor's final case study is the US Battle of 73 Easting, against Iraq in 1991. He sees the 1991 conflict as perhaps the ultimate expression of World War 1 tactics. He considers this war a lost opportunity to move 'beyond industrial-age warfare to … highly mobile, joint, integrated, aerospace and sensor dominated forces'. Instead, the US Services each fought their own wars, in their preferred manner. MacGregor notes that airpower was not able to defeat the Iraqi army in the field but did prepare the way for the ground attack. He criticises the failure to combine the air and ground efforts in an early joint operation, which might have produced a clear victory.

The final chapter is the core of the book. In it, MacGregor proposes a way forward for the US in the 21st century. He sees little use for light infantry (or even special forces) in conflicts with a peer or near-peer opponent, dismissing them as '[a]thleticism in uniform'. Rather, MacGregor favours fully mechanised ground forces, operating with air support as a strike/manoeuvre force under a joint and integrated command structure. Whether such a force is affordable by any nation other than an economic giant is a question for non-American readers to ponder.

One element of MacGregor's thesis that is relevant to Australia is defining the nation's 'core, existential interests'. MacGregor does not see nation-building/counterinsurgency in the Third World as a core interest for the US. Without US support, there also can be little realistic belief that these could be core functions for Australia.
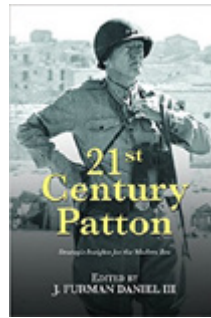
21st century Patton: strategic insights for the modern era

J. Furman Daniel III (ed.)
Naval Institute Press: Annapolis, 2016,
159 pages
ISBN: 978-1-6824-7063-3
US$24.95

Reviewed by Wing Commander Jo Brick, Royal Australian Air Force

Francis Ford Coppola's film, *Patton*, and George C. Scott's portrayal is so iconic that it is likely to cast a shadow over any discussion about General George Smith Patton, Jr—'old blood and guts'. Arguably, the film emphasises the eccentricities of the man—his intemperance and pomposity—and remains silent about the General's unwavering dedication to study, reflection and writing. Admittedly, these activities are not amenable to drawing the interest of a film audience, particularly where military action and drama are more viable alternatives.

Confining our understanding of the man to his depiction in Coppola's movie does a significant disservice to the study of leadership and professional military education. Patton's life and his dedication to the study of warfare provide many lessons for contemporary military professionals. There are myriad books on Patton, including Carlo D'Este's comprehensive biography, *Patton: a genius for war*. However, *21st century Patton* offers something more than a biographic account of the man. This book is part of the 21st Century Foundation series from the Naval

Institute Press, which aims to give 'modern perspective to the great strategists and military philosophers of the past, placing their writings, principles, and theories within modern discussions and debates'.

The study of Patton in this book demonstrates the futility of schism in leadership studies between those who believe that leaders are born and those who believe that leaders can be made. Patton's example makes clear that effective military leaders have certain traits that can be honed through education and training. He was unrelenting in his pursuit of excellence through his disciplined approach to physical fitness (he competed in the modern pentathlon in the Stockholm Olympics) and his dedicated study of military history. His focus and discipline contributed to the effectiveness of his self-education.

Patton was also able to take his extensive knowledge of military history, and his own personal experiences in training and warfare, to write persuasive articles that more than likely contributed to the development of military capability at the time. Patton's article on 'The form and use of the saber' distilled his thoughts on the utility of the straight-edged sword over the curved sword in cavalry charges. This ultimately led to the US Army's development of a straight-edged sword and Patton's appointment as 'Master of the Sword' and an instructor in swordsmanship at Fort Riley, Kansas in 1913. His other articles, 'Technology and war', and 'Refining the concept of mechanized war', demonstrated Patton's fascination with new technology and his ability to contextualise the relevance of new capabilities using lessons from history and through an appreciation of the current military environment.

Daniel has focused on Patton's intellect and character through a selection of his works as a demonstration of Patton's enduring relevance to discussions about military affairs and strategy. Daniel has selected a number of Patton's papers that highlight the main themes that underlie his writing—the importance of 'the warrior mindset' and leadership to military success; the intersection between history, culture, politics, technology and the military profession; the continuities in war and the impact of technology on the conduct of war; and the importance of critical thinking, education and training to complex problem solving.

While the book considers the evolution of Patton's writing and his thoughts on warfare and military capability, it was his consistent and enduring study of war that is the key lesson from this book. Patton's wife, Beatrice, wrote about his method of study and listed the key works that he annotated. Beatrice's essay, 'A soldier's reading', is the concluding chapter in the book but is perhaps best read first as an introduction to Patton's intellectual pursuits, his mindset and his writing.

Although Patton died 70 years ago, his story and his writings set an example for contemporary members of armed forces who want to call themselves truly 'professional'. Complexity is a central facet of all warfare, and demands that military professionals continuously learn through historical study or review of contemporary security issues to understand the political and cultural backdrop against which modern military operations may be conducted. Modern military institutions are replete with discussions about technology and platforms but, as Patton rightly highlighted, humans win wars—but only if they take the time to reflect and study the amorphous field that is 'war'.

The ministry of ungentlemanly warfare: Churchill's mavericks, plotting Hitler's defeat

Giles Milton
Hodder and Stoughton: London, 2016,
368 pages
ISBN: 978-1-4447-9895-1
$45

Reviewed by Jim Truscott

Although the World War 2 Special Operations Executive (SOE) was created and dissolved in secrecy, new research into archives has enabled this book to be published. While it was officially called SOE, it operated under the cover name of the Inter Services Research Bureau. This book also puts its history in context with the role of Brigadier Gubbins, who initially established Section D (Destruction) and who ultimately led the organisation as its Chief of Destruction. It is as much a biography of Gubbins as it is a short history of SOE.

Churchill coined the colloquial 'Ministry of Ungentlemanly Warfare' expression with SOE's task to set Europe ablaze. It was also Churchill who decided to bypass the Ministry of Supply and approve the clandestine and illegal building of weapons. Such a 'work outside the law' organisation and freelance approach to warfare could never fit with the conventional military. It is little wonder that the Ministry of Economic Warfare was placed in overall charge of guerrilla warfare, as it was not constrained by military rules, command structures and centralised barracks.

Gubbins and Jefferis (an engineer), both of whom had won Military Crosses in World War 1, started the organisation by producing the first ever instructional manuals in the history of the British Army to teach men how to wreak havoc on civilian targets with a small bag of explosives. *The art of guerrilla warfare*, *The partisan leaders handbook* and *How to use high explosives* were all about killing, incapacitating or maiming the maximum number of people. Their first task was to build a 3000-person home guerrilla army in the UK. They selected people who were polar explorers, mountaineers and oil prospectors: men who knew how to survive in a tough environment. In this way, the fabled Fairbairn and Sykes duo, who were experts in 'gutter killing', set up a killing school in Scotland. The fundamental principle was that irregular soldiers armed with nothing but homespun weaponry could wreak havoc.

Woman were also employed early on in SOE. Independent companies were formed to wage guerrilla warfare in Norway and the Commandos were later formed from the independent companies as specially trained hunter troops who could develop a reign of terror. Hundreds of saboteurs were trained and sent to multiple countries through use of Halifax and Lysander planes guaranteed by Churchill.

The book has strong focus on technology. The Limpet munition was initially designed in 1937 in a backyard workshop by a mechanic with parts from local shops, using condoms and aniseed balls as a timing device. The magnetic Limpet was a game changer in countering the German's naval expansion, and Hedgehog mortars were also later successful in destroying submarines. Churchill directly supported the development of the W-bomb (the Limpet was known as water bomb) and 1700 bombs were dropped to the Poles but it was all too late.

Limpet mines were subsequently used to destroy a power station in France supplying a submarine base. Another sticky bomb was developed to attack German tanks including by castrating the occupants. The attack on the Tirpitz dry dock was enabled by an L-delay fuse based on lead from Broken Hill. There were also exploding rats and self-detonating camel dung. The development of the hollow charge was another game changer leading to the PIAT and

beehive munition. The assassination of Heydrich in Czechoslovakia was enabled with a special grenade with biological agents.

Security and cover enabled SOE's country sections to dispatch agents and assassins into multiple countries. There were always months of intense training followed by radio silence when they were inserted. The issuing of death (cyanide) pills was a consistent theme. Not every operation was sophisticated, as 20 agents were actually sent to Poland prior to the invasion with consecutively numbered passports! The operation however did lead to the Enigma typewriter being obtained even before the war began.

Gubbins used pirate tactics with a raiding vessel in Spanish territory in West Africa and propaganda to deny British involvement. Blind parachuting was used to insert saboteurs and attack the railway line viaduct in Greece that supplied the Germans in North Africa. It was also timed to occur with Operation Torch. The destruction of the hydro plant in Norway was the greatest sabotage mission of World War 2. During the Normandy landings, the French Resistance cut some 1000 railways lines, more than the entire Air Force effort over the previous two months, and their hit-and-run tactics prevented a German tank division from counter attacking until after the beachhead had been established.

The book contains many themes that still resonate for the conduct of successful special operations today, including the need for a very senior person to be a sponsor to counter the antagonism of more conventional commanders, the need for funding channels outside normal appropriations and the leveraging of operatives with leading-edge technology. While SOE was not part of Australia's direct military history, this book is a useful compendium.

**AUSTRALIAN
DEFENCE FORCE**