AUSTRALIAN DEFENCE FORCE

Australian Defence Force JOURNAL

Journal of the Australian Profession of Arms

Issue No. 204, 2018

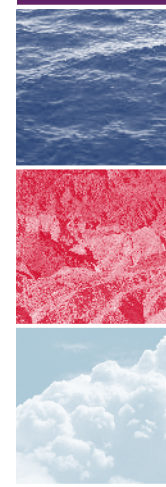


AUSTRALIAN
DEFENCE FORCE

Australian Defence Force
JOURNAL

Journal of the Australian Profession of Arms

Issue No. 204, 2018



Copyright

Disclaimer

National Library of Australia
ISSN 1444-7150

Published by Australian Defence College
PO Box 7917
CANBERRA BC ACT 2610
<http://www.defence.gov.au/adc/cdss/>

DPS: FEB018-18

Contents

Foreword

The role of the three Services is evolving with the development of our joint warfighting capabilities. With the formation of the Joint Capabilities Group in 2017, we now also possess a fourth Service; one that is charged with developing the joint capabilities that provide the connective force to achieve unity of effort across the Services, other elements of Government and our international partners.

This issue of the *Australian Defence Force Journal* features articles and commentaries on the evolving nature of air power within this joint force. The articles examine the fundamental importance of air power, within a joint or coalition construct, to achieving the security of our nation. Debate and discussion around the different challenges, disruptors and technological advancements faced by air power will only strengthen our ability to innovate and respond, and to work together effectively. These articles speak to a range of issues that all the Services will face in an integrated joint environment and contested global security environment.

Encouraging serving members of the ADF, Defence staff, academics and industry partners to pursue robust and sustained debates and conversations is essential to push the boundaries of knowledge critical to mastering our profession of arms. These conversations must be contextually driven, underpinned by a profound awareness of the geopolitical climate in which Australia operates, and the ADF will be engaged. This will drive adaption in the military and the national security environment, focusing our attention on the intellectual, moral, technological and human components that make war a complex national endeavour.

Over subsequent issues, I intend that the *Australian Defence Force Journal* will increase its engagement in the global professional military education dialogue through social media and a continued commitment to publishing high-quality professional discourse, research and scholarship. The *Australian Defence Force Journal* must be a beacon of advocacy for professional mastery to nurture the desire in military and civilian personnel to achieve individual and collective professional excellence.

Major General Mick Ryan, AM
Chair, *Australian Defence Force Journal*
Commander, Australian Defence College

My Fifth Generation

Wing Commander Chris McInnes, Royal Australian Air Force

The Lockheed Martin marketeers who came up with the 'fifth generation' slogan for the F-22 Raptor must be very pleased. The three Services of the ADF, led by the Royal Australian Air Force but joined more recently by the Royal Australian Navy and Australian Army, have embraced the goal of becoming a fifth-generation force. It has become the catchphrase of choice to differentiate where the Services are going from where the Services have been.

There is enormous value in having such a unifying theme and the habitual use of 'fifth generation' in formal presentations and informal discussion would suggest it has firmly taken root. However, despite its widespread use, the characteristics of a fifth-generation force remain ambiguous. Someone invariably asks 'what exactly is a fifth-generation force and how will we know when we get there? Come to think of it, what were generations one to four?'

These are valid questions. But I tend to think it has been quite useful not to have too much specificity so far. The absence of specifics has prompted each Service tribe, their myriad sub-tribes, and their partners to think what fifth generation means to them in their circumstances. But we are perhaps getting to the point where we need to put some flesh on the skeleton of what it means to be a fifth-generation force. This commentary is my attempt to do that, or at least prompt a discussion that will help people put meat on the bones of their own version of fifth generation.

In my view, a fifth-generation force is an organisational response to the Information Age and the characteristics of fifth-generation systems. 'Fifth generation' began as a technology descriptor, and assessments of that technology's impact on warfare have been used to derive a notion of fifth-generation warfare. The missing leg of the triad so far has been the organisational change necessary to operate fifth-generation technology most effectively to fight fifth-generation warfare. This appears to be, as Peter Layton points out in his article elsewhere in this *Journal*, a 'very

complicated way of war', so organisational considerations are important.

So as not to stray too far from the origins of the fifth-generation nomenclature, I have sought to characterise a fifth-generation force by adapting the characteristics that define fifth-generation systems. The characteristics of fifth-generation fighter aircraft are generally perceived to be stealth, manoeuvrability, advanced avionics, networked data fusion and multi-role capabilities.

Stealth becomes 'signature aware'. Stealth is the combination of low-observable technologies and signature-optimisation tactics. Similarly, in organisational terms, a signature-aware organisation matches an awareness of its physical, electromagnetic, virtual, resource and social signatures with practices and behaviours that optimise that signature for given scenarios. This is an extension of current practices, such as public affairs, operational security and lean business practices.

However, viewing the management of an organisation's footprint through the operational lens of signature management is an important response to the proliferation of sensors, scrutiny and threat vectors. A signature-aware organisation broadens the awareness and pursuit of signature-related objectives beyond specialist staff, such that all personnel can shape their actions and footprint in support of the desired outcome.

Manoeuvrability becomes 'adaptivity'. Fifth-generation aircraft manoeuvrability is linked to sustained high speeds, such as the F-22's super-cruise, and a capacity to rapidly change directions. I view adaptivity as a concept that incorporates organisational flexibility (range of change), agility (rate of change) and a readiness, if not eagerness, for the organisation to change. Most importantly, in adaptive organisations formal leaders do not direct change: they set the conditions that foster change from within the organisation.

I think we are relatively well postured for this requirement on an individual level. But I'd suggest there a few areas that need focus to shift from being an organisation with adaptive people to a genuinely adaptive organisation. A culture of delegated decision-making, distributed collaboration and a looser coupling to formal decision systems, such as risk and acquisition processes, are necessary to foster a more adaptive collective.

Formal decision systems are important instruments but they should inform and support while not constraining decision-making flexibility. The character of future warfare drives this requirement. Events are simply going to move too fast for the formal leader- and process-centric decision-making that mark our current organisational constructs. In an adaptive organisation, the worst thing you can do is not make a decision.

Advanced avionics becomes a 'human-machine team of teams'. Fifth-generation platforms use hardware and software to optimise the wetware of their crews. A fifth-generation force needs to be founded on human-on-the-loop human-machine team of teams to optimise decisions. This is a step beyond our current human-in-the-loop approach that supports and accelerates but rarely optimises decisions.

Rather than simply using computers to automate processes—the 'traffic lights' in so many command and control systems are essentially a digitised checklist—a fifth-generation force will exploit the processing power of computers to 'roll the dice' on possible options and present recommendations to a human decision-maker to apply human judgment.

The human-machine combination will be critical to the force's ability to deal with the uncertainty and chaos of a war that is potentially being fought on a pulse-to-pulse basis. And just as Facebook tells you which of your friends are interested in a particular event or page, the human-machine team would capitalise on machine processing to identify and alert teams that are working in a similar area or on a similar problem, fostering a 'team of teams' approach. Any conflict posing human-machine teams against humans-with-machines will be a very one-sided fight.

Networked data fusion becomes 'cognition-centric'. Fifth-generation aircraft have been designed with the collection, transmission and processing of information as their defining feature, to enhance the cognitive capacity of their crews. Initially, I called this characteristic 'information-centric' but I realised that this placed the value in the wrong place. 'Information-centric' portends an organisation that considers information as having value in itself.

A cognition-centric organisation, by contrast, views information only as a means to an end. Information is simultaneously terrain to be controlled and exploited, a weapon to be targeted and employed, and a supply to be husbanded and secured. The value of the information in all these perspectives is the impact it can have on the cognition and decisions of actors in the environment. Thus, a cognition-centric organisation values education (how to think) as much or more than training (what to think), so that the potential cognitive value of information can be realised.

A cognition-centric organisation recognises the futility of efforts to control information flows or 'the message' in an information-rich world and understands that the value of freer information flow in your own organisation, principally through better thinking and superior decisions, outweighs the associated costs. Starting from a basis of control-by-exception also allows the organisation to focus on securing only those things that absolutely must be protected.

Multi-role capabilities become 'outcomes-based'. Fifth-generation aircraft can shift from one role to another in single missions, and are less constrained by traditional 'type' roles such as fighters or bombers. A fifth-generation force shifts from effects-based or platform/system/domain/stovepipe-centric views of the organisation or operations to an outcomes-based view.

The shift from effects-based to outcomes-based thinking is similar to the move in Western planning doctrine from centre-of-gravity-oriented planning to objectives-oriented planning. Effects, like centres of gravity, are simply instruments to be used to achieve larger purposes but both of these grew larger and more intricate than the purpose for which they were conceived, namely achieving outcomes.

As our organisations avail themselves of a wider array of effects, coming from or through multiple domains, we need to recognise that outcomes may provide the only relatively constant, organising logic across time, space and organisation. Individual effects, their utility and how they are generated will be transient, and success may require the orchestration of a myriad effects in potentially non-repeatable combinations.

A consistent, organising logic based on outcomes will be a useful means of providing unity of effort and focus while fostering initiative among people who understand what the boss wants, and have a cunning plan to give her exactly that.

A fifth-generation force is not simply one that operates fifth-generation equipment or fights fifth-generation wars. It must also be a fifth-generation organisation. These are my five characteristics of a fifth-generation force. I'm not sure they are right and I'm quite certain some of you think they are wrong. I'd love to hear why.

Notes

1 This is a reproduction of a post published on *The Central Blue* blog on 3 December 2017 – see <http://centralblue.williamsfoundation.org.au/> It is reprinted with permission of the editors.

Contesting ideas: the importance of encouraging critical discussion to the future of Australian air power

Wing Commander Travis Hallen, Royal Australian Air Force

> Air power is not a static concept; rather it must be studied, reflected upon, debated, and challenged. As air-minded members of the profession of arms, Air Force personnel have a responsibility to participate in this contest of ideas. It is far, far better that we should respectfully engage in that contest than to hide our thoughts, only to find them wanting when it matters most.
>
> Air Marshal Leo Davies, Chief of Air Force, August 2017[1]

The effectiveness of Australian air power depends on the intellect of the airmen that employ it.[2] Such a statement may seem trite at first but the reality is that airmen spend precious little time developing their faculties for reasoning and critical thinking.

There are many reasons why critical thinking skills attract such little attention but, in my experience, one of the main factors is the heavy focus placed on technical mastery. There is a culturally engrained belief that knowledge of and proficiency in tactics, systems and processes are the key to effective air power. This belief has been enabled by the favourable technology gap that Western militaries have enjoyed since the end of World War 2.

Although technology will continue to play an important role in providing a qualitative edge over some adversaries, global military modernisation is reducing the West's accustomed technological advantage, making it increasingly difficult and costly to maintain a qualitative edge through technology alone. Success in the future battlespace will therefore rest on the development of innovative and creative approaches, and organisation of military force that will provide a capability advantage, albeit a transitory one, over future adversaries.

In the US, the development of the Obama-era 'Third Offset Strategy' was an explicit response to this emerging challenge. In outlining the

strategy, then-Deputy Secretary of Defense Bob Work placed critical and innovative thinking about new operational concepts and organisational structures on par with the development of new technologies in the pursuit of continued strategic advantage for the US military.[3] The situation is no different in Australia.

The Royal Australian Air Force (RAAF) is in the process of becoming one of the most technologically sophisticated air forces in the world. However, the introduction into service of the F-35A Lightning II, P-8A Poseidon and EA-18G Growler alone will not provide the RAAF with a capability edge over adversaries in the future battlespace. There is no question that the RAAF will rapidly adapt to the introduction of these and other new systems—and will no doubt achieve a high degree of technical mastery in the operation.

However, a high level of technical proficiency in the operation of systems will be a necessary though not sufficient condition for future success. Achieving and maintaining an advantage over our future adversaries will require innovative approaches to the way air power is developed, organised and employed. Innovative applications of air power require airmen who can understand context, anticipate change, and adapt the development and application of air power in response to complex operational challenges as they emerge.

The RAAF understands this; ongoing improvements to the professional military education and training system since 2009, and the creation of Plan JERICHO in 2015, reflect a commitment to developing professional mastery and innovative thinking at both the individual and organisational level. But there are limits to the current system. Air Force professional military education and training remains skewed towards providing knowledge, not developing critical thinking or argumentation skills.

As a result, the RAAF lacks effective mechanisms and processes to foster critical discussion within the organisation. Without these mechanisms in place, the RAAF cannot develop, let alone exploit, the diversity of thought and perspectives that provide the foundation for the innovative application of air power.

This is not to suggest that RAAF policies, doctrines and operational concepts are not regularly subjected to internal critique. Any visitor to a crew room or mess will undoubtedly hear robust and lively debate on various aspects of Air Force life and operations; however, these types of unstructured discussions add little to organisational and operational innovation. Mess debate rarely involves the in-depth analysis of key issues and validation of core assumptions that separates the airing of grievances from effective argumentation. Although useful as an outlet for voicing opinions on the organisation, these are not the forums for engaging in the contest of ideas that is needed.

Outlets for critical discussion and debate on Australian air power issues do exist; the *Australian Defence Force Journal* and the Air Power Development Centre's working paper series provide a means through which to draw attention to current and future air power issues. However, they are not often used by airmen; the length and academic style requirements for these publications have acted as a deterrent for many to contribute. What has been lacking, until recently, has been a less formal and less academically rigorous outlet for debate that is more accessible for those unwilling or unable to invest the significant time required to research and write a 3500+ word article conforming with academic writing standards.

A positive sign that progress is being made to create a more accessible means to engage in critical discussion has been the burgeoning of public online and digital forums addressing Australian defence issues over the past couple of years. Blogs such as Army's *The Cove* and the Williams Foundation's *The Central Blue,* podcasts like *The Dead Prussian* and actual physical forums such the 'Defence Entrepreneurs' Forum-Australia' have diversified the character and content of public debate on defence issues.[4]

The *Australian Defence Force Journal* has introduced an opinion/commentary section, simplifying requirements and thereby encouraging more serving members to articulate ideas and engage in critical discussions. Although these new outlets may not require strict adherence to academic strictures, they still place a premium on reasoning and expression, thereby promoting the development of effective argumentation skills.

The public nature of these forums does, however, limit their utility as a forum for candid critical

discussion on certain topics. Contributions must be unclassified, which severely limits the scope of the topics that can be discussed and the depth of the analysis and discussion that can be engaged in. Even if the topic is not of a classified nature, there are risks associated with the promotion of critical debate on organisational issues in public forums. The furore surrounding Captain Sally Williamson's opinion piece on 'Sex and War: a conversation Army has to have' that appeared on Army's *Land Power Forum* on 6 November 2017, and was removed on 15 November, highlights how the discussion of defence matters in public forums can be counterproductive.[5]

But learning how to engage in public discussion in an appropriate and constructive way is itself an important part of an educational process that aims to develop professional mastery in the workforce. We should not be shying away from the challenges of engaging in critical discussions in the public domain by creating unnecessarily burdensome hoops to be jumped through before publication. Instead, we should develop mechanisms and procedures that integrate educational, mentoring, editorial and approval roles into a simple and timely process to support members engaging in professional discussion on issues that matter to Air Force.

Ideally, this should be implemented at the local command level. Commanders have the responsibility to develop their workforce towards the attainment of professional mastery. This responsibility extends to fostering the development of critical thinking and argumentation skills necessary to engage in the contest of ideas that will play a key role in generating the creative and innovative approaches to air power needed to ensure a continued capability advantage into the future.

The creation of an ecosystem of outlets for the critical discourse is a necessary but not sufficient requirement for the promotion of a contest of ideas about the future of Australian air power. What is needed is for airmen to become active within the various forums, presenting their ideas, defending them, challenging those of others, and modifying their views based on the progress of the debate. This will require a cultural shift within Air Force that sees participation in the open debate on air power issues as not only permitted but actively encouraged, mentored and supported.

This is starting to occur at the higher level of the organisation as Chief of Air Force's comment quoted at the opening of this commentary attests. However, the risks associated with public comment generate an understandable reticence among some senior officers to encourage open debate. This needs to change.

Not every subject of interest to defence is amenable to public discussion, nor is every airman suited to engaging in public debate. However, we need to find a way to enable those with ideas to disseminate, have them tested, validated, adapted and, if appropriate, implemented in order to ensure that Australian air power is in the best possible position to success into the future.

This contest of ideas will be critical to ensuring that Air Force is ready and able to adapt to the dynamic and complex operating environments of the future. Accordingly, we must start to view the development of critical thinking skills and the fostering of critical discussions within Air Force as key components of our strategy to maintain a competitive advantage over future adversaries. We must not fear debate, we must encourage it.

Notes

1 'A Central Blue debrief with Air Marshal Leo Davies, AO, CSC – Chief of Air Force', *The Central Blue* [website]. 20 August 2017, available at <http://centralblue.williamsfoundation.org.au/a-central-blue-debrief-with-air-marshal-leo-davies-ao-csc-chief-of-air-force/> accessed 9 January 2018.

2 Air Force has adopted 'airmen' as a gender-neutral term covering both sexes.

3 Bob Work, 'National Defense University Convocation', speech to National Defense University, 5 August 2014, available at <https://www.defense.gov/News/Speeches/Article/605598> accessed 28 November 2017.

4 'The Cove', <https://www.cove.org.au>; 'The Central Blue', <http://centralblue.williamsfoundation.org.au>; 'The Dead Prussian', <http://www.thedeadprussian.com>; and 'DEF Australia', *Grounded Curiosity* [website], <https://groundedcuriosity.com/category/defaus> all accessed 9 January 2018.

5 Sam McPhee, 'Australian Army captain recommends soldiers should be visited on the front line by prostitutes to "relieve stress"', *Daily Mail* [website], 4 December 2017, available at <http://www.dailymail.co.uk/news/article-5141151/Australian-army-captain-says-prostitutes-allowed.html> accessed 9 January 2018.

Air power in the 21st century: enduring trends and uncertain futures

Dr Sanu Kainikara, Air Power Development Centre

> There is a tide in the affairs of men.
> Which, taken at the flood, leads on to fortune;
> Omitted, all the voyage of their life
> Is bound in shallows and in miseries.
> On such a full sea are we now afloat,
> And we must take the current when it serves,
> Or lose our ventures.
>
> William Shakespeare, *Julius Caesar,*
> Act 4, Scene 3, 218-24

Introduction

The past few decades have seen the acceptance of a new calculus in the role that air power can—and will—play in the future security environment. This is the result of fundamental shifts in the character and conduct of war and the technology-aided ability of air power to rapidly adapt to emerging situations. Wars or conflicts that have been fought over the past half century have all been irregular in character even if the intensity, tempo and spread have been as much as, and at times more than, what could be termed high-intensity war.

The conduct of such wars defies an accurate description and therefore the term irregular warfare, meaning other than conventional wars, has been used. The unique combination of evolving capabilities, new operational concepts and technological opportunities has created a situation where air power has been able to overcome rapid changes in the character and conduct of war.

Even though it was conducted nearly 30 years ago, Operation DESERT STORM is undeniably a watershed moment in thinking about air power. From the enormous success of that operation in 1991, air power has been continually, and at times rapidly, evolving to an extent that some analysts have termed an 'evolutionary revolution'.[1]

This evolution of air power is still a work in progress and, therefore, the enduring trends in air power and its future perspectives are interminably

intertwined. The developments of the past few decades not only entrench the enduring trends in the application of air power but also have significant implications for the future of air power.

Enduring trends

There is no doubt that the classic roles of air power will be enduring. Changes that will take place will only be in terms of the conduct of these roles. Air superiority, long taken for granted by the surface forces of Western nations, will still be a pre-requisite for all operations to succeed. Strike operations that are time-sensitive and delivered with accuracy, discrimination and proportionality to create the necessary effect will continue to be the primary contribution of capable air power.

Responsive and adequate airlift, both for the transport of men and materiel as well as for the insertion, sustainment and extraction of Special Forces, has proven to be a battle-winning capability. Airborne intelligence, surveillance and reconnaissance (ISR) envelopes the battle space, providing information to decision-makers across the chain of command that ensures decision-superiority for the engaged forces. These roles are enduring.

The trend in the development of air power is towards making these roles more effective. For example, the enhanced range of air-to-air weapons that now reach beyond visual and sensor range automatically increases the 'air superiority bubble' that can be provided; strike capabilities have become much more accurate and responsive, cutting down the time in delivering a strike; airlift too has become faster while delivering more in one lift; and the sensor horizons of ISR assets have moved further away and become more discerning.

These trends ensure that air power is more responsive, accurate and reaches out to touch things much farther afield in a speedier manner than ever before. While these are salutary developments, the fact remains that the evolution of air power has plateaued in the past few decades. No doubt further refinements in its application will continue to be sought and achieved but air power has 'matured' as an instrument of national power projection.

Air power has always been acknowledged as being technology-enabled. However, the key to the maturation of air power has been technology-integration, rather than being purely 'enabled', mostly in the more advanced air forces of the world. The rate at which technologies and related concepts are introduced and assimilated, especially the expanding information technology, opens new opportunities for the application of air power in an increasingly innovative manner.

At the tactical level, computing, sensing and data compression will continue to change the way in which air power is applied. Further, innovations already combine different aspects of finding, fixing, tracking and neutralising a target in one platform, increasing the reliability of this process and clearly reducing the targeting cycle time. At the operational level, air power can now create the desired effects with absolute assurance and minimum collateral damage. At the strategic level, national security has become completely reliant on rapid power projection and mobility provided by air power.[2]

Since most technology-integrated air forces are inherently professional, acceptance of new technologies should not pose any difficulties. However, the new technologies that are being accepted only make the established trends in air power more entrenched, and normally do not create quantum changes in capability. They remain enduring trends in the application of air power.

Uncertain futures

In the past few decades, air power has been at the vanguard of the application of military power, especially by the more developed nations of the world. This trend is unlikely to change because of a number of factors, the most important being the question of adequate attrition tolerance, or the lack of it, because of casualty aversion in the Western world.

Air power with its promise of low casualty, at least to own forces, becomes the weapon of choice in all conflicts other than wars of necessity. Further, in all future conflicts where air power is at the vanguard, it will be required to undertake the entire range of missions that it has been fulfilling so far. In effect, even though the capabilities

will get sharpened, there will not be any tangible change to the application of air power.

The characteristics of the air environment vis-à-vis the pursuit of control of the air has always dominated the development, employment and efficacy of air power—and it will continue to define air power development. In this context, the air environment is characterised as permissive or benign, contested or denied.

In the past 50 or so years, Western nations with adequate air power have not had to operate in any other but a permissive air environment, never having to really fight to obtain control of the air. While this situation has brought in a sense of complacency, the future may not be the same. A benign air environment could become contested very rapidly, and the threats that will emerge could lead to a denied air environment. Successful air operations could become difficult at best.

The challenges that the changed air environment will present will in turn create unprecedented conceptual and technological innovation. The awareness of the possibility of the air environment changing from benign to a denied state has influenced the development of air power capabilities and already created the first 'system of systems' concept. In this concept, the air power capabilities that may have been resident in separate airborne platforms are combined in one 'system' that may not be a single platform but a group that functions as one system.

Uninhabited aerial vehicles on ISR missions, operating in conjunction with 4.5-generation strike aircraft provide an early example of this development. It is envisaged that the system of systems approach will culminate in making air power a seamless web that will not expose its vulnerabilities but will be able to dominate contested or even denied air spaces successfully. However, these developments are more applicable to improving the efficiency of operations and are not radically different in the fundamental concept of the application of air power.

Step-change functions. Only a step-change function in the capability will bring about changes to the manner in which air power is generated, sustained and employed. There are two such functions that are being developed in the realm of air power—the uninhabited aerial vehicle and artificial intelligence (AI). The uninhabited aerial vehicle, and its armed derivative (uninhabited combat aerial vehicles [UCAV]), are already operational realities—and are being perfected in their employment.

Both UCAV and AI, if and when fully incorporated into the concept of air power—meaning incorporated into the development, application and sustainment activities, will change the realities of air power as perceived today. The future of air power will be shaped by these two emerging capabilities and, since the full envelope of their capabilities is yet unknown, the future is unpredictable and therefore uncertain.

Uninhabited combat aerial vehicles

The UCAV and its employment has matured to a level that they are now routinely used to strike and neutralise time-sensitive targets, especially in the context of irregular wars. The UCAV must be seen as an uninhabited system, since it combines ISR and strike capabilities of air power in a single platform.

The ability of UAVs to loiter at will for a long period of time, removed from the constraints of human endurance, is optimally merged with precision-strike capabilities to create a system that is potent and verging on the cusp of omnipotence. This development can be considered a step-change function that has altered the application of air power. Long-term surveillance that can be buttressed by near real-time kinetic response is now available to decision-makers through the employment of the UCAV system.

While the UCAV systems have clearly indicated the future possibilities, they continue to function with a 'human-in-the-loop', even though the human is not physically located within the body of the vehicle.[3] Even more important is the fact that the decision to launch a lethal weapon is always taken by a human being within the mission-control cycle.

Although technology exists to ensure fully autonomous operations, it has not been incorporated into systems that apply lethal force, for a variety of reasons such as ethics, morality and international law. Therefore, the UCAV system sits in a

half-way point between traditional strikes from inhabited platforms and the concept of complete autonomy in the weapon release function.

Operationally, UCAVs have already proven their efficacy repeatedly. However, their unrestricted employment as an instrument of military power remains a vexed topic. A number of unresolved issues and challenges continue to inhibit their use, even as UCAVs are being employed almost in a routine fashion in on-going conflicts in the Middle-East and South Asia. The first and perhaps the most contentious challenge is the legal status of the UCAV operators vis-à-vis the laws of armed conflict.

The complexity is increased because a number of UCAV operators are civilians who are dealt with in a different manner to uniformed soldiers within the purview of the law. The other issues that challenge the employment of UCAVs are resource related—the cost-benefit analysis of their use; asset requirement to ensure adequacy of availability and the cost escalation thereof; survivability in contested air spaces; and the cost escalation per unit system which make them anything but expendable. However, these are not show-stoppers and can be addressed at the politico-military level.

UCAV systems, with the assurance of having a human-in-the-loop in the decision-cycle, have proven to be effective in irregular wars where the air environment if benign. However, a basic question needs to be answered before these systems can be fully absorbed into the force structure to create a tangible step-change function. Will the conventional air forces of the world be fighting irregular wars in a benign or permissive air environment for the foreseeable future? If the answer is no, which seems to be the right answer, then the efficacy of UCAVs will have to re-evaluated in terms of cost-effectiveness and legal permissibility of the manner of their employment.

The developmental thrust of UCAVs will be influenced by the context of future wars, their characteristics and conduct. Currently, UCAVs have an ambiguous status, especially in smaller air forces, of a combat system that is 'good to have' rather than a 'must have' asset. Since there are moral and ethical 'doubts' associated with uninhabited systems, only a visionary approach to the concept of their employment will be able to balance their capability in relation to other air power systems.

Artificial intelligence and autonomy

The concept of autonomy in weapon release brings forward the question of the employment of AI in warfighting functions. In this article, the discussion will be restricted to the utilisation of AI in the application of air power. The employment of UCAVs has created a number of challenges to the military forces, mainly in the area of legal, moral and ethical considerations. Into this somewhat muddied atmosphere, the question of AI has been introduced.

Viewed in an unbiased manner, future concepts of operations and emerging employment opportunities that combine UCAVs and AI into a single system point towards a step-change function in the application of air power. However, both have to be considered individually before the practicalities of their combined employment can be studied.

Defining AI is considered an impossibility, since it is an absolutely nuanced entity and means different things in different circumstances. In a military air power context, AI could be generically explained as the 'intelligence' introduced into a 'robot'—the term robot denoting any machine capable of perambulation and conducting its own activities and regardless of the domain manner—to ensure that it functions in an autonomous manner with no human input for the full span of an independent mission. From a purely scientific feasibility point of view, autonomous operation is already a reality.

Even though autonomous capability has been repeatedly demonstrated, and AI has reached close to being a human-like capability in some contexts, the employment of a UCAV-AI combination for the application of lethal force brings out discernible challenges. These challenges are not technological but conceptual and mental. Irrespective of the challenges to the employment of AI, its introduction into the decision-making cycle is considered possible in the not too distant future.

The challenges to UCAV-AI becoming operational are mainly human in nature. The lack of trust in AI, exacerbated by the fear of a 'wrong' decision being made with disastrous consequences; the inherent human tendency to resist change; and the apprehension of not being in control, compounded by the inherent human need to maintain superiority over machines, individually and in combination, inhibit the unrestricted use of AI.

Stemming from the purely cognitive human element of trust, there is also a clearly visible political unwillingness to give complete freedom of operation to fully automated combat vehicles. This reluctance is particularly visible when the mission involves engaging an adversary with the application of lethal force at the discretion of the machine-AI combination. For some inexplicable reason, this reluctance is reinforced when the combination is part of air power.

In some respects, the fear of collateral damage from a UCAV-AI combination could be at the source of this hesitancy to give full autonomy to AI-controlled UCAVs. Considering the challenges, mostly originating in human reluctance to trust, it would seem that fully autonomous application of lethal air power is still a faraway dream. However, technical capability exists to achieve this step-change function.

It is difficult to predict the timeframe within which the UCAV-AI combination will find its niche in air power. With its maturation, air power will transcend another invisible step in being the power projection capability of choice. There is no doubt that an AI-capable UCAV, able to make weapon release decisions without a human-in-the-loop, will be fielded at the operational and tactical levels of war sooner rather than later. The acceptance of such a situation will be incremental and will start in the not too distant future.

The impact of artificial intelligence on air power

When the political and military strategic leadership accept the efficacy and the necessity of permitting the UCAV-AI system operate in a fully autonomous mode, there will be visible and long-lasting changes in the force structure of the air force, in the conduct and characteristics of war, and a necessary revision of the concepts of operations to achieve strategic objectives.

However, a number of questions will need to be answered satisfactorily before the UCAV-AI system can be made fully operational. Is there a role for humans in this system while the mission is in progress? Should there be a built-in monitoring system that has a human-in-the-loop to exercise a 'veto' if necessary? And, if so, can the system be considered truly autonomous? These questions are at the conceptual level of what constitutes autonomy.

If the issues of autonomy are overcome, the real impact of AI on the development and application of air power will become apparent through answering a series of questions. How will an autonomous system affect the philosophical level doctrine and the strategy of air power? Will the changes to strategy manifest as necessary changes to force structure and capability development? What changes will have to be incorporated in the ability of a force to generate and sustain air power? The answers to these questions will lead to more challenges and issues that will have to ameliorated before autonomous systems will be able to deliver on its promise.

Air power is poised to plunge into a great unknown. The situation is reminiscent of the time between 1918 and 1935, when a large number of theories regarding air power were developed, based on conjecture and buttressed by some wishful thinking. Such flights of fancy were unavoidable, since there was no explicit experience to base the development of theories and concepts. Today, there is no background experience to base the concepts regarding the employment of the UCAV-AI system. The maturing of the system's operational capability will mean charting a course into the unknown.

Artificial intelligence and focal points

The foundations of a force that generates and employs air power, more often than not an air force, is encompassed in four focal points—concepts for its employment; capabilities to operationalise the concepts; an organisation that provides the framework for employing the force; and people who make it possible. Any change

in the strategic framework of the force, irrespective of the reason for making that change, will also alter the relative balance between the focal points. It is critical to ensure that all changes to the equilibrium of the four focal points are carried out in such way as to retain the flexibility and efficiency of the force.

Air power delivered by a combination of machine and AI is the future. It is the step-change function that will elevate air power to the next level of competence. However, unlike the many evolutionary changes that have influenced the improvements in the application of air power, this step-change will involve a major resetting of the four focal points of an air force.

The unhindered acceptance of AI and autonomous mission-capable aerial vehicles will bring about a quantum change in the generation and application of air power at the strategic level. Changes at the strategic level to the focal points will obviously have a cascading effect on the conduct of an air campaign. On the other hand, at the operational level, the major roles of air power are unlikely to change, although they will be conducted with much lesser ambiguity and in a more responsive manner. The tactical level actions will remain almost the same but will once again be more responsive in the creation of the necessary effects.

The impact of unrestricted use of AI and the ensuing autonomous systems will manifest on the concept of operations and the four cardinal roles of air power. The necessity to have control of the air for autonomous systems to operate will pose a challenge to the UCAV-AI system. Their utility in the air superiority campaign and employment in a dedicated air combat role will change the manner in which control of the air is obtained.

In the extremely complex mission profiles that constitute an air superiority campaign, autonomous systems will need to be integrated minutely into the overall picture. This will require a complete overhaul of the existing command and control capabilities. In turn, the command and control infrastructure will have to be revamped to include far-reaching changes from the strategic to the tactical levels. Only after these changes have been instituted should the concept of operations be altered.

Similarly, the concept of strike will also undergo a transition with UCAV-AI systems becoming operational. There can be a 'launch-and-forget' capability that will stay airborne till the objectives are met, and also systems that can be kept in 'hiding' for long durations to track and then neutralise the target at the opportune time. However, this capability would yield better results when employed in irregular wars rather than in conventional high-intensity conflicts.

The more intriguing concept is that of a gradual shift towards an inhabited 'mother ship' controlling a number of semi-autonomous vehicles in all the major roles of air power. The changes will start to be effected at the lowest tactical level and only move to the strategic level at a very slow pace.

The concepts of operations will obviously have to adapt to an altered command and control system that will be unable to exercise the 'veto' option after a mission has been launched. This situation will have far-reaching significance and consequences, since the decision-cycle will be automated, and in a sense irretrievable, after mission launch. Since the concepts will have to be altered, it will automatically impinge on the capability development cycle.

The current cycle is long drawn. It is also cumbersome for nations that do not have indigenous industrial capability to produce air power systems. While the induction of AI and autonomous systems will also suffer from the same drawback, the manner in which information technology is evolving gives hope that the availability of AI and autonomy will not be as difficult as the more sophisticated earlier generation air power technology.

Capability development to support the concepts of operations will invariable lead to the need to analyse and alter the force structure. An air force of calibre should at all times be going through the process of force structure review to fine-tune and adjust the existing structure. This will depend on the organisation of the force, which provides the framework for the generation of air power of the required calibre and quantity.

An air force with a rigid organisation will find it difficult to create the necessary agility to identify, accept and apply AI and operationalise the

concepts of autonomous operations. Air forces are known for their flexibility, which must not be confined to operational and tactical levels of functioning but must be anchored at the strategic level of conceptual evolution of capability and command and control.

The key to force-wide flexibility is the people who continue to be the critical link in a chain that can be as long or as short as required, depending on the context of the application of air power. This factor itself is the flexibility of air power, in a strategically holistic manner. Air forces will have to take a broom to the current or traditional processes of selection, training and employment of their personnel. The ethos of an air force is influenced by the past.

All fighting forces glorify their past and base the present and future, to a certain extent, on the achievements of the past. With the step-change that AI and autonomy brings to the force, there has to be a clean and visible break from the past. This is not to suggest that the past is to be forgotten but that the new paradigm of the employment of air power surpasses anything that has been done in the past. At least in this case, the past is incapable of pointing the way forward correctly. A new horizon is looming and it will be failing force that does not understand this reality.

AI and entrenched autonomy in mission control will change concepts, capabilities, organisation and the people of the air force. Failure to make the necessary changes, failure to adopt to the emerging future, and failure to jettison the baggage of the past, individually and collectively, will lead to the failure of the force.

Conclusion

It is good to be able to state that air power is at the dawn of yet another glorious era. It is also good to be able to analyse and ponder the changes that today seem to be merely visible at the far away horizon, for this provides an opportunity to fathom the far-reaching consequences that come with step-change functions in the application of air power. Air forces, the primary generators of air power, are on the cusp of such a momentous change.

The technology-dependence of air power will continue to increase. The corollary is that technology will also become more resource intensive. The situation will require nations, and air forces, to maintain a balance between resource availability, allocation and the capabilities necessary to generate air power. The progress of air power through the acceptance of a step-change function, brought about by the combination of UCAVs and AI, may not be an assured possibility for a number of air forces.

However, that is the way of the future, there is no denying it. Not accepting the writing on the wall will only lead to abject failure of an air force when called upon by the nation to deliver security—an unacceptable state of affairs.

Sanu Kainikara is the Air Power Strategist at the RAAF's Air Power Development Centre. He is an Adjunct Professor at the University of New South Wales and the inaugural Distinguished Fellow at the Institute for Regional Security. He is the author of numerous papers on international politics, national security issues and security strategy.

Professor Kainikara is a former fighter pilot of the Indian Air Force, and held various command and staff appointments. He is a recipient of the Air Force Cross. He is a Qualified Flying Instructor, and a graduate of the Fighter Weapons School and the Defence Services Staff College, as well as the College of Air Warfare. Professor Kainikara holds two Bachelor degrees, a Master of Arts in Defence and Strategic Studies from the University of Madras, and his PhD in International Politics was awarded by the University of Adelaide.

Notes

1 Frederick L. Frostic, 'The New Calculus: the future of air power in light of its growing qualitative edge', in Richard P. Hallion (ed.), *Air Power confronts an unstable world*, Brassey's: London, 1997, p. 203.

2 David A. Deptula, 'The future of air power', in John Andreass Olson (ed.), *Global Air Power*, Potomac Books: Washington DC, 2011, p. 411.

3 Sanu Kainikara, *The Cassandra Effect*, Vij Books: New Delhi, 2016, p. 58.

Fifth-generation air warfare

Group Captain Peter Layton, Royal Australian Air Force

The Royal Australian Air Force (and Australia's Navy and Army) is embracing the vision of a fifth-generation future.[1] Originating as a company marketing slogan, the 'fifth generation' expression has evolved into a useful, catch-all term—a simple buzzword—encompassing several important concepts. At its core, 'fifth generation' is about how we conceive waging tomorrow's wars.

Fifth-generation warfare draws on the concepts of John Boyd, a fighter pilot turned strategic thinker, who developed his energy maneuverability theories of dogfighting into the so-called 'OODA loop'. For Boyd, winning at any level of war requires working the 'observation, orientation, decision and action' sequence faster than an adversary. With this, the adversary's reactions to friendly force initiatives will always lag, becoming less and less appropriate to the battle as it evolves.

While seemingly reminiscent of Liddell-Hart, Boyd went beyond such earlier thinking in stressing that the crucial aspect to attaining the requisite superiority in OODA loop speed is rapid orientation. Success lies in building an accurate image of the battlespace more rapidly than the opponent.[2] Situational awareness is the *sine qua non* of victory—a notion military aviators have turned into a mantra.

The process of converting Boyd's 1980s ideas into today's reality has been a somewhat protracted one. This article initially explores the principal approaches on which contemporary fifth-generation air warfare rests, with the second section extending this to discuss some of the practical difficulties in actually implementing this enticing vision. The final section looks at the application of fifth-generation air warfare to battle network and hybrid wars. Together, these two conflict types illuminate some of the

fundamental warfighting issues associated with fifth-generation air warfare.

Fifth-generation air warfare thinking

Fifth-generation air warfare may be considered as comprising four parts: a network, a 'combat cloud' operational concept, a multi-domain focus and a fusion warfare construct. In some respects, the order of these parts reflects the sequence in which they have developed and been incorporated into the overarching fifth-generation idea.

The network

In the fifth-generation air warfare concept, military forces are systems; they are not monolithic entities but are instead composed of many different, interacting parts. This notion of dynamic interaction is key as it means that the system as a whole is more than the sum of its parts. What the system does and how it performs cannot be understood by simply examining each part in isolation. The system can only be comprehended in its totality. This idea has been extended up and down the vertical axis so that complicated organisations like military forces are now seen as being composed of 'systems of systems'. Lower-level systems are embedded within progressively larger systems.

In the age of information technology, the system idea has been made tangible with the building of computer networks of varying scales and intricacy. Originally platform-centric, computing is now network-centric with the worldwide web and countless numbers of intranets and extranets. In the late 1990s, the US armed forces seized upon these developments in information technology, applied them to military operations and popularised the term 'network-centric warfare'.

Today's fifth-generation air warfare concepts incorporate network-centric thinking, with networks seen as comprising four generic elements:[3]

1. **An information grid.** The entry requirement for fifth-generation air warfare is a high-performance information grid. The information grid is a 'network of networks', consisting of communications paths, computational nodes, operating systems and information management applications which enable computing and communications across the battlespace.
2. **A sensing grid.** Sensing grids are composed of individual nodes that scan the battlespace to detect, track and identify targets. The information from the sensing grid is distributed across a force through the connectivity and computing capabilities of the information grid.
3. **An effects grid.** 'Shooters' form the effects grid, engaging targets based on sensor grid information distributed across the communications grid. The 'shooters' aim to create desired effects and can be quite diverse, including manned and unmanned aircraft, surface-to-air missile systems, electronic jammers and cyber systems.
4. **A command grid.** The command grid is principally the province of human decision-makers in involving their perceptions and problem-solving skills. This grid could also include knowledge-based, artificial intelligence software applications that act as command advisers able to recommend courses of actions.

Conceptually, the information, sensing, effect and command virtual grids overlay the operational theatre. The various force elements, from individuals to single platforms to battle groups, are then interacting nodes on the grids; each node can receive, act on, or pass forward data provided from the various grids as appropriate.

The operation of the grids can be visualised using the OODA loop. The sensing grid observes, the information grid orients (through disseminating information), the command grid decides, and the effects grid acts. To achieve a mission, the four grids must all interact and exchange information.

'Combat cloud'

The grid construct is simply an abstraction until turned into a meaningful operational concept. In this, the grid enhances distributed air operations in a particular manner that has been termed the 'combat cloud'.[4] The term derives

from commercially developed 'cloud' computing, where users can exchange information with a virtual cloud, pulling down data and applications as necessary, and adding information others may find useful. A combat cloud created by advanced information technology can bring several tactical benefits.

Firstly, situational awareness is considerably improved. With all aircraft and surface-based systems connected through data-links and able to exchange real-time information, all involved will have the 'big picture'. All involved will know where the hostile aircraft and systems across the battlespace are located, as well as their type and mission profile.

Secondly, the combat cloud makes long-range engagements more practical. Using the data pulled from the combat cloud, friendly aircraft will be able to engage hostile aircraft at extended ranges, well before they near friendly forces, enhancing own force survivability. Greater situational awareness will also allow long-range surprise engagements of hostile aircraft from unexpected directions, allowing friendly forces to gain significant tactical advantages.

Thirdly, with a high-quality distributed air picture, no single aircraft or surface-based system is critical to mission success and so the loss of one input is not catastrophic. The more numerous the aircraft involved, the more detailed, comprehensive and wide-area the air picture developed, and the greater the overall redundancy.

Lastly, the cloud concept allows good use to be made of the different capabilities offered by different platforms. The cloud should be conceived as comprising multiple diverse elements, not simply identical elements; it is heterogeneous not homogeneous. In some respects, the information grid then allows all elements involved to possess the capabilities of all the participants—not just their own individual platform capabilities.

Multi-domain battle

The network-centric idea and the combat cloud construct can be extended beyond the air domain into the other domains of land, sea, air, space and cyber. The resultant multi-domain battle concept then breaks the battlespace up into domains, rather than into Service components as some joint doctrines do.[5]

The key idea animating multi-domain battle is cross-domain synergy; the use of armed force across two or more domains to achieve an operational advantage. The synergy comes when the employment of different domain capabilities produces an effect greater than the sum of their individual effects. Acting in a complementary manner—rather than an additive one—each capability enhances the effectiveness of the whole while lessening the vulnerabilities of each platform individually.[6] Importantly, in using closely synchronised cross-domain synergy, the multi-domain battle concept aims to create and then exploit limited duration windows of opportunity, where friendly forces have the operational advantage and can manoeuvre freely.

In air-land operations in Europe during the Second World War, all sides tried to use air domain forces to pin the enemy down while land domain forces attacked on narrow fronts, aiming to drive deep into hostile territory. Without air domain pressure, an adversary could easily reposition forces to counter the friendly force thrusts but, with air pressure, as soon as adversary forces broke cover and tried to move they became subject to air attack. The enemy was on the horns of a dilemma: remain hidden from air attack and survive but then be destroyed by land attack. The importance of friendly force close synchronisation is manifest.

Fusion warfare

With the creation of large cross-domain networks with diverse sensors, there are concerns that there is now a greater volume of information collected on the battlefield than can be analysed. The solution is seen as fusion warfare. The 'fusion' adjective relates to using improved analytics that fuse data from numerous disparate sensors into a single common picture for decision-makers at the tactical and operational levels of war. The data is not just overlaid but rather carefully combined to give weapons quality tracking information and combat identification—attributes critical to the combat cloud construct.[7]

The fusion process though is just a means to the warfighting end. Future adversaries will also fight using sophisticated multi-domain networks. The fusion warfare idea is to make friendly force decision-making faster so that it stays within the

enemy's OODA loop cycle. In the OODA loop, time is the key variable that determines success or failure. Fusion warfare seeks to compress the time needed to analyse the considerable amount of data continuously collected so friendly forces can have an asymmetric advantage through making well-informed decisions faster.

Fusion warfare allows command and control systems to more effectively manage the increasing volume of information. However, there are growing concerns that adversaries may physically attack the centralised command centres involved or isolate them from the battlefield using cyber and electronic warfare means. The centralised command centre has become a worrying single point of failure.

Fusion warfare offers a partial solution in allowing a move away from the tenet of centralised control and decentralised execution that has long guided air operations. New technologies now make possible a 'centralised command, distributed control, and decentralised execution' construct. Control of air assets could be passed to lower-level commanders as part of making a more agile, flexible and survivable command and control system. Distributed control is seen as allowing collaboration between commanders and operational units in near-real time, leading to a greater focus on solving tactical problems rather than platform tasking.[8]

The fifth-generation air warfare concept involves the combination of network-centric thinking, the combat cloud, multi-domain battle and fusion warfare. As such, this is an intrinsically complicated way of war. Getting the concept to work either in peacetime or operationally is no easy task.

Making fifth-generation air warfare happen

Undertaking fifth-generation air warfare requires moving data around 'system of systems' networks. There are accordingly two crucial elements: data and connectivity. In terms of data, this must be of an adequate quality that decision-makers can use to take action. In terms of connectivity, this must both connect large numbers of diverse nodes and be sufficiently robust to function during stressful military operations. Neither are simple tasks.

Data

Fifth-generation air warfare is data hungry. The 'hunger' of command centres for useful data is readily apparent when considering multi-domain battle and fusion warfare. Less apparent perhaps is that individual fifth-generation air warfare platforms are also heavily data reliant. Major General Jeff Harrigian, when director of the US Air Force's F-35 Integration Office, noted that modern stealth aircraft are 'some of the most data-dependent machines in the US inventory, and require significant amounts of information in order to operate at their best'.[9]

Such aircraft need electronic order of battle data that includes the characteristics and electronic signatures of systems likely to be encountered while on operations. This data is used both to allow mission planning that optimises aircraft survivability, as well as to allow aircraft systems to be able to identify friendly, neutral and adversary systems when airborne.

Without this data, the 'big picture' of the battlespace provided to the aircrew may be inaccurate, incomplete and dangerously misleading. The aircraft can detect targets but, without accurate data, the identity of the targets will remain uncertain, making using beyond-visual range air-to-air missiles risky. If mission data files do not reflect the real world accurately on every sortie, aircrews may launch long-range weapons against incorrectly identified electronic blips, meaning that friendly, neutral or civilian aircraft may be endangered.

Ideally, mission data files should be updated before each sortie to ensure optimum combat effectiveness and aircraft survivability, albeit this is inherently complicated. In broad terms, the process involves extensive support by advanced in-theatre intelligence, surveillance and reconnaissance systems that collect the electronic order of battle data necessary, teams of skilled analysts to make sense of and filter this raw data, unimpeded communication links to carry this information back to the distant software support laboratories, on-call skilled software teams able to quickly translate the evolving tactical circumstances into mission data files and then retransmission to the operational area to load onto each stealth aircraft before every sortie.

Several implications arise from this cycle. Firstly, it is important to have highly specialised electronic data collector systems in-service, albeit these are expensive to acquire and maintain. Secondly, building up a detailed electronic order of battle across a region takes considerable time. Collector systems may be gathering data for years before an operational need arises, as many military emitters may only transmit at rare times for short periods.

Thirdly, the inherent difficulties of collecting data across all potential operational areas suggest that electronic order of battle sharing arrangements with allies takes on a new importance. Fourthly, the faster paced the conflict being waged, the more problematic meeting the mission data file cycle's time updating requirements may become. Lastly, in the most difficult conflicts—those that involve a peer adversary—the whole mission data file cycle may be attacked both physically and virtually.

The problems in the mission data file updating cycle mainly apply to what might be called 'background information' that details the electronic environment within which a military force is operating. There is also another kind of information required. Military command and control systems need to have timely information on the activities within the background environment that friendly, neutral and adversary civil and military entities are undertaking. As noted in multi-domain warfare, this information is needed across the land, sea, air, space and cyber domains.

Unlike parametric data, which might be important at the individual item of equipment level, 'activity information' is most important at the group level. Accordingly, for command and control systems, the information desired is more 'pattern of activity' data. Such activity information might be termed 'foreground data' and, for this, 'big data' is becoming increasingly important.[10]

Big data is defined as 'extremely large data sets that may be analysed computationally to reveal patterns, trends, and associations, especially relating to human behaviour and interactions'.[11] Big data's elements, colloquially termed 'the three Vs', are ever-larger Volumes of data; a growing Variety of sources (old, new and open source) and increasing Velocity with continually greater data flows.

Given these factors, the analytic approach of intelligence organisations has shifted from looking for specific kinds of adversary activity to looking for changes in the normal pattern of activity. The big data analytic approach can be visualised in four phases.

In the initial phase, a high volume and variety of data from multiple diverse sources across time and space is collected, meta-tagged and placed into an information 'cloud'. In the second phase, analysts use software applications to manipulate, visualise and synthesise the data in the cloud, leveraging the relationships between the different data elements.

The third phase involves building situation-specific software tools that can use the filtered pattern data to clarify the kind of activity underway and what this means in terms of future adversary actions. The fourth phase involves a partnership between the data analysts, the collection systems and the operational users. Operational users are no longer just consumers of intelligence information but rather collaborators in its creation.

The concepts of combat cloud, multi-domain warfare and fusion warfare all drive towards being able to make decisions faster than an adversary—to get inside the adversary OODA loop across multiple domains. The big data analytic framework offers a potential way to achieve this.

Connectivity

Without adequate connectivity between the various network nodes, fifth-generation air warfare would fail. Fused sensor information needs to flow at high speed across and between the various platforms and command and control nodes involved, often via intricate communication architectures featuring voice, video, data and imagery transmissions. In this, the key issues are building the network and—given this is a military network—its robustness.

Fifth-generation air warfare requires all the participating nodes to be connected via data-links of varying capacities and capabilities. The archetypal data-link for airborne application is Link 16, fitted to many ADF aircraft, ships and command and control centres. Link 16 has some shortcomings, including in providing only

line-of-sight linkages, and so is used in conjunction with several other types of data-links. The different data-links connect and exchange digital information through optimised gateways, albeit this introduces complications, vulnerabilities and inefficiencies.

Modern stealth aircraft have been developed in a manner that creates data-link connectivity problems. Such aircraft have Link 16 but, when emitting the transmissions, may be detectable by hostile electronic surveillance systems and the aircraft targeted. Accordingly, stealth aircraft use special low probability of intercept (LPI) data-links that, at the moment, are much harder to detect.

These LPI data-links are proprietary systems and cannot link with those used by most other types of aircraft, including other different types of stealth aircraft. To overcome this, special gateways are being developed that can connect the LPI data-links (and other data-link types) to the Link 16 network. In Exercise Jericho Dawn 16-3, undertaken at Puckapunyal in 2016, a gateway hosted on a Grumman Gulfstream business jet successfully linked RAAF fighters, combat support aircraft and Army helicopters.[12]

Sharing data-linked information has some implications during coalition operations. The combat cloud construct involves everybody on the network contributing to the 'big picture' and making tactical decisions based on it. In this, there is an implicit assumption that the picture is accurate. If, however, one nation's forces engage a civilian target because the data provided to the combat cloud by another country's sensors was in error, who is responsible? Will governments be comfortable authorising their nation's forces to launch weapons based on multi-domain network data of uncertain origin and veracity?

The inherently complicated nature of fifth-generation air warfare, with its considerable data processing and information sharing, raises concerns about whether future kill chains can be clear, unambiguous and sovereign. Devising national rules of engagement appropriate to fifth-generation air warfare will present real difficulties.

Fifth-generation air warfare is an enticing vision but its practical implementation is not easy, especially in the face of adversary action. Considerable effort is required to create decision-quality data and then establish the robust connectivity needed to support combat cloud, multi-domain battle and fusion warfare concepts. Making sure that fifth-generation warfare is not overly fragile requires significant preparation before an operation commences, and substantial support during it.

Waging fifth-generation air wars

Fifth-generation air warfare is an operational employment concept rather than a strategy in the conventional understanding. A strategy aims to bring about a particular context-specific political outcome but the fifth-generation air warfare concept is instead a broad, generic 'way of war'. An understanding of its application to wars might be gained by discussing two different conflict types: battle-network wars and hybrid wars.

Battle-network wars

Battle-network wars involve two networks fighting each other.[13] Such wars might occur between near-peer adversaries that both employ advanced information technology and use similar military doctrines. In combat, both sides would try to maintain the integrity of their own network while attacking the hostile one. In this, the focus would not be on simply destroying individual force elements in attrition style battles but rather in attacking the interaction between the network nodes.

The aim would be to disrupt the network on which the adversary relies to wage war through fragmenting it. With mutual support through the network lost, individual hostile force elements could be defeated in detail as necessary. Friendly forces could mass through using the network while adversary forces could not.

One of the first battle networks was the British air defence system that defeated the Luftwaffe in the 1940 Battle of Britain. In retrospect, the Luftwaffe, in trying to gain air superiority to allow a seaborne invasion of Britain, should have concentrated its attack on the Royal Air Force's Chain Home radar stations, the network's sensing grid. Instead, the Luftwaffe attempted

to destroy the much more numerous fighter aircraft, the effects grid, for which the radar warning information was critical. The Luftwaffe focused on destroying platforms, rather than conceptualising the British multi-domain air defences as a network and designing an attack to prevent the interaction between the radars and fighters, and fragment the overall network.

A future air war with both sides using fifth-generation air warfare concepts would see two very complicated, opposing socio-technical structures being directed and fought by military commanders. At the operational level, the battle would probably not involve a series of discrete steps, with large force manoeuvres carefully choreographed and sequenced to progressively lead to the desired outcome. Instead, strategic results would be achieved through the steady accumulation of small tactical successes. The combined effect of these multiple actions occurring in time and space would ultimately fragment and defeat the opposing network.

This high-level outline suggests important considerations for commanders preparing their battle networks for conflict. The networks need to be of a sufficiently large scale appropriate to the commander's plan of attack. They should be designed to operate in a decentralised manner, with no single key node or critical points of failure. Across the envisaged operational area, the networks need to be robust, with an adequate level of redundancy built-in so they can continue functioning while being attacked.

This highlights an intrinsic weakness in that units that transmit as part of a battle network will probably quickly reveal their position to the opposing network, with an attack likely to follow, albeit it may take some time to mount. To counter this, readily deployable air units—able to access numerous permanent and transitory air bases—may be able to employ 'shell game' tactics and be hard to pin down.

Battle networks though are interactive and, as friendly forces take action, so the hostile network will respond. Historical analyses of earlier battle-network wars suggest that the pace of the move-countermove cycle progressively accelerates as each side learns and becomes more effective. Eventually, the pace gets so rapid that one side is either unable to keep up and fails, or instead tries to outflank the adversary attacks by manoeuvring cross domain and forcing the competition into a different regime.

A battle-network war though, as it speeds up, might turn into a war of rapid attrition with the losing side the one that runs out of equipment and skilled people first. Battle-network wars might be attrition 'slugfests'.

There is an even darker future possible. A network-battle war might have two phases. The initial phase might involve a fast and furious exchange of blows that expends the small number of high-technology platforms and systems immediately at hand. The second phase then may involve a drawn-out period of 'broken back' warfare, where warfighting regresses and simpler, more-quickly manufactured weapons are used to continue the clash. During this phase, both sides would be trying to reconstitute their battle-network forces as quickly as they can so as to win the war before the other side can similarly return to full operational capability. Such a battle-network war might be quite protracted and very costly in blood and treasure.

Hybrid wars

There are other types of conflicts that are not characterised by a symmetrical, network-on-network battle. Some of these modes of conflict may be chosen by adversaries so as to limit the effectiveness of the defender's high-technology battle network. One potential mode is hybrid wars.

Hybrid wars are waged using a variety of dissimilar actors: state, non-state, sub-state and highly-motivated individuals. The sensing grids of battle networks are usually designed to detect the signatures of conventional military forces. The grids will accordingly have difficulty discerning the other actors intermingled amongst the society in which the conflict is being waged.

Attributing specific actions to particular actors may become very difficult, inhibiting effective responses. Moreover, the effects grid is also usually designed to engage military units operating away from concentrations from civilians. Hybrid actors, even when detected, may be too close to civilians to be engaged in the manner the defending battle network has been designed for.

In recent years, hybrid wars have been waged using non-state and sub-state actors to quickly seize areas that can then be occupied by conventional military forces able to readily defend them. The advantage of using state and sub-state actors initially is to avoid detection, as battle-network sensing grids are usually looking for conventional military force movements. A prompt response by others is then prevented; they are simply presented with a fait accompli, shifting the onus to fire first onto the defenders.

In a hybrid conflict, the sensing grid would likely need to be restructured to make greater use of non-traditional information resources, such as social media and open sources. The use of non-state and sub-state forces is most likely to be discerned on these first. Broadening the sources in this way plays to a key fifth-generation strength: 'big data'.

As discussed earlier, big data techniques assess large volumes of information flowing at high velocities from various sources—the three 'Vs'—to determine changes in the normal pattern of activity. However, to find these changes, the friendly sensing grid needs to be collecting appropriate background information for a period of time before. In this, the data analytic software and applications in use will also need to be optimised to be able to use the detected changes to forecast the adversary force's future activity.

Hybrid war also impacts the information grid. Non-state and sub-state actors might generally be thought of as possessing inadequate technology or professional skills to exploit or interfere with the communications flowing across the information grid. In hybrid war, however, the state party may well supply its associated non-state and sub-state actors with processed exploited information and, at times, specialist equipment.

Such exploitation, for example, may allow the non-state and sub-state actors to use social media or mobile phones to contact the defending state forces at the individual level to threaten or coerce them immediately before attacks begin. In terms of interference, jammers or cyber assets safe from attack by virtue of being located in the distant homeland might degrade the information grid at critical times. Such interference may be made more effective by providing local non-state and sub-state actors with simple, optimised equipment able to be placed near battle-network nodes.

While there are numerous difficulties in fighting a hybrid war using battle networks, there are some advantages beyond that noted concerning big data. After the initial use of non-state and sub-state actors, the pace of the conflict is likely to slow. The initiative may then pass to the defenders. There may be time to arrange set-piece battles that realise cross-domain synergy and make best use of multi-domain manoeuvre. Multi-domain battle and fusion warfare may be complicated. However, the slower pace of hybrid war may assist making carefully sequenced multi-domain parallel attacks.

There are some further possible advantages. In a hybrid war, an adversary will be aware of the possibility of vertical escalation and will work to keep hidden some information about adversary military forces and, in particular, electronic signatures. Accordingly, friendly force mission data files and electronic order of battle information will probably remain valid significantly longer, easing reconnaissance and software reprogramming tasks. Moreover, non-state and sub-state units may make use of commercial equipment that can be readily jammed, exploited or have false data inserted. There may be significant opportunities for cyber-attacks.

The two different types of war help reveal the complexities in waging fifth-generation air warfare. Its network nature, in particular, influences the manner in which such wars can be undertaken. The symmetrical battle-network war is the most complicated and fastest paced. In contrast, the slower pace of symmetrical hybrid war type might allow friendly fifth-generation air warfare systems to progressively evolve to better meet emerging operational circumstances. This cuts both ways of course. The adversary hybrid forces also then have more time to adapt and introduce effective countermeasures.

Conclusion

From the discussion, it is apparent that the fifth-generation air warfare concept is a complicated one that is both a distinct way of warfighting and noticeably different to traditional approaches. In this, the concept's theory of

victory is clear: operational success is achieved through gaining relative superiority in battlespace understanding through the timely development and sharing of useful information across heterogeneous, geographically dispersed, digital networks.

This theory is unlikely to change. Rather, the fifth-generation air warfare idea is more likely to evolve through technological refinement than major conceptual shifts. In this, there are several caveats that should be borne in mind.

Firstly, the fifth-generation warfare idea relates to what Edward Luttwak termed 'the technical dimension of strategy'.[14] Technology influences how we fight wars, however, there is more to winning than technology. Leading-edge technology was insufficient in itself to prevail in the Vietnam, Iraq and Afghanistan wars—and fifth-generation warfare so far does not appear any different.

Secondly, the article generally neglects software—in terms of the code that makes digital technology function. Suffice to say, software matters make fifth-generation warfare even more complicated, possibly by an order of magnitude.[15]

Thirdly, in being inherently complicated, it may seem that the fifth-generation concept could be incompatible with the nature of war, a social activity dominated by chaos, uncertainty, friction and chance. At least in hybrid wars, it seems these worries are unjustified, if earlier comments about advanced technology being necessary but not in itself sufficient are accepted. Multi-domain battle and other fifth-generation warfare aspects are being combat proven in Iraq in operations against Islamic State.[16]

The concept's appropriateness to near-peer warfare, however, still needs confirmation. A very complicated approach to making war may prove too complicated if opposed by technologies optimised to defeat it. For example, if an adversary can cut most data-links for an extended period, would this invalidate the overall fifth-generation warfare concept?

Lastly, the whole fifth-generation idea rests on trust between all network participants. Within national armed forces, there may be some elements that would rather not share information. Submariners at times are an example of this; they prefer for their vessels to operate alone and not inform others of their presence. Trust also becomes a further issue when conducting coalition operations where concerns range from releasing sensitive tactical information to matters related to defence industrial base issues.

In reality, in most conflicts, the most common situation might be 'balkanised' networks, where some nodes are disregarded leaving others to potentially fight their own separate wars. Such an approach significantly undercuts the logic of fifth-generation warfare.

Fifth-generation warfare usefully integrates network-centric warfare, combat cloud, multi-domain battle and fusion warfare concepts. These are all important ideas that in fifth-generation warfare do not exist individually but rather function together as a 'system of systems', where the whole is greater than the parts. In this, fifth-generation warfare is an evolving way of war; new elements and novel innovations may yet be incorporated. It is an area that remains a work in progress.

Group Captain Peter Layton is a reservist with extensive aviation and defence experience. For his work at the Pentagon on force structure matters, he was awarded the US Secretary of Defense's Exceptional Public Service Medal. He has a doctorate from the University of NSW on grand strategy and has taught on the topic at Eisenhower College at the US National Defense University. For his academic work, he was awarded a Fellowship to the European University Institute. He is a Visiting Fellow at the Griffith Asia Institute at Griffith University.

Notes

1 Brendan Nicholson, 'F-35 will be regional game changer, says RAAF chief', *The Strategist* [website], 12 May 2017, available at <https://www.aspistrategist.org.au/f-35-will-regional-game-changer-says-raaf-chief/> accessed 7 December 2017; Tim Barrett, 'A 5th generation Royal Australian Navy', *The Strategist* [website], 26 November 2015, available at <https://www.aspistrategist.org.au/a-5th-generation-royal-australian-navy/> accessed 7 December 2017; and Brendan Nicholson, 'Angus Campbell: turning a 3rd generation Army into a 5th generation force', *The Strategist* [website], 30 June 2017, available at <https://www.aspistrategist.org.au/angus-campbell-turning-3rd-generation-army-5th-generation-force/> accessed 7 December 2017.

2 David S. Fafok, 'John Boyd and John Warden: airpower's quest for strategic paralysis', in Phillip S. Meilinger (ed.),

The Paths of Heaven: the evolution of airpower theory, Air University Press: Alabama, 1999, pp. 357-98.

3 Peter Layton, *Network-centric warfare: a place in our future?*, Air Power Studies Centre: Fairbairn, 1999.

4 David A. Deptula, *Evolving technologies and warfare in the 21st century: introducing the 'combat cloud'*, Mitchell Institute for Aerospace Studies: Arlington, 2016.

5 Future Joint Force Development, *Cross-domain synergy in joint operations: planners guide*, Department of Defense: Washington DC, 2016.

6 William O. Odom and Christopher D. Hayes, 'Cross-domain synergy: advancing jointness', *Joint Force Quarterly*, Issue 73, April 2014, pp. 123-8.

7 Hawk Carlisle, 'C2 and fusion warfare', *Air Force Association* [website], 2017, available at <http://secure.afa.org/events/AWS/2017/postOrlando/audio/3-2-17-Carlisle.asp> accessed 23 April 2017; and Lani Kass, 'Panel: C2 and fusion threats', *Air Force Association* [website], 2017, available at <http://secure.afa.org/events/AWS/2017/postOrlando/audio/3-2-17-C2Panel.asp> accessed 23 April 2017.

8 David A. Deptula, 'A new era for command and control of aerospace operations', *Air & Space Power Journal*, July-August 2014, pp. 5-16.

9 Jeff Harrigian and Max Marosko, *Fifth generation air combat: maintaining the joint force advantage*, Mitchell Institute for Aerospace Studies: Arlington, 2016.

10 Robert P. Otto, *Data science and the USAF ISR Enterprise*, Department of Defense: Washington DC, 2016; and Nicholas P. Cowan, 'Rethinking command and control of intelligence, surveillance, and reconnaissance', paper presented at the 20th International Command and Control Research and Technology Symposium, July 2015, available at <https://static1.squarespace.com/static/53bad224e4b013a11d687e40/t/55a64e86e4b0e88cf27dcc6d/1436962438969/094.pdf> accessed 23 January 2018.

11 *Oxford English Dictionary*, available at <https://en.oxforddictionaries.com/definition/big_data> accessed 12 December 2017.

12 Lara Seligman, 'Combat cloud', *Aviation Week and Space Technology*, 10-23 October 2016, pp. 40-1; and James Drew, 'Airborne gateway', *Aviation Week and Space Technology*, 10-23 October 2016, pp. 41-3.

13 John Stillion and Bryan Clark, *What it takes to win: succeeding in 21st century battle network competitions*, Center for Strategic and Budgetary Assessments: Washington DC, 2015; and Andrew F. Krepinevich, *Maritime warfare in a mature precision-strike regime*, Center for Strategic and Budgetary Assessments: Washington DC, 2014.

14 Edward N. Luttwak, *Strategy: the logic of war and peace*, The Belknap Press: Cambridge, 1987.

15 August Cole, 'Lesson learned from the next world war–integrated cyber and space operations in ghost fleet', in David Burns (ed.), *RAAF Air Power Conference 2016: Multi-Domain Integration*, Air Power Development Centre: Canberra, 2017, pp. 75-85.

16 Sydney J. Freedberg, 'Iraq: proving ground for multi-domain battle', *Breaking Defense* [website], 27 April 2017, available at <https://breakingdefense.com/2017/04/iraq-proving-ground-for-multi-domain-battle/> accessed 7 December 2017.

Is relying solely on smart weapons a smart approach?

Warrant Officer David Turnbull, Royal Australian Air Force

> Advanced aerospace technology works. In the right circumstances it saves lives on both sides and, when available in sufficient quality and quantity, wins wars.
>
> Attributed to US Defense Secretary William Cohen (1997-2001)[1]

Introduction

The above quote reflects the sentiments of many air power advocates, that advanced aerospace technology and, in particular, advanced weapons technology, wins wars. Alan Stephens also contends that:

> The continuing success of precision-guided standoff munitions … capabilities which facilitate fighting precisely and from a distance … can only generate greater interest and investment in [these] kind of weapons.[2]

Precision-guided munitions (PGMs) have become the standard for kinetic air power application since their revolutionary success in the first Gulf War in January 1990. Cutting-edge PGMs are capable of pin-point accuracy in all weather conditions—by day or night—and often from large standoff ranges. This precision, however, comes at a cost, with increasingly capable technologies driving increasingly eye-watering price tags.

While 'dumb' bombs are markedly cheaper than their 'smart' counterparts, the overwhelming success of precision weapons (politically and militarily) has made the humble 155mm artillery shell, 70mm rocket and Mk82 low-drag 'Slick' and their ilk effectively obsolete in the eyes of many. But is this really the case? According to Mark Thomson:

> If you want to safeguard Australia's national security, then you stockpile guided and smart munitions, not bullets and explosives.[3]

The aim of this article is to critically evaluate this statement in the context of the importance or otherwise of PGMs and the implication that Australia's national security can be assured by the application of high-tech weaponry. It will consider what 'precision' really means and whether 'dumb' munitions still hold a place in planned fifth-generation air power applications; qualitatively examine the associated cost of the technology of PGMs; and test if they are really the infallible 'silver bullet' they have been made out to be. These points will form the basis of a discussion on whether a sole reliance on smart weapons, as suggested by Thomson, is a smart approach.

Considerations

Precision: 'to be precisely accurate'

> Precise forecasts masquerade as accurate ones.[4]

Precision and accuracy are often used interchangeably but, in reality, they have very specific and different definitions, particularly in the world of weapon employment. The darts player aiming for the bullseye who sprays their shots all over the board (and wall) is neither precise nor accurate. The player capable of grouping their darts tightly but off to the left would be regarded as a precision shot, whereas the one landing darts around the bullseye in a loose grouping would be an accurate shot. The ideal then is to combine the two to achieve a tight grouping that centres on the bullseye as the intended impact point—precisely and accurately.

The employment of kinetic weapons is essentially the same as playing darts at the pub, in that to achieve the best effect against a target (bullseye), munitions—particularly PGMs—must be both precise and accurate, especially when utilising low-explosive yield (low-collateral) weapons, where missing by metres may result in the target remaining a threat. For the purpose of this article, 'precision' in the context of precision-guided/smart weapons will equate to the munition being both precise and accurate in its performance when measured against unguided 'dumb' stores.

Do dumb bombs still hold a place in air power application?

> To use air power in penny packets is to disregard the importance of a menacing and even mysterious military reputation.[5]

'Precision' has become a favoured buzzword for the media, politicians and commanders commenting on military operations, such that:

> The ability to create precise effects is not only the hallmark of advanced air forces, but arguably the greatest contribution air power brings to the modern battlespace. The RAAF creates precise effects through its capability to conduct precision attack.[6]

However, the RAAF's *Air Power Manual* notes that 'there is an important distinction between precision as a means to achieve a desired and focused effect and as a descriptor for precision-guided [weapon] capabilities', noting that the precision employment of air power does not always involve the use of PGMs.[7] Conflicts offer up threats and target sets as varied as large industrial complexes to specific individuals. Air power options for negating such targets can range from a single strike using a precision weapon to multiple/mass strikes utilising a number of unguided stores.

The method of attack is determined by a range of factors, including the type and quantity of available weapons and delivery platforms; the specific outcome desired (total destruction versus disruption of operations); operational limitations (such as weather and the quality/availability of intelligence, surveillance and reconnaissance [ISR]); rules of engagement specific to the conflict; and political limitations placed on weapon employment and types (such as the use or otherwise of cluster-bomb munitions).

Regardless of the weapons used or delivery profiles employed, the ultimate aim of striking a target is to realise a precise effect. As an example, Eliot Cohen asserts that the 'massive raids by B-52s raining down conventional bombs helped crush the morale of Iraqi soldiers' during the first Gulf War.[8] While not a pin-point precision strike, the effect desired and achieved was precise with the weapon sets available.

For many years, Western nations have enjoyed advantage in conventional warfighting capabilities, with various enemies resorting to irregular methods such as insurgencies, guerrilla tactics, terrorism and suicide bombings to successfully wage war. Air power is frequently the first—and sometimes only—Western military force applied kinetically in irregular conflict, with PGMs the weapon of choice.

While irregular warfare is the current trend, it may not always be the case and Western nations must remain capable of 'closing with and killing large numbers of the enemy'.[9] Against massed enemy units in the field, the employment of individual cutting edge, high-end PGMs against individual targets (versus area bombing with dumb stores) would be both costly and inefficient.

In this respect, 'carpet bombing' could well be the better choice for a precision effect. Indeed, the simple and brutal fact that war is cruelty, and force works by destroying and killing, means that area bombing may well be required in future conflicts.[10] In certain circumstances, the application of 'penny packeted' PGMs cannot replace:

> [T]he importance of terrifying enemy soldiers through the fear of violent death from tons of ordnance raining down on them—fear of violent death only comes from the imminent possibility of the real thing.[11]

The cost of precision-guided munitions

It was not so long ago that a thousand-dollar bomb would be used against a million-dollar target; it seems now the opposite is true. Although not always the case, weapon cost and precision/accuracy typically go hand-in-hand, meaning absolute pin-point accuracy has a high price-tag attached. The acquisition and sustainment of precision-guided inventories comes at high cost—and does not cease with the last physical weapon delivery.

Ongoing cradle-to-grave requirements of the test and evaluation of new systems, upgrades and concepts; operator/maintainer training; regular live 'raise-train-sustain' employment; periodic maintenance; software/hardware updates; and through-life system upgrades all ensure that valuable sustainment dollars are being spent throughout the weapon life-of-type—and often before a single weapon has been used in anger.

With the rising cost of precision-guided capabilities becoming a concern for many military forces, the ability to keep pace with their technology will limit many to cheaper, lower-technology weapons or very small quantities of high-tech assets. As noted by Richard Hallion:

> Cost trends in precision weaponry are likely to force an evolutionary 'survival of the most capable for the least cost', particularly for those military services with scarce acquisition funding.[12]

For example, fielding AGM-88E Advanced Anti-Radiation Guided Missiles versus AGM-88B High-speed Anti-Radiation Missiles manifests a ten-fold increase in price. While there is no argument that the former is a more capable weapon, the latter is still a very effective anti-radiation capability that would work in the majority of tactical situations in Australia's region of interest—and at one-tenth the cost. Put simply, for every AGM-88E in the inventory, a force could field ten AGM-88Bs; and this is the decision point that many militaries and governments are faced with.

Adding to the spiralling investment dollars required for precision-guided capabilities, the cost of the weapons themselves is just one factor. Increasingly, smart platforms and targeting systems are required to employ smart weapons. While the F/A-18 Classic Hornet in RAAF service has been able to employ laser-guided bombs since its introduction, it was not until the Hornet upgrade program commenced in 1999 that modern precision weapons requiring more up-to-date digital interface (such as the AGM-158 Joint Air-to-Surface Standoff Missile) could be employed.

As improved precision weapons become available, a corresponding (and usually expensive) improvement in platform and/or sensor capabilities—either by way of upgrades to existing assets or new acquisitions—will be required to fully realise the potential of new technologies.

Are precision-guided munitions an infallible silver bullet?

> So long as there remains a substantial period, often up to ten years, between the inception of a new weapon system and its deployment, even the very latest weapons are out of date in terms of what technology could deliver.[13]

The current pace of technological advancement means that what is new today is obsolete tomorrow; and this is true for Apple I-Phones as much as it is for precision weapons. Given the relatively long service life of modern weapons, it is possible that many precision capabilities introduced into service inevitably fail to deliver over the life-of-type, at least from a cost/capability perspective, without some form of expensive upgrade to maintain their edge.

Added to this, no military technology (indeed no technology at all) works all the time: 'the truly fail-proof design is chimerical'.[14] Software glitches, ageing components, flat batteries and a multitude of other technical issues are all possibilities that can render even the best PGMs useless at some stage during their cradle-to-grave journey.

Coupled with this, anti-PGM measures typically keep pace with new technology, which can negate the edge the munition was intended to achieve. Anti-PGM strategies can be surprisingly simple low-tech measures or sophisticated and high-tech in their design and employment. For visual or laser-guided weapons, smoke-screening a target can often be enough to disrupt weapon guidance accuracy. More sophisticated weapons can be rendered ineffective by jamming weapon guidance and target acquisition data signals. As an example, simply moving or hiding Scud missile launchers was enough for Saddam Hussein to frustrate allied air power's efforts to locate and destroy them during the first Gulf War.

The employment of many PGMs also requires a permissive tactical environment; the right operating conditions and operational targeting systems to generate a hit—especially early generation munitions or those at the budget end of the scale. The limitation of many first-generation or low-cost PGMs is that they require visual conditions between the weapon and the target. In bad weather, these systems cannot be used as they require visual or infra-red acquisition of the target. Further, laser-guided weapons require the target to be lasered—some continually—until impact.[15] As noted by Danielle Gilmore:

> When so many environmental [and technical] factors can readily cause a [precision-guided munition] to miss … it is easy to comprehend why they cannot be used in every military strike.[16]

Discussion

> There is no logical reason why bullets or bombs should be wasted on empty air or dirt. Ideally, every shot fired should find its mark.[17]

> In the fall of 1944, only seven per cent of all bombs dropped by the 8th Air Force hit within 1000 feet of their aim point. It took 108 bombers dropping 648 bombs to guarantee a 96 per cent chance of getting just two hits against a German power-generation plant; in contrast, in the Gulf War, a single aircraft dropping two LGBs [laser-guided bombs] could achieve the same results with essentially 100 per cent expectation of hitting the target.[18]

Precision-guided smart weapons work. As contended by Hallion, '[they] combine the attributes of accuracy, range, striking power and portability; and it is that combination that makes [them] a powerful force multiplier in today's military scene'.[19] Dropping thousands of bombs in order to destroy a single target is no longer palatable or affordable for governments or military forces: all modern conflicts demand precision, proportionality and discrimination in the application of force.

This is particularly important in urban conflict where the risk of collateral damage and unintended consequences increases.[20] The political and military fallout associated with collateral air strike casualties and damage manifests rapidly in the modern world and is ferociously meted out by both the enemy (through propaganda) and 'friendly' media/human-rights/anti-war organisations. For these reasons, 'precision attack is the RAAF's chosen means of applying combat air power to create precise effects against an adversary to achieve desired campaign outcomes'.[21]

With the above in mind, precision attack does not imply the use of precision weapons; it is

defined by the precision of the effect created. The destruction of targets such as industrial plants in permissive tactical environments is equally achievable using dumb bombs as it is with PGMs, given the ability of modern aircraft radars and stores management systems to accurately deliver unguided weapons.

Building on the proven capabilities that modern digital interface weapons bring, improved fifth-generation capable aircraft/sensor/weapon interfaces such as the Universal Armament Interface; off-platform capabilities such as the Joint Weaponeering System; and network enabling the complete system in all phases of the 'find, fix, track, target, engage, assess' targeting cycle are intended to further optimise the precision, fidelity and speed of the targeting and weapon employment process.

Due to the introduction of capabilities such as higher-fidelity sensors, the Universal Armament Interface and the Joint Weaponeering System, smart aircraft systems are increasingly better at delivering unguided bombs with accuracy. As noted by Hallion, 'it is undoubtedly cheaper to have a smart airplane drop a dumb weapon' when operational circumstances permit.[22] Ultimately, there is no reason why dumb bombs, in the right circumstances, are not capable of being delivered extremely accurately.

The caveat to this, however, is that the aircraft's operational flight program must incorporate the full suite of ballistic data for all weapons that are to be employed by the platform—particularly dumb/unguided stores. Without appropriate and integrated ballistic data, weapons cannot be employed accurately—and the cost of capturing data, if absent, and validating its veracity is typically more than a cache of cutting-edge PGMs.

The employment limitations of precision-guided munitions

The conflict against Islamic State in Iraq and Syria highlights some of the limitations of precision attack, and demonstrates that the latest and greatest battlefield ISR capabilities and precision-guided munition technologies are not infallible. For example, the battle for Ramadi in early May 2015 saw a surge of IS fighters moving into Anbar and Salahuddin provinces from outer IS-controlled areas. Instead of using Toyota utilities as they had favoured in the past, IS members used nondescript sedans in an effort to blend with the civilian traffic and stay off the radar of US surveillance aircraft.[23]

Additionally, ISIS enforced a blackout of its own media posts from Ramadi to cover the build-up of fighters. Throughout this build-up, coalition air power was unable to detect or prevent the movement of IS fighters who were critical to the taking of Ramadi. According to US sources:

> They displayed admiral operational security. They understand the element of surprise. And they understand how [the coalition] can track them.[24]

As that demonstrates, even the most advanced munitions become useless if targets cannot be located and designated for attack. While these issues are not solely down to any limitations of PGMs themselves, it highlights that a reliance on ISR for target observation, identification and designation can degrade the ability to employ precision-guided assets. Of course, dumb bombs would be no better in these circumstances. But the fact remains that modern ISR and PGM technologies—and targeting processes—do have limits.

Added to this, the simple fact is that increased networked capabilities in the ISR, targeting and weapon engagement sphere will see a commensurate growth in the capacity to disrupt or degrade these systems, meaning that PGM employment in future tactical environments will likely be similarly degraded or denied.[25] If this is the case, building up and relying solely on inventories of smart weapons may well turn out to be a dumb idea. As noted by Cohen:

> The speciation of munitions brings unusual capabilities, but it also poses the risk of creating forces so specialised that they lack flexibility, and weapons so expensive that commanders will have only slender inventories to use when a war starts.[26]

Air power's inherent characteristics of flexibility and adaptability should ensure that dumb bombs still hold a place in air power capability. Seemingly obsolete dumb weapons are currently being revitalised in the counter-insurgency environment. Such weapons as the aircraft gun and unguided rockets are extremely accurate and have a small

collateral damage footprint, which this makes them well suited for use in crowded environments or where unacceptable damage may occur through bombing.[27] The RAAF's *Operational Air Doctrine Manual* usefully contends that:

> Through the careful selection of weapon systems for the task in hand, a commander can concentrate the required amount of force, but still apply the principle of economy of effort.[28]

The cost of capability

For certain targets, such as where low collateral damage estimates are not critical and when employing larger explosive yield weapons that can trade reduced precision for greater blast/damage effects (such as 2000lb class stores), utilising lower cost weapons, such as Paveway Series Laser Guided Bombs or Joint Direct Attack Munitions, may suffice over employing more expensive PGMs, such as the AGM-154 Joint Stand-Off Weapon.

For critical, 'exquisite' targets, it may well be that high-end, pin-point PGMs are the only dependable method of air attack. Critical target and collateral damage estimate analysis in the targeting cycle (especially for deliberate strike missions) can return cost benefits by utilising cheaper weapon options that still deliver a precise effect. Having affordable weapons options available, in conjunction with high-end PGMs, is the key to having the right mix and quantity of eggs in the basket to deal with foreseeable scenarios where Air Force may be called on to employ kinetic weapons—and do it cost effectively.

It would seem reasonable to argue therefore, that Thomson's statement regarding a reliance on smart munitions, which is widely supported by many PGM advocates, is fundamentally flawed as it diminishes air power's inherent characteristics of flexibility and adaptability.[29] Additionally, when and if Australia is ever involved in a future conventional conflict against a highly capable and resourced adversary, PGM stocks could well become a limiting factor by virtue of Air Force simply running out.

Resupply of high-tech smart weapons is not a simple, quick or cheap undertaking. Lead times can be very long for PGMs and, given the contracting timelines (many years) for specialised technology and manufacturing processes required to produce modern smart weapons, there is limited ability for timely surge production.

Countering this limitation, dumb bombs are cheap, easy and quick to produce, and have a built-in advantage of modularity in that they can be configured with a variety of mechanical, electronic or smart fuzes, dumb tail kits or guidance kits that turn them into cost effective smart weapons and increase their operational flexibility and adaptability.

The unguided dumb bomb is dead?

Air Force strike aircraft have dropped hundreds of bombs during Operation OKRA, none of which have been an unguided dumb store. Although unguided bombs have been the stalwart of air power throughout World Wars 1 and 2, Korea and Vietnam, the first Gulf War demonstrated the huge potential of precision weapons, with their use increasing in every conflict fought by the West ever since. This has culminated in the almost exclusive use of PGMs by the coalition in the fight against ISIS, with GPS-aided Joint Direct Attack Munitions the *de rigueur* weapon of choice.

While it is argued that dumb bombs do have a place in modern kinetic conflict, the reality is that these stores simply do not make it to the capacity-limited explosive storage and preparation areas of far off war-zones. Casting an eye across any operational coalition airbase explosives area typically reveals a sea of Joint Direct Attack Munitions, augmented by a handful of backup laser-guided munitions for use in case of issues with GPS or tail kit assemblies. The dumb bomb, regardless of its proven ability, is operationally dead from the new-age, PGM-centric point of view—with their employment relegated to raise-train-sustain activities. Is this how it will be in the future though?

When it all boils down, it is not very smart to put all of one's weapons solely in a cutting-edge PGM basket. While there are times when only a PGM will do, there are others where a Mk82 Slick coming through the door will be more than adequate—and more cost effective. As Hallion has argued:

> Though there is a continuing role for the dumb munition … the reshaping of military affairs that has been wrought by the precision munition will increasingly dominate logistical and strategic planning issues.[30]

Regardless of (and possibly because of) the domination of PGMs, careful requirements assessment and balancing of dumb and smart inventories to ensure adequate logistical/strategic support against all future scenarios (small insurgency conflicts through to all-out conventional war) should be at the forefront of future weapon capability and acquisition planning. The acquisition, storage and distribution, through-life support and disposal of weapons is a vastly expensive undertaking; therefore, weapon costs versus the required capability must be balanced.

To this end, stockpiling cheap, modular smart weapons such as laser-guided bombs and Joint Direct Attack Munitions; maintaining smaller quantities of dumb bombs for insurance; and holding niche PGMs for the exquisite targets sets would ensure that Air Force has the capability to wage war in all foreseeable kinetic scenarios, and also possess the deterrent (and large hammer) that high-end PGMs bring.

Broadening out from air power specifically, the increasing use of PGMs across the wider Defence environment, such as the M982 Excalibur GPA-aided 155mm artillery shell and Advanced Precision Kill Weapon System guidance kits for 70mm rockets means the validity of stockpiling smart weapons is no longer an exclusively Air Force issue—it is fast becoming a joint concern.

Ultimately, there is no single 'silver bullet' weapon solution. What is required is careful matching of desired weapon capabilities to the individual characteristics of the battlefield environment.

Conclusion

The aim of this article has been to critically evaluate Mark Thomson's contention regarding the importance or otherwise of PGMs and the implication that Australia's security can be assured by the application of high-tech weaponry. Australia's security is certainly closely tied to the application of high-tech air power weapons but security assurance is not guaranteed by smart weapons alone.

Maintaining a capability against those circumstances where PGMs are unsuitable (weather, availability, countermeasures, cost, etc) is a smart approach. Future weapon systems must be 'right-tech' for Air Force, in that they should be viable, cost effective and appropriate options—with the key being the ratio of inventories (the appropriate balance between quality and quantity).[31]

Ultimately, an emphasis on smart weapons is a smart approach but it needs to be insured against with a dumb bomb policy just in case: PGMs are not the panacea for every target in every conflict that some would have us believe. Stephens is right in his assessment of the criticality of advanced aerospace technology in modern air power; however, it is his use of the words 'circumstances' and 'sufficient' that are the key.[32]

This article has critically assessed the suggestion by Mark Thomson that Australia's security can be assured solely by smart weapons, and found it wanting simply because the characteristics of flexibility and adaptability that are so important to Air Force need to take into account all the circumstances that Air Force—and the wider ADF—may be required to deal with in the future.

Additionally, the reality of tight defence budgets and spiralling costs of PGM technology mean that Defence simply cannot afford to stockpile guided and smart munitions exclusively. To this end, relying on smart weapons as our only kinetic option is not a smart approach, and Defence should specifically aim to maintain a balanced inventory of conventional and precision munition capabilities that centre on low-cost smart weapons that are commensurate with fifth-generation smart platforms. Anything less could ultimately end up being rather 'dumb'.

Warrant Officer Turnbull enlisted in the Royal Australian Air Force as an Engineering Trade Apprentice in January 1989 and graduated as an Armament Fitter in September 1990. He has enjoyed postings to 75 Squadron, 77 Squadron, 3 Squadron and 22 Squadron; and numerous stints within Capability Acquisition and Sustainment Group in both acquisition and sustainment project offices.

Warrant Officer Turnbull currently works within Air Force Headquarters' Air Capability Enablers Directorate. He completed a Bachelor of Administrative

Leadership through the University of New England in 2010 and a Master of Business through the Australian Defence Force Academy in 2012, and has previously been published in the ADF Journal with his paper, 'A Warrant to Lead' (Issue 187, March/April 2012).

Notes

1 A. Stephens, 'Kosovo or the future of war', *Air Power Studies Centre* [website], 1999, available at <http://airpower.airforce.gov.au/APDC/media/PDF-Files/Archive%20Working%20Papers/paper-77-kosovo,-or-the-future-of-war.pdf> accessed 20 October 2017.

2 Stephens, 'Kosovo or the future of war'.

3 Cited by J. Kerin, 'Gillard urged to close bullet factories', *Australian Financial Review*, 31 January 2013, p. 15.

4 N. Silver, *The signal and the noise: why so many predictions fail—but some don't*, Penguin Books: London, 2012, p. 39.

5 E.A. Cohen, cited by S.J. Cimbala, *Military persuasion in war and policy: the power of soft*, Greenwood Publishing Group: Westport, 2002, p. 109.

6 Air Power Development Centre, *Control of the air, precision attack, and ISR: the foundations of modern air power*, Pathfinder No. 98, Air Power Development Centre: Canberra, 2008, p. 1.

7 Air Power Development Centre, *The Air Power Manual*, 6th Edition, Air Power Development Centre: Canberra, 2013, p. 141.

8 E.A Cohen, 'The mystique of US air power', *Foreign Affairs*, Vol. 73, No. 1, 1994, p. 114, available at <https://www.foreignaffairs.com/articles/1994-01-01/mystique-us-air-power> accessed 25 January 2018.

9 Stephens, 'Kosovo or the future of war', p. 11.

10 Cohen, 'The mystique of US air power', p. 8.

11 Cohen, 'The mystique of US air power', p. 8.

12 R.P. Hallion, *Precision guided munitions and the new era of warfare*, Paper No. 53, Air Power Studies Centre: Canberra, 1995, p. 13.

13 Air Power Development Centre, *High-end or low-end air power capabilities: the debate*, Pathfinder No. 102, Air Power Development Centre: Canberra, 2008, p. 2.

14 Cohen, 'The mystique of US air power', p. 8.

15 G. Beck, *Offensive air power in counter-insurgency operations: putting theory into practice*, Working Paper 26, Air Power Development Centre: Canberra, 2008, p. 29.

16 D.L. Gilmore, *Precision guided munitions and the law of war*, Working Paper 30, Air Power Development Centre: Canberra, 1995, p. 21.

17 P. Meilinger, cited in Hallion, *Precision guided munitions and the new era of warfare*, p. 1.

18 Hallion, *Precision guided munitions and the new era of warfare*, p. 3.

19 Hallion, *Precision guided munitions and the new era of warfare*, p. 1.

20 Air Power Development Centre, *Facets of air power: employment in urban conflicts*, Pathfinder No. 163, Air Power Development Centre: Canberra, 2001, p. 1.

21 Air Power Development Centre, *Control of the air, precision attack, and ISR*, p. 1.

22 Hallion, *Precision guided munitions and the new era of warfare*, p. 14.

23 M. Coker, 'How Islamic State turned the tables on the battlefield', *The Australian*, 27 May 2015, p. 10.

24 Coker, 'How Islamic State turned the tables on the battlefield', p. 10.

25 Department of Defence, *Future Operating Environment 2035*, Director General Joint Force Analysis, Department of Defence: Canberra, 2016, p. 21.

26 Cohen, 'The mystique of US air power', p. 114.

27 Beck, *Offensive air power in counter-insurgency operations*, p. 31.

28 Department of Defence, *The Operational Air Doctrine Manual*, 2nd Edition, Director General Air Command Operations, Royal Australian Air Force: Glenbrook, 2006, p. 2-2.

29 Air Power Development Centre, *High-end or low end air power capabilities*, p. 2.

30 Hallion, *Precision guided munitions and the new era of warfare*, p. 13.

31 Air Power Development Centre, *The reality of air power and irregular warfare: striking a balance*, Pathfinder No. 115, Air Power Development Centre: Canberra, 2009, p. 2.

32 Stephens, 'Kosovo or the future of war'.

Open system architectures for the ADF: opportunities and challenges

Dr Shane Dunn, Defence Science and Technology Group
Wing Commander Jesse Laroche, Royal Australian Air Force
Group Captain Pete Mitchell, DSC, OAM, Royal Australian Air Force

Introduction

Increasing uncertainty in our strategic environment, coupled with high rates of change of technology and the wider availability of sophisticated military technologies to state and non-state actors, have been identified as contextual trends in the *2016 Defence White Paper*.[1] The need for the ADF to adapt to these trends will pose challenges for the development, acquisition and sustainment of our military capabilities.

To manage the risks and opportunities posed by the above trends, the *2016 Defence White Paper* and the *2016 Defence Industry Policy Statement* have identified the following needs for the ADF:

- Systems with increasing operational agility, supported by technical flexibility;
- To be a smart buyer of increasingly technologically complex systems, maximising operational capability and value for money; and
- Systems with through-life agility enabled through partnership with a sustainable defence industry sector and academia.[2]

The *2016 Defence White Paper* also recognised that addressing these needs will require a highly capable Defence workforce with a more diverse range of skills. Air Force's Plan JERICHO's key themes of improving joint force integration; developing an innovative and empowered workforce; and improved acquisition and sustainment of capability are directly related to the above strategic needs.[3]

This article reports on a study carried out for Plan JERICHO which examined the potential of exploiting a design concept known as 'open system architectures'. An overview of the principles of open system architectures is presented, describing the effects of degrees of modularity and openness of an architecture. Some examples are then identified where these concepts are being exploited in military systems,

principally by the US Department of Defense. The article concludes by exploring some of the opportunities and challenges that might present if the ADF were to more widely exploit such system architectures.

Open system architectures

Open system architectures have been proposed by defence-related acquisition agencies (principally the US Department of Defense) for many years as offering potential for timely, agile and improved capabilities that are less expensive to acquire and maintain. There are many definitions for open system architectures. An ideal for Defence's purposes would be a model that enables hardware and/or software modules to be competitively sourced and integrated by a range of developers of Defence's choosing without being constrained by intellectual property considerations.

Practicalities typically compromise this ideal, with competing considerations arising from issues such as security, intellectual property, performance, safety, etc. These considerations will be evident in the system design through trade-offs in the degree of modularisation and the level of openness of the interfaces between modules.

The implementation of open system architecture concepts has been policy in the US Department of Defense for over 20 years, and more recently in the UK Ministry of Defence.[4] Strategic guidance for its application in the US Department of Defense can be found in the 'Better Buying Power' initiatives that describe the need for improved value for money in acquisition and for systems that can be adapted quickly to address new threats and technology developments.[5] In underpinning the development of a competitive buying environment, Better Buying Power 'emphasize[s] competition strategies [that] create and maintain competitive environments … [and] enforce open system architectures and effectively manage data rights'.

> While Australia does not mandate the use of open system architectures, needs expressed in the *2016 Defence White Paper* can be directly related to opportunities offered through the use of these design concepts.

Modular architectures

Open system architectures arise at the intersection of modular architectures and open standards. The design of a system from the perspective of how its various sub-systems are interconnected is described in its system architecture. A high-level definition for a system's architecture is:

> The fundamental organisation of a system embodied in its components, their relationships to each other and to the environment, and the principles guiding its design and evolution.[6]

Hence, the architectural design of a system is key to addressing force needs by defining the system's development process, complexity, evolvability and its relationship and interoperability with its environment and other systems.

A well-architected modular system manages complexity by creating modules, in hardware and software, such that the capability delivered by these modules can be developed, maintained and upgraded with minimal risk to the technical performance of other modules in the system. The level of impact one module has on another defines how tightly coupled that module is.

Modules that are loosely coupled and able to deliver a scalable and/or extendable system that can be upgraded or have modules added with minimal testing is desirable for system flexibility.[7] Older, monolithic systems did not partition or modularise the design, such that interdependencies between systems were not clear and any change could present a significant risk through accidental influences on unrelated sub-systems that could only be mitigated through extensive testing.[8]

How modules are defined within a system will be decided through trade-offs, considering the range of competing technical and business requirements and related constraints inherent in any complex design process. The modularity of a system can conceptually sit on a continuum that ranges from every part/line of code being able to be changed without recourse to regression testing to a purely monolithic system where no change can be made without full system regression testing.

Technical constraints constraining the degree of modularity may include compromises to size, weight and power considerations, meaning that systems with tighter constraints on these issues can expect a higher cost from increasing modularity.[9] A business factor leading to constraints could be from intellectual property considerations or that management of too many interfaces may be prohibitively expensive relative to the expected gain.[10]

Open standards

Fundamentally, an 'open standard' provides sufficient information for physical and data interfaces to enable a module to be modified without recourse to an original vendor or other intellectual property restrictions. The following is a definition for an open-standard that has been synthesised from a range of definitions available in the literature:

> An open standard is a well-defined, consensus-based and non-proprietary standard of sufficient maturity to be widely accepted and used by competing vendors and system developers. For a standard to be open, it should be developed collaboratively, open to change through collaboration, and be readily, if not freely, available with no barriers to implementation by a third party.[11]

Given the range of requirements in the above definition, and that many of the requirements are inherently subjective, it is not surprising that the practical application of such definitions has been described as being 'hazy at best', and that openness of a system is best considered as being 'not black and white but rather a matter of degree'.[12] The result is that the degree of openness of a standard sits on a continuum depending on the degree to which it meets each of the criteria in the above definition.

Modularity and open standards present opportunities to achieve the White Paper goals of increasing system agility through partnership with Australian defence industry, as well as helping to manage complexity and deliver improved value for money. A key to achieving Defence's aims from the application of open system architectures will be managing the spectrum of modularity and openness of the interface standards to ensure the required level of access to best meet the ADF's strategic needs.

The range of open system architectures

There are numerous open system architecture concepts that have been designed for use in different domains and for different intended applications. For example, a 2014 RAND report outlined nine open architecture concepts in various stages of development for uninhabited systems across air, land and maritime domains and with varying mission roles.[13] Based on the range of technical drivers, and given the different performance targets of the various concepts, the report concluded that the US Department of Defence should not attempt to develop a single architecture model for its uninhabited systems.

Indeed, for example in two large-scale projects, the US Navy and US Army are collaborating in the development of the 'Future Airborne Capability Environment', and the US Air Force is developing 'Open Mission Systems', with each using quite different architectural models, which are largely incompatible, despite being designed to meet similar goals.[14]

To ensure that the design and maintenance of an open system architecture remains manageable, rather than trying to be all-encompassing, each should be designed to meet the operational requirements of the environment in which it will operate. In addition, its design—with its architectural topology, identification of key interfaces, the standards used and their degree of openness—needs to consider the business and technical drivers and consequent cost-benefit trade-offs in the overall system design.

These trade-offs need to be assessed through broad stakeholder engagement, providing traceable, defensible decisions supported by a rigorous assessment process. This will also be required for system maintenance and development.[15]

Opportunities provided by open system architectures

A design based around modularity helps to mitigate risks arising from uncertainties about future requirements by enabling a system to be brought into service without meeting all its envisaged requirements. With an extensible

architecture, modules can be developed and added with relative ease after a capability has entered service, facilitating an evolutionary spiral acquisition process. Operators can bring their experience with the use of the system to the design and test process to help ensure that subsequent iterations deliver real operational improvements.[16]

Beyond design, development and acquisition, open system architectures enable improved obsolescence management through the life of a capability. Not being tied to an original equipment manufacturer (either the prime system integrator or module developers) for through-life support should enable competitively sourced alternatives for maintenance and upgrades, will provide Defence with choice in how systems are evolved, and will offer potential for greater innovation through competition.

Rapid development of technologies is a growing driver of obsolescence risk. Such obsolescence may simply present as missed opportunities for performance improvement through to sustainment challenges arising from diminishing manufacturing sources and material shortages where parts can become prohibitively costly or unobtainable. These obsolescence issues have been particularly evident in electronic hardware, driven by the rapid development of microprocessors, and are increasingly being seen in software.

These risks can be exacerbated by increasing use of commercial-off-the-shelf components, particularly given reducing commercial product life-cycles.[17] For example, the US Navy found that during the development process of a surface ship sonar system, from 1996 through to its first installation in 2002, over 70 per cent of the off-the-shelf parts became 'out of production (un-procurable)' before the first system had been installed.[18]

With capabilities being increasingly delivered through software functionality, open system architecture principles address some of these obsolescence risks by providing 'wrappers' that enable software to be easily hosted on a range of hardware platforms. In this way, hardware and software upgrades can be applied independently.[19]

An exemplar application of this is the US Navy's 'Acoustic – Rapid COTS [commercial off-the-shelf] Insertion' program. This program implements what the US Defense Science Board has called an 'incremental, iterative acquisition process' employing a continual spiral development approach that has shortened the technology insertion cycle for these types of systems from 12 years to two for software, and four years for hardware.[20] This process has helped US Navy anti-submarine warfare capabilities address increasingly quiet adversary submarines by exploiting up-to-date hardware and software developments that are competitively sourced and able to be continually improved through operator feedback.

As of 2011, this program had been in progress for more than 15 years and has been considered a great success from cost, performance and timeliness perspectives. Similar processes for processor and software upgrades are now being implemented for the US Navy's 'AN/BYG-1 Submarine Combat Control System' and for the Aegis combat mission system.[21]

Hardware and software module re-use across defence systems offers additional opportunities for the application of open system architecture principles across the ADF. There are many examples where sub-system components and algorithms fulfil similar or identical requirements across platforms and domains: a few generic examples are sensors and sensor pods; data processing/data fusion; communication system hardware and software; and human-machine interfaces.

A specific example of such re-use has been the development of an open architecture track manager in collaboration between General Dynamics and Lockheed Martin for the US Navy for its Aegis combat system and for the 'Ship Self Defense System' used on its large deck ships.[22] This development has led to a single system track manager and track server being used on both combat system types.

Such re-use of modules across the ADF, and with coalition partners, offers considerable potential for improved efficiencies in joint force capability management, as well as potential training benefits through increased commonality of functions and human machine interfaces. It would also enable smoother transition for personnel working across multiple systems.

Mission modularity occurs where systems are designed to operate with hardware and/or software modules that are easily swapped in and out for tailoring to specific mission requirements (for example, an operator may be able to choose between a range of intelligence, surveillance and reconnaissance sensors, communications packages and/or electronic warfare systems). Such modularity is a typical design feature in new unmanned aerial systems, emphasising the multi-role utility of many of these systems.[23]

Modular systems have the potential for improved force-level integration through the application of open system architecture principles by enabling sensors and communications systems to be adaptable to mission requirements. However, the benefits are typically focused on individual combat systems, and broad interoperability requires a joint system-of-systems architecture that goes beyond what is typically considered in open system architecture designs.[24]

Implications of open system architecture-enabled systems for the ADF

Many of the platforms and associated systems the ADF acquires are sourced from other nations. While Australian applications will be similar to those of the host nation, it is to be expected that Australia will have other requirements for these military capabilities, which may also include a greater number of roles than the system's original design purpose.

Carrying out indigenous modifications to military systems for Australian-specific requirements without original manufacturer support has proven to be challenging and expensive, particularly due to a lack of Australian knowledge base and intellectual property restrictions. Modularity can be expected to assist in providing a greater degree of multi-role applications through improved ability to tailor a system for specific missions, while the application of an open system architecture should enable module development by Australian industry tailored to Australian needs.

With a growing impetus towards the use of open system architectures in military capabilities, systems acquired from other nations will potentially offer increasing degrees of access to parts of the system for Australian-developed modifications. To get the required access, Australia will need to influence the development of projects to ensure sufficient access to the interface specifications required to exploit opportunities for Australian-sourced hardware and software modules.

By way of example, using the AIR 7000 maritime patrol aircraft replacement program, the P-8 Poseidon aircraft is expected to have elements of its mission system modularised with open interfaces by increment three of its development, while the Triton unmanned aircraft system is to have open system hardware and software modularity, enabling the integration of payloads without affecting the rest of the system.[25] However, it should be noted that these architectures are designed for the benefit of US operators and it is not yet clear if the ADF will have sufficient access to exploit these concepts. The F-35 joint strike fighter is also reported to have some level of open system architecture-enabled modularity such that the Israeli Air Force is reported to be able to add its own command, control, communications and computing system.[26]

Provided these systems are being architected to enable modular upgrades, they should not require full system regression testing to demonstrate that there are no safety implications or other significant performance risks.[27] The Collins submarine combat mission system is an example where Defence has access to system interfaces to enable Australian-developed modules/applications for improved functions, such as tracking algorithms and human-machine interface, to be submitted to the certifying authority (US Navy in this case) for inclusion in the next block upgrade.[28] This process has proven to be very successful with regards to addressing Australian requirements and enabling Australian innovation.

The 'Evolutionary Layered ISR [intelligence, surveillance reconnaissance] Integration eXemplar ARchitecture' (ELIIXAR), developed by Australia's Defence Science and Technology Group, is an exemplar enterprise architecture, comprising hardware and software built using open-systems principles designed to enable integration across diverse systems/sub-systems.[29] ELIIXAR

is currently being trialled within Army. However, being an Internet protocol-based enterprise architecture, ELIIXAR is not a real-time system, meaning it is not a suitable backbone for real-time, tightly integrated systems.

The 'Layered Approach to Service Architectures for a Global Network Environment' (LASAGNE) is a distributed embedded open system architecture framework, also developed by Defence Science and Technology Group, that spans real-time tactical to enterprise environments and can support real-time integration requirements.[30] In addition to being open system architecture frameworks for Australian designed systems, models such as ELIIXAR and LASAGNE offer potential as Defence-managed middleware that can be built on to foreign-sourced systems that may come with their own open system architectures.

Use of such indigenous architectures involve additional system overheads and Defence would then have the responsibility of maintaining that interface. However, the potential benefit in having an Australian outward-facing open system architecture to provide a more controlled interface for Australian industry may outweigh the cost implications.

Key requirements for the success of the Australian programs that have exploited open system architecture principles have been high-fidelity test beds for the development and testing of upgrades. These test beds have fully representative operator interfaces enabling direct involvement by operators in setting the requirements and performing evaluations of these proposed modifications for operational utility.

Communication systems are an area of rapidly improving technology in the civilian world but are relatively slow to progress in military systems due to considerations related to security, robustness and interoperability. An aim of open system architecture-enabled systems is to provide greater flexibility in hardware and software for communications, delivering improved integration and interoperability.[31]

Facilitation of interoperability across joint and coalition forces is expected with the growing application of open system architectures across the three Services. Chief of Army has asserted that Army's future vehicle fleets, including Land 400, should exploit common vehicle architectures and integration standards, and that effective partnership with industry will be enabled through more federated and open C4I [command, control, communications, computers and intelligence] architectures. Chief of Army also contended that:

> Open hardware and software architectures, shared integrations and more modular systems will be central to the manner in which our Army will train and fight as a digitised, joint force into the future.[32]

The application of open system architectures in Defence systems can be expected to have a strategic impact through supporting the White Paper goals to develop and maintain an indigenous, technologically advanced defence industry capability. Through enabling the more direct involvement of Australian industry in the development of modules for Defence systems, industry can expect greater export opportunities and Australia will have a workforce that is better prepared to respond to Defence's needs.[33] The prospects offered by increasing commonality and system flexibility across the Services should also facilitate joint force integration and interoperability.

Challenges arising from the implementation of open system architectures on ADF systems

Open system architectures promise better delivery and maintainability of Defence capabilities, and have been promising this for many years, noting that their use in systems acquired by the US Department of Defense has been mandated in various forms since 1994. Certainly, there have been many hurdles to the implementation of open system architectures—and the promise is still a long way from being realised.

The US Government Accountability Office has described two key challenges as being culture and investment in the defence acquisition community, and a lack of adaptation by industry to an open system architecture model that enables competition—noting that the development of a suitable model for compensating industry for its

intellectual property to enable the ideal application of open system architecture principles is an ongoing challenge.[34]

A case study from the commercial sector is the development of the IBM personal computer, which employed an open system architecture to develop a system based on widely available components and standards. These principles enabled third-party developers to create additional hardware and software accessories that contributed to systems based on this architecture gaining the dominant personal computer market share.[35]

The IBM personal computer is also an example of the challenges that can be faced by original manufacturers in embracing open system architecture principles. IBM's design became the market leader but, because of the openness of its standards and with no licensing constraints on its component suppliers, IBM lost control of its design, enabling compatible machines to take the dominant market share. Defence will have to be cognisant of the concerns of original manufacturers that similar outcomes could potentially threaten their business models.

The patchy and relatively slow progress with the US Department of Defense's implementation of open system architectures is instructive for Australia's application of these concepts. A report by the US Government Accountability Office on the use of open system architectures in unmanned aircraft systems across the Army, Navy and Air Force highlighted that the US Navy is the only Service prioritising its use, albeit in three of its four unmanned aircraft system programs.[36] None of the three Army and three Air Force programs examined in the report included open system architectures at the design stage.

Increased upfront costs can be expected with the design of a well architected system, with the payoff coming with reduced through-life management costs and improved system flexibility. However, project managers' incentives are typically more directly related to minimising acquisition costs, leading to 'brittle or unscaleable architectures that significantly increase life-cycle costs'.[37]

Also, the US Air Force and US Army have not had the expertise required to assess and manage a system employing an open system architecture. A key factor in the US Navy's uptake of these concepts has been a cultural willingness in its acquisition community to embrace the concepts, underpinned by a cadre of personnel skilled in the application of open system architectures. It was noted by the Government Accountability Office that stronger leadership is required across the US Department of Defense to enforce the application of open system architectures, and that this must be resourced by the organisation, including the provision of skilled personnel to support it.[38]

The trend of increasingly long in-service life of military systems has resulted in long times between new acquisitions. In this context, industry seems supportive of a model that enables continuous technology insertion as a means to maintain industry capability between large programs. Supporting continuous improvement, however, does not necessarily translate to supporting the concept of open competition. This has led to a range of proprietary modular architectures for which the complete interface definitions will not be fully disclosed, and original manufacturer support for integration will be required.[39]

In this way, the original manufacturer reaps the integration efficiency benefits of a modular architecture without having to submit to open competition. This could be considered a partial win for Defence, as it should reduce schedule and cost risks in upgrade programs, although the other benefits of a truly open system, such as widely sourcing innovative concepts and Defence-wide module re-use would not be realised.

Exploiting the opportunities offered by open system architectures for the ADF

There will be some military systems for which Defence will have ultimate design and certification authority. However, some other systems will be acquired, and likely maintained, in partnership with a foreign agency. For these systems, Defence may be able to influence the architecture and standards to ensure they meet Australian requirements through partnership in the development process. Where Defence does not have influence in the development process, modern systems will likely come with some

degree of modular design that may be exploited if the appropriate access rights can be negotiated.

Given this range of acquisition models, Defence will need the ability to work with a wide range of open system architecture concepts to exploit the opportunities that will enable Australian-sourced innovation and agile system development. For foreign-sourced systems, it is to be expected that a foreign agency will be the system integrator with final certification authority. In these cases, there is the risk that Australian integration requirements may not have high priority, leading to slower than anticipated introduction into service.

A risk to accessing the requisite rights to these open system architectures for foreign-sourced systems and components is that they may be subject to export restrictions, such as those that may arise from the *International Traffic in Arms Regulations*, which may limit Defence's ability to engage with Australian industry. Ensuring opportunities for Australian industry to develop innovative modifications involving systems subject to such restrictions will require careful management by Defence.

If the ADF requires a truly agile capability for modular development of its capabilities that is not constrained by foreign defence and industry priorities, an Australian-controlled organisation, infrastructure and personnel base will be required to enable design and test through to certified integration. The degree of testing required to mitigate integration risks would be dictated largely by the system architecture relating to the component being modified, particularly with regards to any safety risks that may arise. To enable indigenous integration, the ADF would also need a robust certification process, enabled by flexible developmental, acceptance and operational test and evaluation processes for open system architecture-enabled new modules or upgrades.

An aspect in defining where module boundaries lie will be the anticipated rate of change of technologies that deliver that function. Technology and capability road-mapping (or forecasting) is an important requirement when designing and maintaining defence capabilities that utilise modular architectures.[40] Such road-mapping will look at future capability requirements framed around potential future threats and opportunities that future technologies may provide.

If a functional role is anticipated to be subject to rapid technological development, then that function should be encapsulated by key interfaces enabling ease of upgrade of such technologically volatile components of the system. At the architecture design phase, this would help prioritise where the boundaries for these key interfaces should be. The openness of the standards employed at these interfaces defines the degree to which these modules can be competitively replaced or upgraded.

Reasons for interfaces not being open may include that the overhead associated with enforcing and maintaining an open interface is too high compared to having a proprietary, or no, standard; conformance to a standard may unacceptably decrease system performance; or there may be security concerns raised through conforming to a particular standard.[41]

For all systems where the ADF is reliant on open system architectures for a capability's through-life management, Defence will need access to the expertise required to ensure that the system architecture and the nature of 'openness' of the interfaces is appropriate and that the standards for these interfaces are maintained through the life of the capability.

It is important to note that there needs to be confidence and resourcing to ensure that standards will be maintained and keep pace with technology developments. Standards enable innovation by having a broad range of developers compete for the design of new components.[42] However, being consensus-based and typically having broad application, standards are not inherently agile and, if too constraining or not adequately maintained, may actually stifle innovation.

Defence will need the capability to assess an open system's attributes, influence the development of standards, and manage the risks that may arise from adopted standards not being maintained within useful timeframes. As noted earlier, the road-mapping of technology and capability needs is a requirement that Defence will have to instigate with the explicit aim of planning for and prioritising module-based upgrade opportunities. This capability will also ensure

that interface standards anticipate rather than lag Defence's requirements.

The US Air Force's 'Mission Systems Open Architecture Science & Technology' program has a requirement that the 'open architecture solutions accommodate "built-in" cybersecurity features'.[43] There is, however, the risk that the implementation of open system architectures in military systems could enable vectors for cyber threats, which will need careful management.[44]

One of the proposed benefits of open system architectures in Defence is that they will enable the leveraging of rapid technological development in the civilian sector for use in military systems leading to potential greater use of off-the-shelf components.[45] Software and hardware in such components will be an attractive target for potential adversaries that will be very challenging to avoid.[46]

Considering the security of the interface standards, it has been claimed that an open system architecture based on completely open specifications would be more secure than a proprietary, or otherwise closed, interface because there is effective crowd-sourcing to mitigate the risk of vulnerabilities.[47] The security considerations of open interface standards are related to the issues of security within the open-source software community, where it is still an open question as to how much reliance can be placed on open-sourcing to improve security and how the overall risks around these issues will be managed.[48]

Open system architecture concepts offer the potential to reduce the training burden because of increased commonality of sub-systems across capabilities. However, the pace and nature of system change must be managed to ensure that training does not fall behind upgrades and that force integration issues are considered. If the pace of change is too high, training will not be able to keep up.

A significant potential benefit from the application of open system architectures arises from portability and re-usability of modules, particularly software modules across different systems. This benefit will be best realised across the joint force and will require the development and maintenance of a repository of modules that are available for use across projects.

Broader considerations of a whole-of-mission system arise when considering integrated operations involving other joint and coalition systems. Regression testing of upgrades by systems integrators is currently largely considered at the platform level, and not at the broader system-of-systems level. An overall 'system architect' role will be required to manage risks at the wider system-of-systems level, which would obviously require a high level of understanding of what and how different platforms contribute to a mission.[49]

Where the aspects of the overall mission package are loosely integrated, modular change in one platform should present little risk to the mission package performance. If the mission is dependent on aspects of the overall system requiring tight integration between platforms, then regression testing of modifications will need to consider these larger systemic risks, noting the challenges to test and evaluation that arise when validating systems of systems.[50]

Conclusion

A growing aspect of the capability management of Defence systems will involve exploiting the opportunities offered by open system architectures while managing the risks that this will pose. The main opportunities will be increased system flexibility through modularity; improved ability to keep pace with threats and technological developments; and strategic benefit through increased Australian defence industry capabilities in design and integration of hardware and software modules for Defence. These opportunities contribute to addressing Australia's strategic requirements as articulated in the *2016 Defence White Paper* and *2016 Defence Industry Policy Statement.*

Enabling the successful exploitation of open system architectures by Defence underscores the identified need for a Defence workforce with the requisite skills to manage new technologies with greater agility. Defence will need access to a workforce with the technical and business skills to negotiate system architectures that meet Australia's strategic requirements around delivering operational capability, value for money, and offering opportunities for Australian innovation while also supporting the needs of original

manufacturers for a viable business model. To help achieve these outcomes, Defence needs to learn from US and UK defence projects that have successfully implemented these principles.

Capability managers will need assurance that the risks and opportunities offered by open system architecture-enabled systems are appropriately managed. This will require an acquisition culture and skills base to develop appropriate requirements for Defence and to support projects through their acquisition phase to ensure these requirements are met. These skills could reside within Defence or be sourced from industry, and the development and maintenance of this skills base could be shareable across the whole of Defence. Sharing this resource will assist with ensuring the consideration of mission and force level integration and interoperability.

The benefits of open system architectures will be best realised in an environment where operators and developers can work closely to realise systemic improvements that are grounded in operational needs. Exploiting the opportunities through the life of a capability will place responsibilities on capability managers for providing this development environment, as well as the need for appropriate test and evaluation infrastructure, organisation and personnel to manage the risks of development and/or integration of modular upgrades. This can evolve as different systems become available, with the scale to be matched to the level of complexity or risk that the capability manager is willing to accept.

Dr Shane Dunn completed his Bachelor's degree in Aeronautical Engineering from the Royal Melbourne Institute of Technology in 1986 and was awarded a PhD from the University of Melbourne in 1992. Shane has over 30 years' experience in Defence Science and Technology Group in air platforms and systems, and air power-related research. He is currently the Science Team Lead for Air Power Future Concepts in the Joint and Operations Analysis Division.

Wing Commander Jesse Laroche completed his Bachelor's degree in Science at the Australian Defence Force Academy in 1996 and completed a Master of Military Operational Art and Science in 2015 and a Master of Philosophy in Military Strategy in 2016 at the US Air Force's Air University. Jesse has served in numerous positions throughout his 24 years in the Royal Australian Air Force, primarily as a pilot flying both air lift and maritime patrol aircraft. He is currently posted to Air Force Headquarters, closely involved in the implementation of Plan JERICHO.

Group Captain Pete Mitchell joined the Royal Australian Air Force in 1993 and graduated as a pilot in 1995 before qualifying on the F/A-18A and serving with No. 75 and No. 77 Squadrons. He served on exchange with the US Marine Corps, again flying F/A-18A aircraft before his command tours with Forward Air Control Development Unit, Joint Electronic Warfare Operational Support Unit and No. 75 Squadron. He has deployed to the Middle East twice, in 2003 and again in 2015. He is currently the Director of Plan JERICHO in Air Force Headquarters.

Acknowledgements

The authors would like to gratefully acknowledge the assistance and support of the following during the study that led to this paper: Air Commodore Andrew Campbell and Air Commodore Robert Chipman for initiating the study and helping to guide it through its early stages; subject-matter experts from the Maritime Electronic Warfare Systems Program Office, and Aerospace, Maritime, Land, Joint Operations and Analysis and Cyber and Electronic Warfare Divisions of the Defence Science and Technology Group.

The time and assistance offered by the LASAGNE and ELIIXAR development teams of Weapons and Combat Systems and National Security and ISR Divisions respectively was of particular value. It is the insights developed through practical experience from the subject-matter experts from all of the above areas that has been key to shaping this paper.

Notes

1 Department of Defence, *2016 Defence White Paper*, Commonwealth of Australia: Canberra, 2016.

2 Department of Defence, *2016 Defence Industry Policy Statement*, Commonwealth of Australia: Canberra, 2016, available at <http://www.defence.gov.au/WhitePaper/Docs/2016-Defence-Industry-Policy-Statement.pdf> accessed 23 January 2018.

3 Royal Australian Air Force, 'Plan JERICHO', *Air Force* [website], available at <https://www.airforce.gov.au/our-mission/plan-jericho> accessed 23 January 2018.

4 Under Secretary of Defense for Acquisition, Technology and Logistics, 'Memo amplifying DoDD 5000.1: guidance regarding modular open systems approach implementation', *Office of the Assistant Secretary of Defense for Logistics & Materiel Readiness* [website], available at <http://www.acq.osd.mil/log//mpp/ats_

opensystems.html> accessed 23 January 2018; also UK Ministry of Defence, *Defence Standard 23-09 - generic vehicle architecture*, UK Ministry of Defence: London, 2010.

5 N. Guertin and T. Hurt, *DoD Open Systems Architecture Contract Guidebook for Program Managers: a tool for effective competition*, Defense Acquisition University: Fort Belvoir, September-October 2013.

6 International Organization for Standardization (ISO), 'Systems and software engineering – architecture description', *ISO* [website], 2011, available at <http://www.iso-architecture.org/ieee-1471/defining-architecture.html> accessed 23 January 2018.

7 MITRE Corporation, *Systems engineering guide – collected wisdom from MITRE's systems engineering experts*, MITRE Corporation, Bedford, 2014.

8 For example, integrating a new camera on the Northrop Grumman Triton unmanned aircraft system required 'as much as 66 per cent' less software regression testing than would have been required for an architecture that was not modularised: US Government Accountability Office, 'Defense acquisitions – DoD efforts to adopt open systems for its unmanned aircraft systems have progressed slowly', *US Government Accountability Office* [website], July 2013, available at <https://www.gao.gov/products/GAO-13-651> accessed 23 January 2018.

9 Katja Hölttä, Eun Suk Suh and Olivier de Weck, 'Tradeoff between modularity and performance for engineered systems and products', *CiteSeer*^{x} [website], abstract available at <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.116.4138> accessed 23 January 2018.

10 D. Firesmith, 'Open system architectures: when and where to be closed', *Software Engineering Institute* [blog], available at <https://insights.sei.cmu.edu/sei_blog/2015/10/opensystemarchitecturewhenandwheretobeclosed> accessed 23 January 2018.

11 B. Sims, 'Approaches to open technology systems specification', *Defence Science and Technology Organisation* [website], May 2012, available at <https://www.dst.defence.gov.au/sites/default/files/publications/documents/DSTO-TN-1087%20PR.pdf> accessed 23 January 2018.

12 R. Black and M. Fletcher, 'Open systems architecture - both boon and bane', *Academia* [website], 2006, available at <http://www.academia.edu/20896448/Open_systems_architecture_-_Both_boon_and_bane> accessed 23 January 2018; also Firesmith, 'Open system architectures'.

13 D. Gonzales and S. Harting, *Designing unmanned systems with greater autonomy: using a federated, partially open systems architecture approach*, RAND Corporation: Santa Monica, 2014.

14 J. Cernezia, 'Introduction to The Open Group and the FACE™ Consortium', *The Open Group* [website], 4 August 2015, available at <https://www.opengroup.us/face/documents/17354/SOSA_FACE_Overview_Industry_Day_2.pptx> accessed 23 January 2018; US Air Force Research Laboratory, 'Mission systems open architecture science & technology (MOAST)', unpublished paper by Avionics Vulnerability Mitigation Branch, Sensors Directorate, Air Force Research Laboratory, 12 Aug 2015; and J.L. Tokar, 'A comparison of avionics open system architectures', *Sigada* [website], January 2017, available at <http://sigada.org/conf/hilt2016/paper-Tokar.pdf> accessed 23 January 2018.

15 See, for example, J. Tyree and A. Akerman, 'Architecture decisions: demystifying architecture, *IEEE Software*, March/April 2005, pp. 19-27, available at <https://www.utdallas.edu/~chung/SA/zz-Impreso-architecture_decisions-tyree-05.pdf> accessed 23 January 2018.

16 MITRE Corporation, 'Systems engineering guide'.

17 US Department of Defense, *Diminishing manufacturing sources and material shortages – a guidebook of best practices for implementing a robust DMSMS Management Program*, Defense Standardization Program Office, US Department of Defense: Washington DC, August 2012.

18 P. Singh and P. Sandborn, 'Obsolescence-driven design refresh planning for sustainment-dominated systems', *The Engineering Economist*, Vol. 51, No. 2, April-June 2006, pp. 115-39.

19 The concept of 'wrappers' is embodied in the open system architectures-related software development concept known as 'service oriented architectures'.

20 Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, *Report of the Defense Science Board 2010 Summer Study on Enhancing Adaptability of US military forces – Part A. Main Report*, Department of Defense: Washington DC, January 2011.

21 US Department of Defense, 'AN/BYG-1 Combat Control System' (under 'Navy Programs in FY 2012'), in *Director of Operational Test and Evaluation (DOT&E) Annual Report*, US Department of Defense: Washington DC, December 2012; P. DeLuca *et al.*, *Assessing Aegis Program transition to an open-architecture model*, RAND Corporation: Santa Monica, 2013.

22 G. Fein, 'Navy developing path forward for open architecture implementation', *Defense Daily*, 21 August 2008.

23 For example, the US Navy's small tactical unmanned aerial system program anticipates having at least 32 different payloads from 24 different manufacturers: US Government Accountability Office, 'Defense acquisitions – DoD efforts to adopt open systems for its unmanned aircraft systems have progressed slowly'; and Gonzales and Harting, *Designing unmanned systems with greater autonomy.*

24 S. Sommerer *et al*., 'Systems-of-systems engineering in air and missile defense', *Johns Hopkins APL Technical Digest*, Vol. 31, No. 1, 2012.

25 US Government Accountability Office, 'Defense acquisitions – DoD efforts to adopt open systems for its unmanned aircraft systems have progressed slowly'.

26 E. Tegler, 'Israel's F-35 app and its implications', *Aviation Week & Space Technology*, 22 April 2016.

27 An important consideration of open system architecture implementations is that systems should be loosely coupled as much as possible and tightly integrated only where required: MITRE Corporation, 'Systems engineering guide'.

28 See <https://www.dst.defence.gov.au/projects/collins-class-submarine-replacement-combat-system>

29 See <https://www.dst.defence.gov.au/projects/

evolutionary-layered-isr-integration-exemplar-architecture-eliixar>

30 Defence and Science Technology Group (DST), 'Layered Approach to Service Architectures for a Global Network Environment (LASAGNE)', *DST* [website], available at <https://www.dst.defence.gov.au/sites/default/files/publications/documents/DSC%201753%20Avalon%20Air%20Show%20LASGNE%20.pdf> accessed 23 January 2018.

31 Sims, 'Approaches to open technology systems specification'.

32 Lieutenant General Angus Campbell, 'Chief of Army address to the Defence Magazine Conference', *Army* [website], 9 February 2016, available at <https://www.army.gov.au/our-work/speeches-and-transcripts/chief-of-army-address-to-the-defence-magazine-conference> accessed 23 January 2018.

33 From a UK perspective, one of the key aims of adopting open system architectures is the opportunity for improved local science and technology involvement in Ministry of Defence systems development and the strategic and export opportunities this creates: UK Ministry of Defence, *National security through technology: technology, equipment, and support for UK defence and security*, Ministry of Defence: London, February 2012.

34 US Government Accountability Office, *Defense acquisitions: review of private industry and Department of Defense open systems experiences*, US Government Accountability Office: Washington DC, 26 June 2014; and S.I. Erwin, 'DoD clashes with suppliers over data rights', *National Defense*, January 2014.

35 H.W. Chesbrough and D.J. Teece, 'When is virtual virtuous? Organizing for innovation", *Harvard Business Review*, January-February 1996.

36 US Government Accountability Office, 'Defense acquisitions – DoD efforts to adopt open systems for its unmanned aircraft systems have progressed slowly'. 'Fire Scout' is the only US Navy unmanned aircraft system program considered that did not consider this.

37 J. Doyle, *B2PCOE Open Systems Architecture – Final Report*, ACI Technologies Inc.: Philadelphia, 2011; also B. Boehm, *Tradespace and affordability – Phase 1*, Systems Engineering Research Center, Stevens Institute of Technology, Hoboken, 9 July 2013.

38 US Government Accountability Office, 'Defense acquisitions – DoD efforts to adopt open systems for its unmanned aircraft systems have progressed slowly'.

39 National Research Council, *Responding to capability surprise: a strategy for US naval forces*, The National Academy Press: Washington DC, 2013; Doyle, *B2PCOE Open Systems Architecture – Final Report*.

40 Sims, 'Approaches to open technology systems specification'.

41 Firesmith, 'Open system architectures'.

42 R. H. Allen and R.D. Sriram, 'The role of standards in innovation', *Technological Forecasting and Social Change*, Issue 64, 2000, pp. 171-80.

43 US Air Force Research Laboratory, 'Mission systems open architecture science & technology'.

44 US Air Force, 'Global horizons, final report', *Homeland Security Digital Library* [website], 21 June 2013, available at <https://www.hsdl.org/?abstract&did=741377> accessed 23 January 2018; C. Sledge and D.C. Schmidt, 'A discussion on open-systems architecture', *Software Engineering Institute* [blog], 23 November 2015, available at <https://insights.sei.cmu.edu/sei_blog/2015/11/a-discussion-on-open-systems-architecture.html> accessed 23 January 2018; B. Meyer, '4 best practices for open software ecosystems', *Software Engineering Institute* [blog], 17 November 2015, available at <https://insights.sei.cmu.edu/sei_blog/2015/11/osa-4-best-practices-for-open-software-ecosystems.html> accessed 23 January 2018.

45 Leveraging off-the-shelf developments is an explicit aspect of some military open system architecture programs, particularly with regards to processor upgrades: see, for example, M. Boudreau, *Acoustic rapid COTS insertion: a case study in spiral development*, Naval Postgraduate School: Monterey, 30 October 2006.

46 Defence Science and Technology Group, *Future cyber security landscape – a perspective on the future*, Cyber and Electronic Warfare Division, Defence Science and Technology Organisation, May 2014, available at <https://www.dst.defence.gov.au/publication/future-cyber-security-landscape-perspective-future> accessed 23 January 2018.

47 Sledge and Schmidt, 'A discussion on open-systems architecture'.

48 G. Schryen, 'Is open source security a myth?', *Communications of the ACM*, Vol. 54, No. 5, May 2011, pp. 130-9.

49 N.H. Guertin, R. Sweeney and D. Schmidt, *How the Navy is using open systems architecture to revolutionize capability acquisition*, Naval Postgraduate School: Monterey, May 2015.

50 J.D. Dahmann, K.J. Baldwin and G. Rebovich, 'System of systems and net-centric enterprise system', *MITRE* [website], 2009, available at <https://www.mitre.org/publications/technical-papers/systems-of-systems-and-netcentric-enterprise-systems> accessed 23 January 2018.

The current crisis in the Persian Gulf in the context of hybrid warfare

Associate Professor Sascha-Dominik Bachmann, Bournemouth University and Swedish Defence University

Introduction

The Middle East, or New Middle East as it also has become known after the Arab Spring of 2011, is going through seminal geographical and political changes and challenges.[1] In the end, the Arab Spring did not lead to the advent of an Arab renaissance of democracy and good governance but only to increased regional instability. The latter has been highlighted by the rise of Islamic State (IS), firstly in Syria and Iraq, and then Libya, where it managed to exploit the vacuum left after Qaddafi.

The present crisis among the members of the Cooperation Council for the Arab States of the Gulf (GCC but known colloquially as the Gulf Cooperation Council) began when Saudi Arabia and the United Arab Emirates (UAE) cut diplomatic ties with Qatar and imposed a land, sea and air embargo in early June 2017, in response to the alleged role of Qatar in aiding and abetting Islamist terrorism in the region, as well as its diplomatic ties to Iran.

The crisis has laid bare the region's insecurities and vulnerabilities, against the backdrop of new threats to the region's stability, notably the emergence of so-called hybrid threats and hybrid warfare. This has repercussions far beyond the region for economic, strategic and religious reasons. The arrival of new strategic competitors to US interests in the region, including China and Russia, and the return of Turkey as the successor of the former colonial occupier of Arab lands, the Ottoman Empire, have complicated the situation.

This short contribution discusses the present crisis within the context of security and conflict-related observations from the region, being played out through hybrid warfare, concluding with a brief synopsis of Qatar's potential countermeasures.

The GCC as a focal point of Gulf prosperity and the need for regional security

The GCC states represent some of the wealthiest states in the world (in terms of GDP per capita). After the discovery of oil in many Gulf nations, they united as the world's main oil producers: Saudi Arabia alone is the second-largest producer of crude oil after Russia, and the GCC's share of global oil reserves accounts for about 70 per cent of all global reserves.[2] The global dependency on oil (and liquefied gas) is set to continue, despite increasing initiatives among the G7 states to find non-fossil fuel alternatives, compounded by the steady industrialisation and urbanisation of countries such as India and China.

Consequently, the security and stability of GCC countries has become a matter of global concern. Western nations, in particular, due to their political, military and security interests, have sought to strengthen security in the region, with the US-GCC Strategic Cooperation Forum of 2012 an example of successful cooperation for the advancement of political, military and security interests.[3]

Such security arrangements are clearly necessary given that many GCC countries have experienced armed conflict in recent decades: the Iran-Iraq War in 1980, the Iraqi invasion of Kuwait in 1990, the US-led invasion of Iraq in 2003, and the ongoing war in Yemen all highlight the absence of a GCC security and defence arrangement which is powerful enough to deter or resolve regional disputes.

The problem lies in the nature of the GCC as an economic and political grouping, with little appetite for closer cooperation in the fields of security, conflict prevention or defence. Its founding document, the GCC Charter, was ratified in May 1981 and requires cooperation in financial and economic interests, customs, education and culture, as well as administrative procedures between member-states.[4] However, there is no provision for external security or defence arrangements.

A planned GCC Internal Security Pact, as a successor to the failed Internal Security Agreement of 1982, focuses more on internal challenges and has been criticised for its potential to be used as a tool of internal persecution.[5] The findings of the Doha Declaration of 1990, which highlighted the ineffectiveness of GCC defence and security arrangements, are still valid.[6] While a number of GCC countries have bilateral defence agreements, there is no doubt that addressing these concerns in the GCC Charter could strengthen the GCC and regional security.

The Second Lebanon War 2006 as a precursor of hybrid threats/warfare

Hybrid warfare is an emerging notion of 21st century conflict that combines four elements along the spectrum of warfare, namely conventional warfare, irregular warfare (terrorism and counter-insurgency), asymmetric warfare (waged by resistance groups) and compound warfare (wherein irregular forces supplement a conventional force).[7]

As a potentially new method of warfare, it expands on existing doctrinal elements in three ways: firstly, by furthering unconventional warfighting capacities alongside conventional methods but beyond the existing compound (spectrum) operations, such as cyber-warfare; secondly, by pursuing activities in the so-called 'information sphere' and, thirdly, by using 'lawfare' to achieve political and strategic objectives.[8]

The use of hybrid warfare in the Middle East became recognised during the Lebanon War in 2006, when Hezbollah fought a multifaceted campaign against Israel, blending conventional (the use of rocket bombardments of northern Israel and employing robust anti-tank warfare against Israeli armour) with unconventional methods (such as the use of improvised explosive devices) and cyber-based operations (such as the sending of text messages of an official character to Israeli mobile phone users notifying them of the false death of a soldier on the front).[9] Frank Hoffman described Hezbollah's methods as constituting both hybrid threats and hybrid warfare.[10]

More recent examples include Russia's involvement in the conflict in Ukraine, and IS operations

in Iraq and Syria, as well as its recent recruitment and radicalisation campaigns in EU countries for the 'jihad' in Syria and 'martyrdom' operations in Europe. These examples use a holistic mix of conventional and non-conventional forms of warfare, information operations, lawfare and cyber-attacks, aimed at testing the resilience of the affected states and societies. The way the current GCC crisis has unfolded allows for some comparison with these conflicts and how methods of hybrid warfare are being employed to exploit vulnerabilities and lack of resilience, both as measures and countermeasures.

As early as 2010, NATO identified 'hybrid threats' as low-intensity, kinetic and non-kinetic threats to international peace and security, including cyber war, low-intensity asymmetric conflict scenarios, global terrorism, piracy, transnational organised crime, demographic challenges, resources, security, retrenchment from globalisation, and the proliferation of weapons of mass destruction.[11]

One such type of hybrid threat is cyber threats, which constitute threats in the 'fifth dimension' of warfare, as cyberwarfare is often described.[12] Cyber threats refer to sustained campaigns of concerted cyber operations against the IT infrastructure of a targeted state, including mass web disruption, spam use and malware infection.[13]

While cyber-attacks do not involve the use of force *per se*, their effects in terms of loss of life and material damage to property may be comparable to the effects of an armed attack. Indeed, the *Tallinn Manual*, authored by a panel of international experts and published by NATO's Cooperative Cyber Defence Centre of Excellence in 2013, contends that cyber-attacks, if they cause death, injury or damage, can be regarded as the use of force.[14]

Cyber-attacks can therefore constitute a method of warfighting *sui generis*, as evident in Russia's cyber-attack on Estonia in 2009, or as part of a conventional military campaign in a supporting role and function. The use of cyber as a force multiplier was also evident in Russia's use to augment its military capabilities during its military campaigns against Georgia in 2008, and more recently in Ukraine since 2014.[15]

Between 2010 and 2012, NATO—recognising hybrid threats as a major risk—began work to identify these threats and define a comprehensive approach for countering them by including state and non-state actors in a comprehensive defence strategy. According to NATO's

Bi-Strategic Command Capstone Concept of 2010, hybrid threats represent complex and non-linear threats that are difficult to resolve using one-dimensional measures such as military action.[16] Specifically, hybrid threats are defined by NATO as 'those threats posed by adversaries with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives'.

Perhaps short-sightedly, given Russia's aggression in Eastern Europe, this project was discontinued in 2012 due to lack of support from NATO members. However, in December 2015, NATO announced the development of a new *Hybrid Warfare Strategy* which, in essence, recognises the existing capstone document of 2010 as a blueprint for countering hybrid threats 'in a comprehensive way [and] in the complex geostrategic environment posed by globalisation'.[17] That clearly was in response to events in Ukraine and Russia's annexation of Crimea, in which Russia used security, military, political, legal, informational, technical and economic means to advance its interests.

Another element of hybrid warfare can be the use of 'lawfare', the use of law as a weapon.[18] Russia has succeeded in using law as a means of warfare in its movement into Crimea, as the absence of a clear definition of the nature of 'intervention' has made the action difficult to categorise in international law. As a result, in addition to Russia's denial of these actions, the legal assessment in terms of legality/illegality has become a partisan undertaking.[19] What has become clear is that countering hybrid threats/warfare will shape NATO's future role in addressing armed conflict and global risk and crisis management.

Recent cyber-attacks in the Gulf as a precursor to the current crisis

Even before the current crisis, Qatar and other GCC states recognised their vulnerability to cyber-attacks on their critical infrastructure, not least because of prior attacks directed against Qatar and Saudi Arabia. In 2015, Qatar's Minister of Information and Communication Technology asserted that protecting the nation's critical infrastructure is a key objective of its cybersecurity policy:

> Qatar has taken steps for transitioning from a traditional hydrocarbon-based economy to a digital economy…. However, digital inter-connectedness is only beneficial if we can ensure our citizens and businesses are safe in the digital world that we are transitioning to a digital government.[20]

Security experts have hinted that Qatar may face a high risk of cyber-attacks as the host of the upcoming FIFA 2022 World Cup, cautioning that the nation's financial, oil and gas sectors continue to be vulnerable to cyber-attacks.[21] Indeed, an increasing number of cyber-attacks have recently been reported in the Gulf. In 2012, Qatar's second-largest liquefied natural gas producer, RasGas, was attacked by Shamoon, a computer virus that caused its system to go offline.[22] Earlier, in 2010, it was reported that a sophisticated virus/worm called Stuxnet had been used, allegedly by Israel and/or the US, to sabotage Iran's nuclear weapons program.[23]

This vulnerability and the occurrence of such attacks makes Qatar (and other GCC states) an interesting case study for examining the nature and form of cyber-attacks in terms of the *Tallinn* guidelines, and as a form of hybrid threat or a method of hybrid warfare. With its vast reserves of natural resources and critical infrastructure, and its strategic position in the Persian Gulf, Qatar is particularly vulnerable to cyber and hybrid attacks.

The Saudi Arabian Oil Company)ARAMCO) was hacked in 2015, an act that has been described as one of the most severe in the history of the GCC.[24] The impact of this cyber-attack and its exploitation of network-related vulnerabilities shook the confidence of Saudi Arabia's global business partners and contractors of ARAMCO. The GCC position has been that this attack originated from or on behalf of Iran, and led to a consensus of how to improve resilience and develop counter-attack options in the future. That leads to the question of whether other GCC states would have protected each other in such instances prior to the current GCC crisis, given the lack of a regional defence consensus or arrangement.

The use of hybrid warfare in the current Qatar-GCC crisis

In early June 2017, three GCC member states (Saudi Arabia, UAE and Bahrain) cut diplomatic ties with Qatar, imposed a trade embargo, and expelled Qatari nationals from their territories, as well as banning any travel to Qatar. These measures were justified as constituting a legitimate response and countermeasure to Qatar's continuing support for terrorist organisations in the region.[25]

The boycott/embargo was supported by several regional but non-GCC states, such as Egypt, Jordan, Yemen and other countries that are generally seen to follow or be influenced by GCC countries. The ensuing crisis was further escalated by President Trump's statement on Twitter that Qatar 'has been a funder of terrorism at a very high level', which directly contradicted Secretary of State Tillerson's attempts to ease tension in the region.[26]

The present anti-Qatar policy is a model mix of 'diplomatic, information, military, and economic' actions, targeting political, military, economic, social, information and infrastructure effects.[27] The Saudi and UAE-led blockade was supported by classical 'soft power' action, notably Saudi Arabia's decision to close its land border with Qatar, the only land border of the Qatari peninsula. The 'blockade' countries have also blocked their respective air space for any air travel to and from Qatar.

The blockade policy by Saudi Arabia and UAE, utilising a means short of the use of force, falls within the operational spectrum of hybrid warfare. Given that the blockade has been augmented by other supporting action, which also falls under the wider umbrella of hybrid warfare, it seems appropriate to view the current GCC situation as falling within the wider hybrid warfare/hybrid threats warfare spectrum. Other examples include exercising direct pressure on religious leaders in Qatar, and the use of the international media and information sphere to support Saudi Arabia's narrative of Qatar's terrorism links, as well as the attempt to use Arab writers, intellectuals and tribal leaders to take a stance against Qatar's government.

The blockade of Qatar's sea, land and air borders prevented Qatari citizens from entering or leaving the country. They were also forced to leave the affected states (and Saudi and UAE citizens residing in Qatar were forced to leave Qatar in response to pressure from their home countries). These actions, which violate both international law and GCC law, have surprised both the Qatari people and their government, particularly given the close links within GCC member-states along and across tribal and family lines.

Saudi Arabia's decision also to send back camels (and sheep) from Saudi Arabia to Qatar has hit a particular raw nerve in the Arab nation due to its cultural attachment to camels.[28] Camels are not only the main means of transport in the region but are synonymous with the region's pre-petroleum wealth. Saudi Arabia also imposed conditions on pilgrims from Qatar arriving in the country for the annual Hajj of 2017, which was more-widely condemned as affecting their freedom of religion.[29]

The current crisis commenced with a cyber-attack targeting the Qatar News Agency and the uploading of fake news involving statements allegedly made by the Emir of Qatar (which he later accused some of the embargoing countries of using as a pretext to carry out the blockade).[30] *The Washington Post* reported in mid-July that the UAE may have been behind this cyber operation.[31]

The Gulf states' campaign against Qatar has the hallmarks of a hybrid warfare campaign, combining a variety of non-kinetic means and tools, including information operations, economic and diplomatic blockade, and cyber operations. Missing so far has been the use of covert operatives, so-called local volunteers and other non-attributable operatives, to escalate the conflict to the next stage, which would turn the present crisis into a fully-fledged hybrid warfare campaign comparable to Russia's Crimea campaign of 2014.

The use of hybrid warfare is not new to the GCC. Another example of such multi-modal hybrid warfare could be seen in the Bahraini protests of 2011. Bahrain has a population of various religions and sects (predominantly Sunni

and Shia). In 2011, demonstrators in Bahrain demanded improved economic conditions and human rights. What began as a local protest became a hybrid threat when peaceful gatherings turned into a sectarian protest of the Shia minority against the rule of the Sunni Emir. The protestors were edged on by Shia leaders from Iran and its Lebanese affiliate Hezbollah, media outlets in Iran, and Hezbollah-supported protestors on the ground.

This turned the original protests into a Sunni-Shia conflict, with an increase in violence originating from domestic and outside actors aimed at the government of the state. The situation became so volatile that Bahrain had to ask for military assistance from a Saudi-led GCC coalition. This could be considered an example of hybrid warfare, as internal unrest was turned into a regional security threat with the support of an external state (Iran) and its non-state affiliates. Iran, while denying any interest and involvement, used diplomacy, media operations and eventually lawfare to support the unrest in a fashion used successfully by Russia three years later in Crimean.[32]

Conclusion

It seems that the Gulf states continue to be vulnerable to both unconventional warfare and hybrid attacks alike, whether originating from GCC states, other states or non-state actors. The only solution would seem to lie in the development of an effective GCC defence arrangement, rather than the continuation of unilateral efforts—which create vulnerabilities on their own and often lead to an increase in mutual distrust among the GCC nations. It is also clearly important, both for regional and broader global stability, that the situation returns to a pre-crisis status quo.

Qatar's answer to the current crisis is not an easy one. Indeed, given the quantity and quality of the hybrid warfare campaign being targeted at it, the response will require an equally comprehensive approach combining diplomacy, lawfare, information operations and economic countermeasures. The question remains, which countermeasures should Qatar employ and what would be the ramifications. For example, were Qatar to use Al Jazeera more aggressively, as a propaganda tool in the information sphere, how would that play out? Could it escalate or deescalate the situation?

Similarly, if Qatar were to deploy cyber countermeasures against Saudi Arabia, what could be achieved and how would this play out in terms of achieving the overall objective of resolving the present crisis? Is Qatar, realistically, able to do very much, apart from sticking to the lawful response through lawfare? The Charter of the GCC may be the legislative instrument to address this situation. However, to date, the Charter has largely only dealt with administrative matters. So attempting to elevate the Charter to security issues may put the cooperative future of the GCC at stake.

At present, Qatar seems inclined to utilise hybrid countermeasures, using 'lawfare' in the wider sense, by making a legal complaint to the World Trade Organization over the economic blockade, and complaining to the International Civil Aviation Organization, albeit without success to date.[33] It has also increased its production of liquid gas by 30 per cent as an economic countermeasure, as well as utilising trade and diplomacy as strategic leverage.[34]

Given the continuing strategic relevance of the GCC region for US and European foreign policy, the re-emergence of the threat posed by Iran, and the need to reduce tensions among GCC member-states in order to maintain US (and other) strategic interests in terms of trade and strategic cooperation, it seems likely that the crisis will be resolved in the not too distant future. In the meantime, it is a good example of the broadening use and prospective success of hybrid warfare.

Sascha-Dominik Dov Bachmann is an Associate Professor in International Law at Bournemouth University (UK) and Associate Professor in War Studies at the Swedish Defence University. As a reservist in the German Army, he served in peacekeeping missions in an operational and advisory capacity. He took part as NATO's 'rule of law subject-matter expert' in NATO's 'Hybrid Threat Experiment' of 2011 and in related workshops at NATO and national level. He has widely written on the subject of hybrid threats/warfare and lawfare from an operational perspective.

Notes

1 See P. Danahar, *The New Middle East: the world after the Arab Spring*, Bloomsbury: London, 2013 for an authoritative introduction and discussion of the term within its political and historical context.

2 Trading Economic, 'Crude oil production', *Trading Economic* [website], available at <https://tradingeconomics.com/country-list/crude-oil-production> accessed 18 July 2017; *Arab News*, 'GCC share of global oil reserves likely to raise to 70%', *Arab News* [website], available at <http://www.arabnews.com/gcc-share-global-oil-reserves-likely-rise-70> accessed 18 July 2017.

3 See, for example, the British position highlighted in *Al Jazeera*, 'Britain to deepen security cooperation with the GCC', *Al Jazeera* [website], 7 December 2016, available at <http://www.aljazeera.com/news/2016/12/britain-deepen-security-cooperation-gcc-161207102311180.html> accessed 18 July 2017; see also *SUSRIS,* 'US-GCC Strategic Cooperation Forum', available at <http://susris.com/glossary/us-gcc-strategic-cooperation-forum/> accessed 18 July 2017.

4 For an English version, see International Relations and Security Network (SRN), 'Charter of the Gulf Cooperation Council (GCC)', *SRN* [website], available at <https://www.files.ethz.ch/isn/125347/1426_GCC.pdf> accessed 20 July 2017.

5 See Human Rights Watch, 'GCC: joint security agreement imperils rights', *Human Rights Watch* [website], 26 April 2014, available at <https://www.hrw.org/news/2014/04/26/gcc-joint-security-agreement-imperils-rights> accessed 20 July 2017.

6 See, for example, C. Koch, 'The GCC as a regional security organization', *KAS International Reports* [website], <http://www.kas.de/wf/doc/kas_21076-544-2-30.pdf?101110135754> accessed 18 July 2017.

7 S.D. Bachmann and A.B.M. Mosquera, 'Lawfare and hybrid warfare –how Russia is using the law as a weapon', *Amicus Curiae*, Issue 102, 2015, abstract available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2841277> accessed 17 July 2017.

8 S.D. Bachmann and H. Gunneriusson, 'Eyes wide shut: how Russia's hybrid warfare exposes and exploits Western vulnerabilities', *Georgetown Journal of International Affairs*, 18 January 2017, available at <http://journal.georgetown.edu/eyes-wide-shut-how-russias-hybrid-warfare-exposes-and-exploits-western-vulnerabilities/> accessed 17 July 2017.

9 F.G. Hoffman, *Conflict in the 21st century: the rise of hybrid wars*, Potomac Institute for Policy Studies: Arlington, 2007, p. 37.

10 Hoffman revisited his discussion of the hybridity of Hezbollah's warfighting approach in subsequent academic works where he discussed the interchangeable nature of the terms hybrid threats and warfare. See, for example, F.G. Hoffman, 'Hybrid warfare and challenges', *Joint Forces Quarterly*, Issue 52, 1st Quarter 2009, pp. 1-2; and F.G. Hoffman, 'Hybrid vs. compound war: the Janus choice of modern war: defining today's multifaceted conflict', *Armed Forces Journal*, October 2009, pp. 1-2.

11 S. Bachmann, 'Hybrid threats, cyber warfare and NATO's comprehensive approach for countering 21st century threats—mapping the new frontier of global risk and security management', *Amicus Curiae*, Issue 88, January 2012; and NATO, 'NATO countering the hybrid threat', *NATO* [website], available at <http://www.act.nato.int/nato-countering-the-hybrid-threat> accessed 17 July 2017.

12 S. Bachmann and H. Gunnariusson, 'Russia's hybrid warfare in the East: the integral nature of the information sphere', *Georgetown Journal of International Affairs*, 2015, pp. 198-212.

13 S. Bachmann and H. Gunnariusson, 'Hybrid wars: the 21st century's new threats to global peace and security', *South African Journal of Military Studies*, Issue 43, No. 1, 2015, pp. 77-98.

14 See the latest edition at Cooperative Cyber Defence Centre of Excellence, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, 2017, available at <https://ccdcoe.org/tallinn-manual-20-international-law-applicable-cyber-operations-be-launched.html> accessed 25 January 2018.

15 Bachmann and Gunneriusson, 'Eyes wide shut'.

16 P. Fleming, 'The hybrid threat concept: contemporary war, military planning and the advent of unrestricted operational art', *Homeland Security Digital Library* [website], available at <https://www.hsdl.org/?view&did=700828/> accessed 17 July 2017.

17 NATO, 'Press statements by the NATO Secretary General Jens Stoltenberg and the EU High Representative for Foreign Affairs and Security Policy, Federica Mogherini, 1 December 2015', *NATO* [website], available at <http://www.nato.int/cps/en/natohq/opinions_125361.htm> accessed 17 November 2015.

18 S.D. Bachmann and A.B.M. Mosquera, 'Lawfare in hybrid wars: the 21st century warfare', *Journal of International Humanitarian Legal Studies*, Issue 7, 2016, p. 63, with reference to Dunlap who coined the term in 2001.

19 S.D. Bachmann and A.B.M. Mosquera, 'Lawfare and hybrid warfare –how Russia is using the law as a weapon', *Amicus Curiae*, Issue 102, 2015.

20 H. al-Jaber, 'Protecting critical infrastructure key to Qatar's cyber security approach', *Gulf Times* [website], 19 April 2015, available at <http://www.gulf-times.com/qatar/178/details/435549/%E2%80%98protecting-critical-infrastructure-key-to-qatar%E2%80%99s-cyber-security-approach%E2%80%99> accessed 23 November 2015.

21 Aarti Nagraj, 'Qatar faces high risk of cyber-attacks during FIFA 2022 World Cup', *Gulf Business* [website], 23 April 2015, available at <http://gulfbusiness.com/qatar-faces-high-risk-cyber-attacks-fifa-2022-world-cup/> accessed 24 November 2015.

22 *The New Arab*, 'GCC businesses are facing a major cybersecurity deficit', *The New Arab* [website], 12 June 2017, available at <https://www.alaraby.co.uk/english/comment/2017/6/12/gcc-businesses-are-facing-a-major-cybersecurity-deficit> accessed 3 June 2017; P. Paganini, 'RasGas, new cyber-attack against an energy company', *Security Affairs* [website], 31 August 2012, available at <http://securityaffairs.co/wordpress/8332/malware/rasgas-new-cyber-attack-against-an-energy-company.html> accessed 3 August 2017.

23 C. Williams, 'Stuxnet: cyber-attack on Iran "was carried out by Western powers and Israel"', *The Telegraph*

[website], 21 January 2011, available at <http://www.telegraph.co.uk/technology/8274009/Stuxnet-Cyber-attack-on-Iran-was-carried-out-by-Western-powers-and-Israel.htm> accessed 25 January 2018.

24 J. Pagliery, 'The inside story of the biggest hack in history', *CNNMoney* [website], 5 August 2015, available at <http://money.cnn.com/2015/08/05/technology/aramco-hack/index.html> accessed 20 July 2017.

25 For a short overview, see *BBC News*, 'Qatar crisis: what you need to know', *BBC News* [website], 5 July 2017, available at <http://www.bbc.co.uk/news/world-middle-east-40173757> accessed 3 August 2017.

26 *The Guardian*, 'Gulf crisis: Trump escalates row by accusing Qatar of sponsoring terror', *The Guardian* [website], available at <https://www.theguardian.com/us-news/2017/jun/09/trump-qatar-sponsor-terrorism-middle-east> accessed 20 July 2017.

27 R. Hillson, 'The DIME/PMESII Model Suite Requirements Project', *NRL Review* [website], available at <https://www.nrl.navy.mil/content_images/09_Simulation_Hillson.pdf> accessed 20 July 2017.

28 Bethany Allen-Ebrahimian, 'Saudi Arabia deports 15,000 Qatari camels', *Foreign Policy* [website], 20 June 2017, available at <http://foreignpolicy.com/2017/06/20/saudi-arabia-deports-qatari-camels-gulf-diplomacy/> accessed 20 July 2017.

29 The Euro-Mediterranean Human Rights Monitor, 'New report: travel restrictions on Qataris seeking to perform religious rituals in Saudi Arabia is serious violation that requires investigation', *The Euro-Mediterranean Human Rights Monitor* [website], 21 November 2017, available at <https://euromedmonitor.org/en/article/2180/New-report:-Travel-restrictions-on-Qataris-seeking-to-perform-religious-rituals-in-Saudi-Arabia-is-serious-violation-that-requires-investigation> accessed 25 January 2018.

30 See, for example, R. Windrem and W. Arkin, 'Who planted the fake news at center of Qatar crisis', *NBC News* [website], 18 July 2017, available at <http://www.nbcnews.com/news/world/who-planted-fake-news-center-qatar-crisis-n784056> accessed 20 July 2017.

31 Karen DeYoung and Ellen Nakashima, 'UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to US intelligence officials', *Washington Post* [website], 16 July 2017, available at <http://wapo.st/2tvcnXx?tid=ss_tw&utm_term=.2c9ddcf63846> accessed 20 July 2017.

32 M. Slackman, 'The proxy battle in Bahrain' *The New York Times* [website], 19 March 2011, available at <http://www.nytimes.com/2011/03/20/weekinreview/20proxy.html> accessed 25 January 2018.

33 Reuters, 'Qatar makes legal complaint over Gulf trade boycott', *The Guardian* [website], 1 August 2017, available at <https://www.theguardian.com/world/2017/jul/31/qatar-makes-legal-complaint-to-wto-over-gulf-trade-boycott> accessed 25 January 2018.

34 Reuters, 'Qatar announces huge raise in gas production amid diplomatic crisis', *CNBC* [website], 4 July 2017, available at <https://www.cnbc.com/2017/07/04/qatar-ratchets-up-gas-production-30-percent-despite-sanctions.html> accessed 25 January 2018. See also The Associated Press, 'Seeking closer ties, Qatar to expand base used by US troops', *Military.com* [website], 1 February 2018, available at <https://www.military.com/daily-news/2018/02/01/seeking-closer-ties-qatar-expand-base-used-us-troops.html> accessed 5 February 2018; and UK Ministry of Defence, 'Defence Secretary signs multi billion pound jet contract with Qatar', *Ministry of Defence* [website], 7 December 2017, available at <https://www.contracts.mod.uk/do-features-and-articles/defence-secretary-signs-multi-billion-pound-jet-contract-with-qatar/> accessed 5 February 2018.

Bridging the gap between cyber strategy and operations: a missing layer of policy

Major Christopher Wardrop, Australian Army

Introduction

Whether one is a proponent of the 'information revolution' or a more gradual evolution in the development, use and reach of information communications technology, there can be no denying that the emergence of cyberspace and the ever-increasing interconnectedness of technology has had significant social, economic and political effect in Australia and globally.[1]

In 2005, Charles Weiss detailed how advances in science and technology have subtly yet fundamentally altered concepts of security, sovereignty and power.[2] Developed and developing nations are coming to understand, prioritise and deal with these changes differently, as reflected through the variety of approaches taken in national cyber strategy documents.[3]

The Australian Government recognises that the cyber threat is increasing and presents a genuine risk to Australia's national security and economic prosperity, as well as the ADF's warfighting capability.[4] Indeed, the unique characteristics of cyber operations present one of the most significant challenges to modernisation of the ADF, with the *2016 Defence White Paper* emphasising the importance of strengthening national cyber capabilities.[5]

Australia's current cyber security strategy commits $400 million to strengthening cyber capabilities over the next ten years but does not include any specific tasks, roles or responsibilities for the ADF.[6] As observed by then Brigadier Marcus Thompson, the *2016 Defence White Paper* 'emphasises the development of cyber security capabilities'—and Australia's investment program funds such development—yet 'an additional layer of actionable policy is required to ensure appropriate implementation of the Government's intent at the operational and tactical levels'.[7]

This article seeks to identify who is responsible for formulating and enacting the policy to

bridge the gap between strategic intent and operational planning and implementation. It also defines the cyber domain and threats, identifies the key challenges of military cyber operations, and examines the trajectory for the growth of cyber capabilities within the ADF.

One of the challenges of this analysis in the Australian context is the lack of operational policy and doctrine in the public domain. It is likely that many of the considerations discussed below have already been made and that a large body of work has been completed or is well underway. This is, of course, a problem in itself, as the limited distribution of such policy does little to raise awareness or encourage discussion of cyber security and operational issues more broadly among Defence commanders and their headquarters staff.

Responsibility

In a sign of the importance that the Australian Government places on cyber security, its most recent cyber security strategy was released by the Department of the Prime Minister and Cabinet, rather than the Attorney-General's Department (which had previous carriage of cyber policy).[8]

Within Defence, responsibility for the development of policy on cyber operations has not always been clear, with no champion until relatively recently. However, the Vice Chief of the Defence Force is now the capability manager, with the newly-formed Information Warfare Division, part of Joint Capabilities Group, having responsibility to identify existing cyber capabilities and gaps, develop a coherent joint capability, and integrate cyber operations into and across Defence.[9]

It is recognised, however, that the development of policy and doctrine has a broad range of stakeholders, including the Prime Minister and Cabinet, law-enforcement agencies, strategic intelligence agencies, Headquarters Joint Operations Command, the three Services, and defence industry and its commercial partners, as well as Australia's allies and coalition partners.

This means that while the Vice Chief of the Defence Force is ultimately responsible for the development and implementation of military-related cyber capabilities, policy must be developed with broad consultation and cooperation in order to be effective.

Characteristics of the cyber domain

To formulate any policy to bridge the gap between Australian cyber strategy and operational-level requirements, it is vitally important to first understand both the technological context in which Defence operates and the key characteristics of cyberspace and the cyber domain.

Since 2008, the ADF has made significant progress in improving its command, control, computing, communications, intelligence, surveillance and reconnaissance (C4ISR) capabilities.[10] Much of this progress has been made through the acquisition of major platforms by Navy and Air Force, and ongoing efforts to digitise and modernise Army's command, control and communications systems.[11]

Modern Western military forces have relied on communications networks and technology to enable 'decision superiority' to bring overwhelmingly lethal force to bear at decisive moments in space and time, with the conventional joint land combat phases of the 1991 Gulf War and the 2003 Iraq War often cited as striking examples of the military success that decision superiority can afford.[12] More recent experiences, notably in Iraq and Afghanistan, have shown the inherent difficulties in achieving the degree of situational awareness required to enable decision superiority when engaged against insurgent and irregular forces capable of concealing themselves within the population.[13]

The complex, interconnected systems that modern military forces have become reliant on to gain and maintain a high degree of situational awareness are increasingly vulnerable to infiltration and disruption through cyberspace. As noted by Major General Fergus McLachlan in 2015, '[modern C4ISR systems are] no longer stand alone or isolated'.[14] Current adversaries, such as Islamic State—and future adversaries, be they state or non-state actors—will attempt to exploit these systems for their own military advantage through cyberspace.

A well-formed and pragmatic concept of cyberspace is the logical starting place for any policy attempting to bridge the gap between national strategic intent and operational implementation. In the Defence context, cyberspace is more commonly referred to as the cyber domain. This fits with the past conceptualisation of land, sea, air and space as warfighting domains.

Defence is presently grappling with the emergence of cyber as an additional domain for its military planning, even while the multi-domain warfare construct comes under increasing criticism, including from Australia's current Vice Chief of Defence Force.[15] Indeed, neither the *2016 Defence White Paper* nor Australia's current cyber security strategy provide an adequate conceptualisation of the cyber domain for Defence's operational purposes. However, feasible definitions and concepts can be found in the strategy documents and doctrine of others, and among a range of academic works, which are explored below.

Firstly, it is useful to recognise that the cyber domain is both physical and non-physical. Physical aspects of the domain include international submarine communications cables, satellites, network routers, wireless infrastructure, servers, computers, industrial control modules and every smart device with Internet connectivity. Non-physical aspects of the cyber domain include the data and knowledge that is created in or flows through cyberspace; software for the creation, collection and dissemination of data; codes for the control of financial and industrial systems; and malicious software, cyber weapons and the codes to counter them.[16]

While this duality sets the cyber domain apart from land, sea, air and space, it is not a completely unique concept. ADF operational doctrine currently includes domain concepts which comprise both physical and non-physical components.[17] So the cyber domain could easily be adapted as an additional domain, connected with the existing domains of land, sea, air and space.

Secondly, it must be understood that the cyber domain is man-made, continually increasing in complexity, and in a state of 'constant flux based on the ingenuity and participation of [its] users'.[18] In many ways, this sets the cyber domain apart from the traditional domains, as the cost of participation can be exceptionally low, technological growth and application may occur in non-linear ways, and actors and their actions are difficult to identify.

Finally, there is significant overlap between the cyber domain and the existing domains. This is true with both physical connection to land, air, sea and space domains, and physical and non-physical interactions with the information and human domains. The role of Internet communications and social media in galvanising public unrest—from Tunisia to Wall Street—demonstrates the clear overlap between the cyber and information domains, and the cyber and human domains.[19]

The real world impact of cyber weapons, exemplified in the reported physical effects of the Stuxnet virus in its attack on Iranian nuclear facilities, is an unequivocal illustration of the overlap between the physical domain and the vulnerability of 'stand-alone' systems.[20] While Stuxnet remains an outlier in terms of sophistication, complexity and consequence, it nevertheless serves to demonstrate the vulnerability of 'stand-alone' systems and the potential military and national security implications of threats generated through the cyber domain.

Any policy intended to bridge the gap between strategic intent and operational capabilities and objectives should contain a concept of the cyber domain that accounts for Defence's technological context and the characteristics of the cyber domain. The development of such a concept from the existing information domain concept, rather than from the environmental domains, would seem to be more in line with Vice Admiral Grigg's views on designing and building an integrated force.[21] Furthermore, it would clearly show how 'cyber space unifies all domains of warfare, especially its political control and political impacts',[22] as presented schematically at Figure 1.

While certainly not being the only possible conceptualisation of the cyber domain, it is the author's view that this model, or one similar to it, would prove most useful in any policy intended to bridge the gap between Australian cyber strategy and the application of the Government's intent at the operational and tactical levels. In this model, the cyber domain underpins

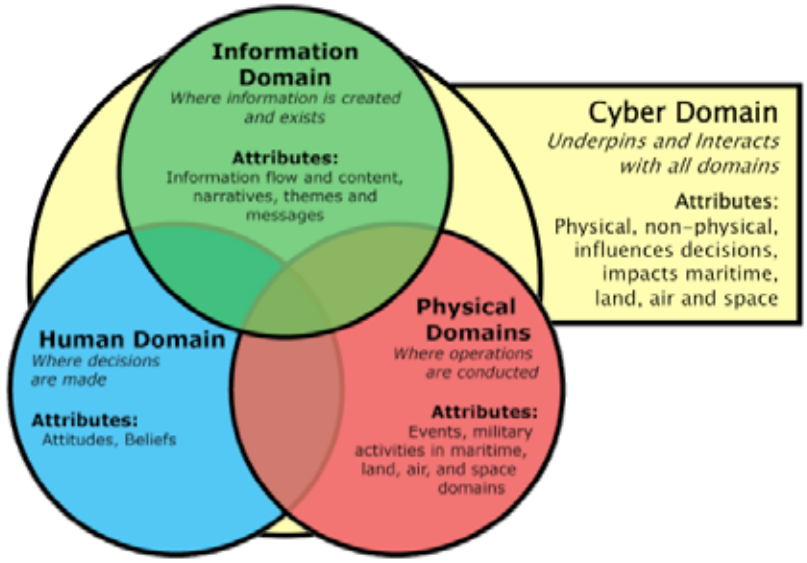


Figure 1: How cyber can unify the traditional domains of warfare (as adapted by the author)

and interacts with the information, human and physical domains. The level of interaction would increase over time as individual and societal levels of inter-connectedness continue to increase.

Understanding the threats

With a model of the cyber domain in place, the next logical step in bridging the gap between strategic intent and operational effects is an understanding of the likely threats. There is little by way of consensus to be found in allied policy and doctrine or academic works regarding threat models. Several commentators have identified 'attack vectors' or 'types of attacks', while US doctrine identifies specific countries and groups as 'threat actors'.[23] Neither approach, however, is particularly well suited to policy intended to bridge the gap between national strategy and operational capabilities and effects.

Ronald Deibert and Rafal Rohozinski identify 'risks to cyberspace' and 'risks through cyberspace' although, in a military policy and doctrinal context, they are in fact discussing threats.[24] Their threat model lends itself well to operational policy and doctrine, where threats to the cyber domain would include any threats to the physical elements of cyberspace, including networked military hardware and stand-alone government, military and industrial systems. Expanding on this idea, these threats may come from cyber weapons being used to infiltrate and disrupt information communications technology, or as physical attacks on network infrastructure, hardware or power supplies.

One of the more obvious examples of threats through the cyber domain is the spread of extremist ideology inspiring disenfranchised individuals to conduct attacks in Western countries. The spread of knowledge and ideas via the cyber domain has been exploited by issue-motivated groups to mobilise protests which triggered regime change in Egypt and, separately, in Tunisia in 2011.[25] While the cyber domain was not the decisive domain in either example, both serve as case studies to illustrate how the cyber domain underpins and interacts with the physical, information and human domains. Other threats through the cyber domain include fraud, blackmail, unauthorised disclosure and espionage.

While the above model is an effective treatment of the types of threats, it does not address the potential threat actors. For this, the work by Richard Harknett is useful in his categorisation of threat actors as state actors, state proxies or non-state actors.[26]

For example, the US has identified China, Russia, Iran and North Korea as the most prominent states actors in the cyber domain. States

are somewhat constrained by international law, norms, diplomacy and deterrence; however, they may take increased risks in the cyber domain due to the inherent difficulty in attributing and responding to attacks.

State proxies are reliant on states for funding, training and technological access. State proxies are able to conduct cyber operations while their sponsor maintains plausible deniability. China, in particular, has focused on making maximum use of the skills present in its civilian workforce to develop 'cyber militias', which could potentially be categorised as state-proxies depending on how they are employed.[27]

Non-state actors range from criminal groups committing fraud via the Internet to violent extremists, such as Islamic State, which pursue aggressive intelligence gathering and propaganda campaigns. The absence of state control reduces the constraints on such groups, with the cyber domain enabling them exponentially to increase their reach.

The potential threat posed by any of these threat actors needs to be analysed in relation to the specific operational context. Any group may pose a threat to the cyber domain or a threat through the cyber domain, depending on their capability and intent. For example, threats to stand-alone industrial control systems, intended to cause physical damage, require greater skills, knowledge, resources and time than hasty propaganda campaigns intended to sway public opinion. A depiction of the potential targets of threat actors is shown at Figure 2.

The incorporation into ADF doctrine of a cyber domain concept and threat model similar to that discussed above would provide military intelligence professionals, planners and commanders with pragmatic tools for understanding the cyber operating environment, analysing threats to and through cyberspace, and developing concepts of cyber operations.

Challenges of cyber operations

The nature of the cyber domain, its characteristics and the threat types and actors all combine to create a series of challenges for the

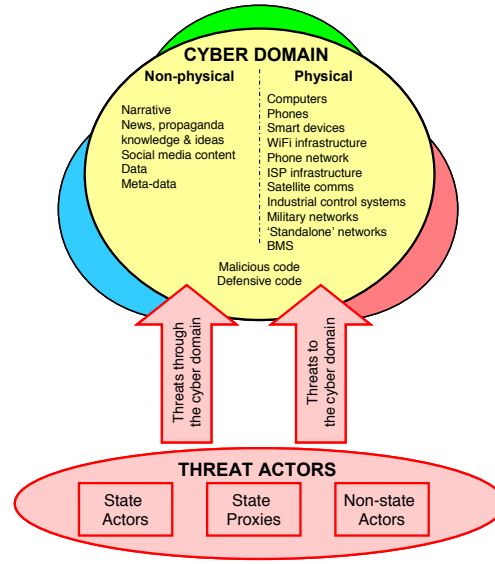


Figure 2: The potential targets of threat actors in the cyber domain (as adapted by the author)

application of cyber effects in a military context. It is these challenges that will be the most difficult for policy to address. The ubiquitous and borderless nature of the cyber domain, combined with the relative anonymity of actors and inherent difficulties in technical, legal and political attribution, have potentially fundamental effects on traditional national security concepts of defence and deterrence.[28]

Traditional notions of deterrence through military power are likely to be ineffectual against dispersed non-state actors and state-proxies that fear neither attribution nor retaliation.[29] Even ignoring the difficulties of attribution, effective deterrence requires the threat actor to understand to some degree the retaliatory capabilities of their target. The current level of secrecy surrounding Australian offensive cyber operations prevents that, and potentially undermines any deterrent effect.

Effective geographic defence of the cyber domain is technically not feasible, meaning the extension of sovereignty into the cyber domain is highly problematic. Traditional notions of defence are reliant on military power to seize and hold territory, control sea lines of communication and exert air superiority. Such actions are not possible in a borderless, highly complex and constantly evolving domain. Instead the cyber

domain offers ever-increasing opportunities for weak military powers and non-state actors to infiltrate, disrupt and degrade stronger adversaries.[30]

With the increasing importance of the cyber domain to Western notions of war, and a desire for decision superiority (or at least ever-increasing situational awareness), comes the many challenges of 'distributed warfare'.[31] Through the development of cyber capabilities, military units are likely to possess increased coercive powers. There will be increased cross-over between military and civilian organisations, and blurred lines between state, state proxies and non-state actors. Furthermore, deployed units will not be able to rely on a permanent link with higher headquarters in a disputed cyber and information environment. This serves to add to the complexity and uncertainty of military operations.

It is these challenges, and likely many others that have not yet been identified, that must be addressed—in terms of force structure, authorities, training and education, as well as platform and technical superiority—in any policy that aims to bridge the gap between strategy and operations.

Policy and force structure

As the ADF grows its cyber operations capability, commensurate policy and doctrine will be required to ensure continuing alignment with strategic objectives. Much of what has been discussed under the characteristics of the cyber domain and understanding the threat would neatly fit into joint doctrine. But doctrine alone will only partially bridge the gap between strategic intent and operational and tactical implementation. Specific policy, formulated by Joint Capabilities Group and endorsed by the Service chiefs, will be required to ensure that force structure, rules of engagement, research and development, and recruitment, among other considerations, are aligned with strategic intent.

US Cyber Command has provided some good insights into what that policy might cover.[32] However, to be truly useful, any Australian equivalent would need to be less aspirational and include quantifiable tasks. Drawing on the US example, Australian policy should also emphasise that cyber capabilities are 'not administered but rather led by commanders who understand they are always in real or imminent contact with [their] adversaries'.

That would ensure that cyber security and the cyber domain moves beyond the realm of technical specialists and into the common understanding of all military commanders and headquarters staff. Achieving this will require supporting direction in relation to cyber education, training and exercises, as well as force structure to ensure commanders are adequately supported to enable them to lead cyber alongside conventional capabilities.

Australian military cyber operations policy must also address the mission or, perhaps more appropriately, likely cyber tasks or cyber actions. Currently, there is scant discussion of the cyber mission in the public domain beyond an 'aim to retain freedom of manoeuvre in cyberspace, accomplish the joint force commander's objectives, deny freedom of action to adversaries, and enable other operational activities'.[33]

To date, cyber actions discussed publicly have been 'cyberspace defence', 'cyberspace security', and 'routine actions in cyberspace'.[34] However, such actions require considerable elaboration to be applicable to operational and tactical commanders. Furthermore, there is an obvious lack of discussion regarding offensive cyber capabilities that must be addressed more openly if the ADF is to catch up with the US and meet the stated strategic objective of Australia's defensive and offensive cyber capabilities as '[enabling deterrence and response] to the threat of cyber-attack'.[35]

However, directions to commanders, the development of policy to increase cyber education, training and exercises, and a defined cyber mission and detailed tasks will all be of little practical relevance without the manning and force structure to support them. The $400 million committed to strengthen cyber capabilities over the next ten years pales in comparison to the US Department of Defense's $6.7 billion budget for cyber operations in 2017.[36]

Even ignoring the order-of-magnitude funding disparity, the ADF is simply too small for the establishment of a Cyber Command similar to the US model. In his 2015 presentation on the

Australian Army's future force structure options, Major General Fergus McLachlan contended that the Army cannot rely on size to achieve advantage but must use cooperative activities to 'achieve strategic mass'.[37] The same obviously holds true for the ADF's cyber capabilities. Bridging the gap between strategic intent and operational application will require a policy that maximises cooperation with allied nations, other government agencies and industry stakeholders, and contains a means for 'mobilising cyber-capable reservists or civilians in times of military crisis'.[38]

A radical technological transformation of the ADF to meet the challenges of cyber operations is not feasible given competing Defence priorities, funding and manning limitations, declining education standards across society, and a general lack of science, technology, engineering and maths qualifications and experience across the workforce.[39]

Details of Australia's cyber force development plan are not publicly available, preventing meaningful analysis of force structure options. Nevertheless, deliberate growth of a cadre of specialist cyber operators, combined with increased cyber education of commanders, intelligence professionals and planners over the next ten years is a realistic path.

A force structure that sees Headquarters Joint Operations Command, Deployable Joint Force Headquarters and the deployed Joint Task Force Headquarters supported with fully integrated cyber operations teams would enhance the ADF's interoperability with its allies and the achievement of cyber defence tasks. Manning, funding, education and training, and policy currently dictate that slow and steady growth is the most rational path for the ADF to take.

Conclusion

Australian national strategy and cyber strategy documents place a clear emphasis on the development of cyber capabilities within the ADF. While Joint Capabilities Group has the lead in translating this strategic intent into operational capability and effects, bridging the gap between strategic intent and operational capability is currently hindered by the lack of public conversation and understanding of the cyber domain.

In that regard, joint doctrine clearly has an important role in raising awareness of cyber operations and bridging the gap between strategic intent and operational and tactical applications. It is also the appropriate vehicle for addressing the nature of the cyber domain, types of cyber threats and categories of threat actors.

It has been argued in this article that agreement on a cyber domain concept and threat model would undoubtedly increase engagement and awareness of cyber operations across Defence, with policy then being developed to bridge the remaining gap between strategic intent and operational and tactical capabilities and effects. Such policy should address the unique challenges of military cyber operations and cover force structure and development, measures for cooperation, and cyber education, training and exercises.

A two-pronged approach along those lines should serve to ensure that considerations of the cyber domain and cyber operations move beyond the realm of technical specialists, and that the Australian Government's strategic intent is successfully translated by the ADF into operational objective and tactical actions.

Major Christopher Wardrop is an Australian Intelligence Corps officer, currently posted to the Intelligence Branch of Headquarters Joint Operations Command. His postings have included 4th Field Regiment, North West Mobile Force, Headquarters 1st Brigade, Headquarters 1st Division, 1st Intelligence Battalion and the Warrant Officer and Non-Commissioned Officer Academy. He has served on operations in Uruzgan and as an Intelligence Staff Officer on Australian Joint Task Force Headquarters in both Kabul and the Middle East region. Major Wardrop holds a Bachelor of Arts in History and Politics.

Notes

1 Myriam Calvety and Elgin Brunner 'Information, power and security – an outline of debates and implications', in Myriam Cavelty, Victor Mauer and Sai Krishna-Hensel (eds.), *Power and security in the information age: investigating the role of the state in cyberspace*, Ashgate: Farnham, 2013, 2007, pp. 201-493.

2 Charles Weiss, 'Science, technology and international relations', *Technology in Society*, Vol. 27, No. 3, August 2005.

3 A great number of which are available on the NATO Cooperative Cyber Defence Centre of Excellence website,

available at <https://ccdcoe.org/cyber-security-strategy-documents.html> accessed 20 June 2017.

4 [Australian] Department of Defence, 'White Paper at a glance: intelligence, surveillance and reconnaissance, space, electronic warfare and cyber security', *Department of Defence* [website], p. 1, available at <http://www.defence.gov.au/Whitepaper/AtAGlance/ISR-Cyber.asp> accessed 10 October 2017.

5 Commonwealth of Australia, *2016 Defence White Paper*, Department of Defence: Canberra, 2016.

6 Commonwealth of Australia, *Australia's cyber security strategy: enabling innovation, growth and prosperity,* Department of the Prime Minister and Cabinet: Canberra, 2016, p. 3.

7 Marcus Thompson, 'The ADF and cyber warfare', *Australian Defence Force Journal*, No. 200, 2016, p. 47.

8 Commonwealth of Australia, *Australia's cyber security strategy*.

9 See 'Information Warfare Division', *Department of Defence* [website], available at <http://www.defence.gov.au/jcg/iwd.asp> accessed 10 October 2017; see also Andrew Davies and Malcolm Davis, 'ADF capability snapshot 2006: C4ISR–winning in the networked battlespace', *Australian Strategic Policy Institute (ASPI)* [website], 21 June 2016, p. 3, available at <https://www.aspi.org.au/report/adf-capability-snapshot-2016-c4isr-winning-networked-battlespace> accessed 10 October 2017;

10 Davies and Davis, 'ADF capability snapshot 2006', pp. 2-4.

11 Michael Clifford, Michael Ryan and Zoe Hawkins, 'Mission command and C3 modernisation in the Australian Army: digitisation a critical enabler', *ASPI* [website], 17 December 2015, p. 9, available at <https://www.aspi.org.au/report/mission-command-and-c3-modernisation-australian-army-digitisation-critical-enabler> accessed 10 October 2017.

12 Davies and Davis, 'ADF capability snapshot 2006', p. 4

13 Major General Fergus McLachlan, 'Address to Australian Strategic Policy Institute's "Army's Future Force Structure Options Conference"', Canberra, 25 June 2015, available at <https://www.army.gov.au/our-work/speeches-and-transcripts/head-modernisation-strategic-planning-address-to-aspi-conference> accessed 10 October 2017.

14 McLachlan, 'Address to Australian Strategic Policy Institute's "Army's Future Force Structure Options Conference"'.

15 Ray Griggs, 'Building the integrated joint force', *ASPI* [website], 7 June 2017, available at <https://www.aspistrategist.org.au/building-integrated-joint-force/> accessed 10 October 2017.

16 Myriam Calvety, 'Is anything ever new? – Exploring the specificities of security and governance in the information age' in Cavelty *et al*, *Power and security in the information age*.

17 Department of Defence, 'Operation Series: Information Activities', Edition 3, Australian Defence Doctrine Publication 3:13, *Department of Defence* [website], 2013, available at <http://www.defence.gov.au/FOI/Docs/Disclosures/330_1314_Document.pdf> accessed 10 October 2017.

18 Ronald Deibert and Rafal Rohozinski, 'Risking security: policies and paradoxes of cyberspace security', *International Political Sociology*, Vol 4. Issue 1, 15 March 2010, p. 16, available at <https://deibert.citizenlab.ca/2010/03/risking-security-policies-and-paradoxes-of-cyberspace-security/> accessed 10 October 2017.

19 Manuel Castells, *Networks of outrage and hope: social movements in the internet age*, 2nd Edition, Wiley: Milton, 2015.

20 Nicolas Falliere, Liam Murchu, and Eric Chien, 'W32. Stuxnet dossier', *Symantec* [website], February 2011, available at <https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf> accessed 10 October 2017.

21 Department of Defence, 'Operation Series: Information Activities', pp. 1-6.

22 Greg Austin, *Australia rearmed! Future needs for cyber-enabled warfare*, Australian Centre for Cyber Security: Canberra, 2016.

23 See, for example, Marcus Thompson, 'The cyber threat to Australia', *Australian Defence Force Journal*, No. 188, 2012, pp. 59-61; Austin, *Australia re-armed!,* pp. 5-6; and US Department of Defense, 'The DOD Cyber Strategy', *Department of Defense* [website], April 2015, p. 9, available at <https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf> accessed 10 October 2017.

24 Deibert and Rohozinski, 'Risking security', pp. 18-24.

25 Castells, *Networks of outrage and hope*.

26 Richard Harknett, 'Integrated security: a strategic response to anonymity and the problem of the few', *Contemporary Security Policy*, Vol. 24, No. 1, 2003, pp. 29-32.

27 Austin, *Australia rearmed!*, p. 11.

28 Nicholas Tsagourias, 'Cyber-attacks, self-defence and the problem of attribution', *Journal of Conflict & Security Law*, Vol. 17, No. 2, Summer 2012, pp. 229-44.

29 Forrest Hare, 'The significance of attribution to cyberspace coercion: a political perspective', in C. Czosseck, R. Ottis and K. Ziolkowski (eds.), *Proceedings of the 4th International Conference on Cyber Conflict*, NATO: Tallinn, 2012, p. 126.

30 Austin, *Australia rearmed!*, p. 21.

31 Austin, *Australia rearmed!*.

32 US Department of Defense, 'Beyond the build: delivering outcomes through cyberspace. The Commander's vision and guidance for US Cyber Command', *Department of Defense* [website], 3 June 2015, p. 5, available at <https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/docs/US-Cyber-Command-Commanders-Vision.pdf> accessed 10 October 2017.

33 See, for example, Michael Riedy, 'Defence Cyber Coordination Centre', presentation to Military Communications and Information Systems Conference 2015, available at <https://milcis-twenty.squarespace.com/s/2015-3-2_3.pdf> accessed 20 June 2017.

34 Riedy, 'Defence Cyber Coordination Centre'.

35 Commonwealth of Australia, 'Australia's cyber security strategy', p. 28.

36 *Military and Aersopace Electronics*, '2017 DOD budget calls for 15 per cent increase in military cyber

security spending', *Military and Aerospace Electronics* [website], 24 February 2016, available at <http://www.militaryaerospace.com/articles/2016/02/cyber-security-dod-budget.html> accessed 21 June 2016.

37 McLachlan, 'Address to Australian Strategic Policy Institute's "Army's Future Force Structure Options Conference"', p. 3.

38 Austin, *Australia rearmed!*, p. 29.

39 Australian Council of Learned Academies, 'The role of science, research and technology in lifting Australia's productivity', *Australian Council of Learned Academies* [website], 2014, pp. 102-8, available at <http://www.acola.org.au/PDF/SAF04Reports/SAF04%20Role%20of%20SRT%20in%20lifting%20Aus%20Productivity%20FINAL%20REPORT.pdf> accessed 10 October 2017.


A41-210
15
42
208 177

Australia's petroleum supply and its implications for the ADF

Major Keyurkumar Patel, Australian Army

> The primary cause of our failure was a shortage of fuel.
>
> General Paul von Kleist, Commander Panzer Forces in Russia (Liddell Hart, 1947)

Introduction

Between 2003 and 2015, Australia suffered a 50 per cent reduction in its domestic crude oil refining capacity, largely because of the closure of refineries at Port Stanvac (South Australia) in 2003, Clyde (NSW) in 2012, Kurnell (NSW) in 2014, and Bulwer Island (Queensland) in 2015 (Byrnes *et al*., 2013). If remedial measures are not undertaken, it is projected that by 2030 Australia will have lost all its refining capability (Wraith, 2013).

Compounding this situation is that Australia has limited oil reserves and has become nearly entirely reliant on imported oil for its aviation fuel, marine diesel, gasoline and motor diesel (Dahl, 2015; Wraith, 2013). This overdependence on imports, and the fact that Australia obtains fuel for its military functions from a sole supplier (Caltex), potentially puts ADF operations at risk.

This article examines Australia's energy security, particularly in relation to petroleum supply, and its impact on the ADF. It addresses the key issues relating to Australia's increasing dependence on the import of refined petroleum, such as fluctuations in global fuel prices and existing fuel sources and infrastructure. It also evaluates Australia's refining capacity, existing storage capacity, and sources of refined petroleum and crude oil. Finally, it assesses the potential impact of terrorist activities, instability in source countries, and challenges associated with maritime supply lines, and their potential effects on the ADF.

Changes in global fuel prices

Even though Australia's heavy reliance on imported fuel is not viewed with any particular concern at present, obtaining it from limited sources may turn out to be a problem in the future, especially in the event of reduced availability and continuing high prices (Epstein and Buhovac, 2014). Unpredictable and volatile market forces may also affect the volume of refined petroleum available to the ADF and the country as a whole. Therefore, when developing a national energy security strategy, it is essential that projections be made up to 20 years into the future.

Notwithstanding concerns regarding the surety of supply from overseas sources, the reality is that imported petroleum is cheaper than refining crude oil in Australia (Andrews-Speed and Dannreuther, 2014). Australia currently imports most of its refined supplies from Singapore, which is relatively close to Australia and politically stable, providing a 14-day supply line that is unlikely to be easily disrupted. Even if the major supply line into Singapore from the Middle East were to be disrupted, Singapore has broadened its supply sources and increased its storage capacity, further enhancing the prospects of an adequate distribution of refined petroleum to meet the ADF's fuel requirements (Wraith, 2013).

However, even though Australia currently imports sufficient quantities of fuel at considerably lower costs compared to domestic refining, this scenario might not always be so (Mauter *et al*., 2014). In other words, even if adequate quantities can be obtained from sources such as Singapore, it is essential to have an appreciation of alternative sources, particularly when there is a surplus of supply and when prices are low. Moreover, it is vital to consider the implications of possible disruptions in supply as a result of the non-availability of oil tankers or disrupted maritime routes.

As mentioned, while Singapore is Australia's principal source of petroleum, it relies entirely on imports for its crude oil feedstock (Parker and Stewart, 2014). Additionally, despite substantial export quantities, it has relatively low total refining capacity, meaning it has minimum capacity to expand in response to a surge in demand. Contrarily, Japan and the Republic of Korea, for example, have lower production capacity risk but higher export capacity risk, primarily because their distance from Australia is greater than that of Singapore.

According to a 2012 report into Australia's use of aviation fuel, significant quantities are obtained from domestic refineries using imported crude oil, while the rest is externally sourced, largely from Singapore (Kopp, 2012). This situation puts the country in a risky position should there be significant fluctuations in international oil prices (Belkin, Nichol and Woehrel, 2013). The ADF, which uses several thousand tonnes of fuel every day, would obviously be affected by continuing high prices, impacting its ability to conduct military operations.

Yet with its relatively small population and minimal oil reserves, Australia has very little influence on the price of oil, which often has fluctuated markedly over the space of a decade. For example, in the aftermath of the global financial crisis in 2007-08, oil prices fell to US$40 per barrel. However, by 2011, it had increased to over US$120 per barrel. In 2014, the price of Brent crude—a blend of oils from the North Sea, particularly suited for making gasoline—was around US$115 per barrel. However, few had predicted the price collapse that would take place later that year, when stocks of unsold oil grew steadily and prices in Asia spiralled downwards to around US$29 per barrel in early 2016 (Mulhall, 2016). Today, the price of Brent crude oil is around US$60.

These examples are significant, given Australia's heavy reliance on Singapore, Japan and the Republic of Korea for refined petroleum products (Cleaver, 2013). Moreover, small-use countries such as Australia are competing in the same markets with the likes of China, India and Indonesia. Hence, price rises as a result of an increase in demand—which have occurred and been managed successfully in the past—will likely become more challenging as these countries become more industrialised and urbanised, requiring ever-larger proportions of the available resources.

Nevertheless, Australia can and should develop risk management strategies for its refined petroleum imports through constant assessment of the risks associated with its present sources and the identification of possible alternative

sources. One obvious strategy is to maintain essential levels of domestic refining capacity to act as a strategic reserve. In addition, there is a need to build and retain existing infrastructure to stock more fuel, which would mitigate the threat of disruptions to supply and ameliorate future price increases.

It is also the case that the petroleum industry worldwide is experiencing a number of changes, some of which provide opportunities for Australia to enhance its strategic energy security, such as through a broadening of sources. However, this creates constraints and challenges that must be understood and adjusted to, such as surging demands for a particular refined petroleum product within a particular region, and sudden changes in the global refining sector output (Byrnes *et al*., 2013).

In summary, despite Australia's over-reliance on imported refined petroleum, it is possible to mitigate or treat the known risks by ensuring the employment of sensible infrastructure enhancement and conducting risk management of the sourcing and transportation options. Australia and the ADF can also play an important role in contributing to region-wide efforts to protect the security of the supply line of petroleum, both into source countries and between them and Australia.

Overdependence on imported fuel

There has been considerable discussion over the years as to whether Australia's overdependence on overseas fuel supply is an issue of urgent national energy security or a risk that can be successfully moderated by the changing aspects, extensiveness and free-flowing nature of global petroleum markets. There is, however, a consensual view that Australia needs to maintain essential levels of domestic refining capacity to act as a strategic contingency in case of disruptions overseas which, among other impacts, could limit the availability of fuel for military operations (Mulhall, 2016).

It would seem prudent, therefore, that the government should take steps to prevent the curtailment of Australia's domestic refining capacity. Retaining the operating capacity of the remaining refineries would ensure improved supply resilience on both the east and west coasts of Australia (Australian Army, 2014). In particularly, it would ensure that the remaining capacity is capable of crude oil refining and providing sufficient levels of diesel, petrol, jet and other fuels to meet the requirements of the ADF and other essential services.

However, some commentators have a different take (Mulhall, 2016). They argue that even if the authorities provide the required support to retain Australia's domestic refining capacity, it is possible that the refineries will still be significantly impacted by commercial pressures and ultimately compelled to close. They contend that from a commercial point of view, the domestic supply of petroleum in Australia has experienced increasingly minimal profit margins, which has forced the closure of the refineries (Griffin and Teece, 2016).

Commentators also make the point that even though the government might be willing to increase storage capacity and provide financial support to refining capabilities, it cannot—in a free market economy—force non-state Australian companies to keep refineries operating, let alone those owned by multinationals. Seeking external supplies of refined petroleum is therefore seen as a necessary step to ensure sufficient national energy security for ADF and the nation.

There has been some discussion in recent years on the use of alternative fuels, such as bio fuels (produced through biological processes). This and other potential fuel types are obviously worthy of urgent consideration. Research into the development of synthetic fuels, for example, is being conducted in Queensland through the Linc Energy program, in conjunction with the US developer Syntroleum (Belkin, Nichol and Woehrel, 2013). However, it seems unlikely that these fuel sources, or alternatives such as electric or hydrogen-fuel cell vehicles, will become viable options for the entire ADF in the short to medium term.

Accordingly, the most practical option to ensure the nation's fuel supply security and resilience would seem to be through improving Australia's capacity to store additional stock (Andrew, 2013). Although Australia has geographically dispersed import terminals, its storage capacity

is inadequate to provide a minimum requirement of 90-days' stock, as recommended by the International Energy Agency. Furthermore, the areas of highest fuel requirements are typically located at a considerable distance from existing refineries and import terminals.

One option would be to store crude oil and/or refined product at some of the refineries that have been decommissioned, as they typically still retain considerable tank storage capacity. The storage capacity at current import terminals could also be increased by the installation of additional tanks. A number of new import terminals have also been constructed in recent years, which substantially enhance Australia's storage capacity.

For example, a new import terminal opened in Mackay in 2014, with a storage capacity of 56 megalitres. The facility was specifically developed to supply the expanding fuel requirements of the Queensland mining industry but has also contributed considerably to providing a solution to the decline in Australia's domestic refining capacity. However, while its refining capability has reduced the volume of imported diesel fuel, its output cannot be sustained for more than a few days without the importation of stock.

Another facility is the 85 megalitres fuel storage terminal at Pelican Point near Port Adelaide in South Australia, which also opened in 2014. It was designed to allow for two major future expansion phases, with a potential capacity to store up to 135 megalitres (Beaumont, 2013). A diesel fuel import terminal was also opened at Port Bonython in South Australia (near Whyalla) in 2016, with a capacity of 81 megalitres (Andrew, 2013). Other facilities recently opened have been three chemical and fuel storage sites, built by GrainCorp, in Queensland, Western Australia and New South Wales, with a total capacity of 65 megalitres.

These examples are encouraging developments, and suggest that commercial companies, at least, are responding to the decline in Australia's refining capacity by increasing both the number and capacity of import terminals. However, Australia arguably still needs to enhance its storage capacity to the extent that it becomes less dependent on threats to its supply line from Singapore and other East Asian countries.

Terrorism and instability in the source countries

There have been a number of instances in recent history of fuel tankers being targeted in warfare and by terrorists or criminals. During the Iran-Iraq war between 1980 and 1988, for example, both sides attacked the shipping of the other, including using Exocet missiles against tankers, in what became known as the 'tanker war' (Cribb, 2013). From about 2000 onwards, criminal gangs operating off the Somali coast also interdicted numerous tankers plying from the Persian Gulf, typically attempting to hold their crew and cargo for ransom, until anti-piracy operations—organised by the US and European Union—effectively quelled their activities by around 2012 (Samimi and Bagheri, 2013).

Another example occurred in October 2002, when a small boat packed with explosives was used by al Qaeda-backed insurgents to ram the French supertanker *Limburg*, with a capacity of 300,000 tonnes of crude oil, off the Yemeni coast, resulting in severe damage to the ship and an environmentally damaging oil spill (Dryzek, 2013). Shore-based oil facilities have also been attacked, either in warfare or by terrorist groups. Examples are the attacks against the oil terminal at Basra in Iraq in 2002 by suicide bombers in small boats, followed by a similar attack in 2004, albeit both were relatively ineffective, although they resulted in a number of deaths.

In a similar though less likely scenario, it is possible that individual tankers on Australia's line of supply from Southeast Asia could be threatened and attacked by terrorists or pirates. However, it is unlikely that the supply line between Southeast Asia and Australia—or indeed between the Middle East and East Asia—could be seriously interdicted, other than by the improbable outbreak of conflict (Heidenkamp, Louth and Taylor, 2013).

Similarly, while it is possible that shore-based facilities in Singapore or elsewhere in Southeast Asia or East Asia could be attacked by terrorists, the risk seems considerably lower than in the Middle East. However, even there, which is the main source of Singapore's imports, there have been no serious disruptions to oil-related

facilities since 2004, other than a failed al Qaeda attack on the Abqaiq oil facility in Saudi Arabia in 2006, and the bombing of the pipeline between Saudi Arabia and Bahrain in November 2017, neither of which impacted exports to East Asia.

Nevertheless, it is evident that Australia needs to constantly evaluate potential threats to its petroleum imports (Murphy, 2013). Any serious interruptions to supply would obviously impact the ADF and its ability to sustain its air, sea and land operations (Small *et al*., 2014). This is a strategic imperative, therefore, that needs to be addressed on a close and continuing basis.

Conclusion

Since fossil fuels remain the primary requirement in the civil transportation system and the means by which the ADF operates, Australia has to be reliant on the resilience and security of its petroleum resource. It is generally agreed that Australia overly relies on imported petroleum for its military operations, and that Australia's current fuel-holding capacity is inadequate. There are also a number of potential threats to Australia's fuel supply that need to be recognised and addressed, including the potential loss of Australia's remaining refineries.

A number of other factors, many of them outside the control of Australia and the ADF, such as the global volatility of fuel prices, an upsurge in terrorist activities, and internal conflicts in source countries, are additional energy security concerns. The reality is that Australia's petroleum supply chain is complex and lengthy, and its oil reserves are limited. The ADF's reliance on this supply and its ability to sustain enduring operations seem reasonably assured but should not be taken for granted, either by the ADF or Australia more broadly.

Keyurkumar J. Patel received his Bachelor of Engineering (First Class) from the Bangalore University, Master of Engineering from the Swinburne University of Technology and an Engineering Doctorate from the University of Southern Queensland in 1997, 2001 and 2011 respectively. He has authored more than 50 research studies in international refereed conferences and journals, and has authored four books.

He is a Fellow and Chartered Professional Engineer with Engineers Australia, a Member of the Royal Aeronautical Society, a Senior Member of the Australian Computer Society and a Senior Member of the IEEE. Since 2008, he has been serving in the Australian Army's Royal Australian Electrical and Mechanical Engineers Corps.

Notes

Acharya, A., *Constructing a security community in Southeast Asia: ASEAN and the problem of regional order*, Routledge: London, 2014.

Andrew, W., 'Defence fuel supply chain and remediation program', *Australian Army Journal*, Issue 12, No. 1, 2013.

Andrews-Speed, P., X. Liao and R. Dannreuther, *The strategic implications of China's energy needs*, Routledge: New York, 2014.

Beaumont, D.J., *Logistics strategy, and tactics: logistics in the formation of a medium-weight army*, Department of Defence: Canberra, 2015.

Belkin, P., J. Nichol and S. Woehrel, *Europe's energy security: options and challenges to natural gas supply diversification*, Congressional Research Service: Washington DC, 2013.

Bohi, D.R., and W.D. Montgomery, *Oil prices, energy security, and import policy*, Routledge: London, 2015.

Byrnes, L., C. Brown, J. Foster and L.D. Wagner, 'Australian renewable energy policy: barriers and challenges', *Renewable Energy*, Issue 60, 2013, pp. 711-21.

Cleaver, T., *Understanding the world economy*, Routledge: London, 2013.

Cribb, J., 'Food and fuel forever', *Future Directions International* [website], 23 May 2013, available at <http://www.futuredirections.org.au/publication/food-and-fuel-forever-j-cribb/> accessed 22 January 2018.

Dahl, C., *International energy markets: understanding pricing, policies, & profits*, PennWell Books: London, 2015.

Dryzek, J.S., *The politics of the earth: environmental discourses*, Oxford University Press: Oxford, 2013.

Epstein, M.J., and A.R. Buhovac, *Making sustainability work: best practices in managing and measuring corporate social, environmental, and economic impacts*, Berrett-Koehler Publishers: Oakland, 2014.

Green, B., *Struggling for self-reliance: four case studies of Australian regional force projection in the late 1980s and the 1990s*, ANU Press: Canberra, 2013.

Griffin, J.M., and D.J. Teece, *OPEC behaviour and world oil prices*, Routledge: London, 2016.

Guesmi, K., and S. Fattoum, 'Measuring contagion effects between crude oil and OECD stock markets'. *EconPapers* [website], 2014, available at <https://econpapers.repec.org/paper/ipgwpaper/2014-90.htm> accessed 22 January 2018.

Hawke, A., and R. Smith, *Australian Defence Force Posture Review,* Department of Defence: Canberra, 2012.

Heidenkamp, H., J. Louth and T. Taylor, 'Implications of the government–defence industry relationship', *Whitehall Papers*, Issue 81, No. 1, 2013, pp. 138-52.

Kopp, Carlo, 'Air power v refuelling infrastructure', *Air Power Australia* [website], April 2012, available at <http://www.ausairpower.net/APA-Fuels-Infrastructure.html> accessed 18 January 2018.

Liddell Hart, B., 'Interview with Paul von Kleist', *Spartacus Educational* [website], 1947, available at <http://spartacus-educational.com/GERkliest.htm> accessed 18 January 2018.

Mauter, M.S., *et al*., 'Regional variation in water-related impacts of shale gas development and implications for emerging international plays', *Environment, Science and Technology*, Issue 48, No. 15, 2014, pp. 8298–8306.

Mulhall, D.T., *Defence Logistic Enterprise Strategy 2016-2021*, Department of Defence: Canberra, 2016.

Murphy, M.N., *Contemporary piracy and maritime terrorism: the threat to international security*, Routledge: London, 2013.

Palin, R., *Multinational military forces: problems and prospects*, Routledge: London, 2013.

Parker, R., and J. Stewart, 'Energy and food security: is Australia fragile or resilient?', *Security Challenges*, Issue 10, No. 1, 2014, pp. 51-64.

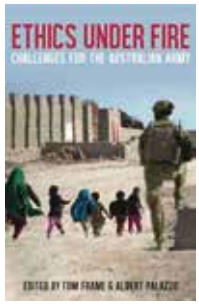
Samimi, A., and A. Bagheri, 'Studying and investigation corrosion in tube line and gas wells in oil and gas refinery', *International Journal of Chemistry*, Issue 3, 2013.

Small, M.J., *et al*., 'Risks and risk governance in unconventional shale gas development', *Environment, Science and Technology,* Issue 48, No. 15, 2014, pp. 8289–97.

The Australian Army, *Future Land Warfare,* Commonwealth of Australia: Canberra, 2014.

Wraith, A., *Defence fuel supply chain and remediation program*, Department of Defence: Canberra, 2013.

Book reviews



Ethics under fire: challenges for the Australian Army

Tom Frame and Albert Palazzo (eds.)
NewSouth Publishing: Sydney, 2017, 320 pages
ISBN: 978-1-7422-3549-3
$39.99

Reviewed by Alexander J. Edgar, University of Adelaide

The ADF, and particularly the Australian Army, is the only statutory body granted legal authority to use lethal force to defend the national interest—and it is equipped with formidable weaponry to complete the task. It is with this authority in mind that this book poses the critical questions that face the modern Australian Army about how it conducts itself in the fulfilment of its duty.

The authors are from non-government organisations, the military and academia, therefore offering a broad range of perspectives from which to analyse the ethical questions facing the Australian Army. Although broken into seven 'parts', the book realistically covers three broad themes: military ethics and expectations in a modern democratic society; the changing face of modern warfare; and how to train our soldiers to deal with ethical dilemmas in the contemporary context.

The first theme is certainly the broadest and most fundamental, exploring how the ethics of Australian society and the military interact and influence each other. The authors highlight the My Lai massacre in Vietnam and Abu Ghraib torture in Iraq as instances where the ethics of the military were compromised, thus diminishing the political will of the people for war.

Charles Dunlap Jnr highlights that upholding proper ethical behaviour can 'substantially affect warfighting capability' because combatants erode their own legitimacy in a war by causing 'unnecessary deaths or damage'. It is clear through this theme in the book that the authors draw an obvious link between the ability of the Australian Army to function as a warfighting force and its willingness to uphold a set of ethics.

This link leads to a discussion about the ethical frameworks by which decisions can be made in a military situation. Drawing the link between the need for ethical analysis and how ethics affects warfighting capability, leads to the next consideration—given the changing face of warfare and the shift in how governments use the Australian Army, are the Army's ethics sufficiently evolving to keep up with the rapid pace of change?

Warfare is changing and how governments use the Australian Army is changing as well, providing a platform for the authors within this theme to discuss how ethical dilemmas facing the Australian Army can be addressed. Cyberwarfare, peacekeeping and the imposition of Western ethics were the three concepts with the most interesting and well-developed discussions.

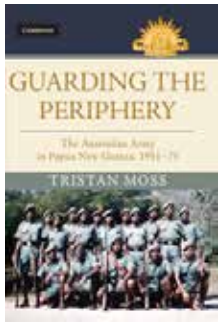
Adam Henschke's chapter on cyberwarfare discusses how the indiscriminate nature of some cyber weaponry can hold it in breach of international laws in *jus ad bello*. Adam Brandt Ford examines how social media is being weaponised and expanding the boundaries of war. Both ideas challenge traditional concepts of war. Lee Hayward poses the most pertinent questions in this area, namely can the Army or Australia make any real difference in areas where social change can take generations, specifically posing questions about changing attitudes toward women in Zambia.

The final theme for consideration is the need to train ethical soldiers and leaders throughout a soldier's career. Commentary throughout the book highlights that Australia is a world leader in ethical training for its Army, albeit there is room for improvement. The book provides ample policy ideas to address this problem.

Dr Deane-Peter Baker offers a nuanced approach that requires academia and the military to use modern research findings to provide situations of direct relevance to students of military ethics, which is a relatively simple policy shift. Baker's most poignant observation is the use of historical failures in ethical dilemmas, such as My Lai, contending that it is too easy for students simply to dismiss these situations saying, 'I would never do that'. He also offers the idea that ethicists need to receive real military experience.

Raising the example of embedded journalists, ethicists could similarly join military operations in a civilian capacity. Jamie Cullens recommends that the Army should have a senior officer at the Colonel or Lieutenant Colonel rank in charge of overseeing ethics training for the Army, a policy recently enacted by the British. The merit of the policy proposals in this book are beyond the scope of this review, however, they are worthy of further consideration.

Ethics under fire offers a thorough analysis of new ethical challenges facing today's Australian Army. The book offers a thematically appropriate approach to ethics and ethical decision-making frameworks, poses contemporary questions about evolving technology, and offers policy proposals to the Army. It should be widely read throughout the Army for its relevance to contemporary warfighting.



Guarding the Periphery: the Australian Army in Papua New Guinea, 1951-75

Tristan Moss
Cambridge University Press: Port Melbourne, 2017, 266 pages
ISBN: 978-1-1071-9596-7
$59.95

Reviewed by Gregory J. Ivey

This book provides a short, readable yet sophisticated analysis of the role played by the Australian Army in Papua New Guinea (PNG) over the 24 years prior to that country's independence. With rare access to archives and servicemen in both countries, as well as a comprehensive body of secondary sources, Moss presents an original and well-argued perspective on integrating PNG soldiers into the history of the Australian Army, which:

> Reconceptualises this institution [the Australian Army] as one that grappled, successfully ... with the employment of a considerable number of culturally diverse foreigners.

Essentially, the text is an empathetic history of the Australian Army in PNG from 1951 to 1975. Of necessity, Moss provides the background of the Second World War roles of the Pacific Islands Regiment (PIR) and the issues arising from its success. The author then discusses the re-establishment, management and development of the PNG Defence Force, including its colonial nature and problems through the 1950s; its upgraded defence role and nation-building initiatives during the 1960s; and the Australian Army's focus on transition towards PNG's self-determination in the early 1970s. The themed chapters are written chronologically, apart from an out-of-sequence account of the lives of Australian servicemen and their families in PNG during that period.

This production is militarily-useful, with a list of senior military appointments, maps, photographs and a substantial index, which includes the names of those servicemen mentioned in the text. While the map of Port Moresby is very useful, the map of PNG might justifiably have been extended to include the neighbouring Indonesian province of Irian Jaya, which featured so prominently in PNG's defence posture throughout this period. The extensive notes and bibliography point to the PhD thesis on which this book is based. While technically costly, the publishers might have considered adding some colour photos, which are readily available and would have considerably enhanced the publication.

Moss has not delineated separately the elements of doctrine, training, command, logistics and force structure. Rather he has integrated these

into the chronological chapter structure. Likewise, and more prominently, Moss addresses the issues of race and civil-military relations. The Australian Army is the disclosed focus—not the RAN or the RAAF—perhaps reflecting the author's sources and funding support. Even then, not all Army Corps are covered as there are only passing references to the groundwork of the Engineers or the mapping work of the Survey teams, both of which undertook substantial 'aid to the civil community' programs in PNG during this period.

Military readers may well feel that their particular area of interest deserved more attention in the text. Nevertheless, Moss has provided end-notes which indicate the sources for further information. Probably for the sake of consistency and focus, the author has covered the Army's PNG-manned units and those standard Army units that included PNG servicemen.

Moss's writing is balanced, restrained with the occasional emphatic statement, and there is no obvious bias. Each decade is analysed evenly and fairly but the author is clear about the crucial period in this history: the second half of the 1960s. While the attention of other historians is reasonably focused on Vietnam at that time, much of vital importance was also occurring in PNG.

Moss describes a number of events during this 'watershed period', notably the process of decolonisation, the creation of PNG Command, the raising of 2 PIR but not 3 PIR, and the arrival of National Service education instructors at the key bases. The book perhaps should have included mention of the 'Act of Free Choice' of 1969 in adjoining Irian Jaya, which occasioned extensive PIR patrols in the western districts of PNG in anticipation of cross-border refugee flows. The combined effect of those activities, as well as the earlier operational patrolling during the period of 'confrontation' between Indonesia and Malaysia, was long-lasting according to Moss.

The text retains its original intent as a subtle yet persuasive argument about the unique character, strategic role and forward-looking progress of the Army in PNG before 1975. While chiefly an outside/objective view of the Army, this book is infused, particularly in Chapter 6 (The 'black handers'), with an internal view of the Army with which former Australian servicemen and some PNG servicemen would likely identify.

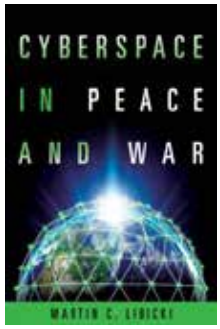
For example, within the prevailing pre-independence employment and education conditions, the indigenous servicemen 'saw themselves as an elite within PNG', being both highly trained and much better educated than the wider PNG population. Indeed, there is an echo of the Second World War, when senior indigenous soldiers had to assert their hard-earned status to insensitive Australian officers at Lae in 1945. The internal view captured in this chapter, however, does not seem to fully reflect the social progress made within the PIR. The quoted assessment of the PIR commanding officer in the mid-1950s about the Australian-PNG social distance could hardly have been sustained after the mid-1960s.

Moss has written a landmark study of this foreign chapter of the Australian Army after the Second World War. It will also be interesting reading for today's PNG Defence Force since, as the author observes, 'PNG has been omitted from the [Australian] Army's history and the Army from PNG's history'. This book provides, as all good history does, a framework suggesting several possible lines of further research: for example, a formal history of the original establishment and management of the force of PNG soldiers from 1940 to 1947; or a conceptual analysis of the funding, command, re-structures and (costly) deployments of the PNG Defence Force after 1975.

Overall, this modestly-sized book is a well-researched, constructive account of the Australian Army's role in PNG before independence. There are examples here of the Army's capacity to successfully train and educate foreign servicemen, to play a model role in mentoring indigenous servicemen towards leadership positions, and to leave a legacy overseas which provides the foundation for future military relationships. Since PNG's independence, the ADF is one of the few government agencies to have maintained a strategic and respectful, rather than colonial, relationship with their counterparts in PNG—and such ADF-PNG Defence Force programs continue today.

Australia's connections with PNG are many, including geography, ethnography, history, economy, hospitality and military. Australia's 2017 Foreign Affairs White Paper endorses its

'enduring partnership' and 'close defence cooperation' with PNG, so this book is both a timely and relevant addition to the Australian Army's History Series.



Cyberspace in peace and war

Martin Libicki
Naval Institute Press: Annapolis, 2016,
496 pages
ISBN: 978-1-6824-7032-9
US$55

Reviewed by Jim Truscott, OAM

This book is most informative about the potential transformation of warfare across the continuum of peace-time friction and kinetic conflict, going well beyond the realm of everyday computer users into a highly-classified and speculative space. It is divided into five major sections, addressing foundations, policies, operations, strategies and norms.

The author draws on considerable material from previously-published RAND reports, some of which he authored. It is a highly-technical read and, by necessity, introduces much new terminology, requiring readers to adapt to language including advanced persistent threats, the 'zero-day vulnerability' in commercial software, and nuclear notions of 'mutually assured destruction'. Much of it, however, is very US-centric, and although the issues are obviously global, it would be interesting to hear Australian perspectives.

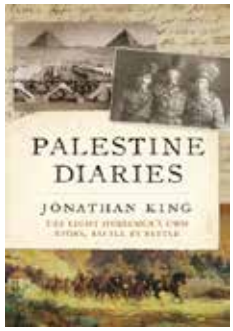
The author introduces a myriad of topics and many current cyber-warfare examples under the themes of disruption, corruption and disruption. I found it intriguing to read that while some organisations know they under cyber-attack, there are also those who don't know they are being attacked, highlighting the obvious need to be able to identify the threat—and ideally the attacker—before remedial actions or counter-measures can be considered.

It is fascinating that cyber war is described as the most serious near-term threat to the US. The fact that US Cyber Command is under US Strategic Command, which also has responsibility for strategic deterrence and global strike, begs the reader to ask why Australia does not have such a Cyber Command. Is the Australian Signals Directorate enough? It reminded me of my early experience with cyber warfare in 1996, when I was serving in the SAS, when the 'adversary' attempted to introduce a virus into the Battlefield Command Support System being fielded by the 1st Brigade in Exercise Phoenix in the Northern Territory.

The author explains that one of the many challenges in developing and executing capability is being able to actually 'weaponise' cyber warfare. I found this an interesting discussion, especially as no-one really makes public their cyber-warfare capability, with the partial exception of what was released by Edward Snowden about the supposed capabilities of the US National Security Agency. Unfortunately, much of the discussion in this section was very technical, and seemingly more suited to academics and researchers than cyber-warfare practitioners.

The author highlights debate over the 'Las Vegas rules' that treat cyberspace as a separate venue of conflict and not subject to the usual laws of armed conflict. It highlights the obvious need for consideration of cross–domain (land, sea, air and space) strategy and its potential escalation into kinetic warfare, regardless of the rules that may apply.

The conclusion about whether the world would be less violent if wars were fought in cyberspace rather than by conventional warfare is thought provoking. This book is a must-read for those in Australia's military high command and other government departments with a responsibility for national security. One thing is certain, the hackers, especially those that are government-sponsored, will already have it on their e-book shelves.



Palestine diaries: the Light Horsemen's own story, battle by battle

Jonathan King
Scribe: Melbourne, 2017, 448 pages
ISBN: 978-1-9253-2266-8
$39.99

Reviewed by Jim Truscott, OAM

When you read the personal stories in this battle-by-battle account, it seems quite extraordinary that only one Victoria Cross was awarded to a member of the Light Horse throughout their multiple legendary actions from Gallipoli in 1915, Sinai in 1916, Palestine in 1917-18, and then Jordan and Syria in 1918. Even more notable is the refusal by General Allenby, who commanded the British Egyptian Expeditionary Force (EEF), to send the Australian Mounted Division to the Western Front.

The desert campaign, which went from the defence of the Suez Canal to an all-out offensive against the Ottoman Empire, is described as a long ride over two and a half years in stifling dust and extreme cold. Remarkably, the EEF captured 40,000 Turkish and German prisoners, with less than 100 Light Horsemen captured. There were five Light Horse Brigades by the end of the war, organised as cavalry, with four-man/horse sections rather than infantry, but with the ability to dismount and fight as infantry.

Romani was the first and close-run battle, in which Lieutenant General Chauvel pushed his men to breaking point, and the first land victory for the Allies in World War 1. Chauvel's ruthless strategy at Romani is described as an 'equine steam roller', which routed the Turks from Romani to El Arish. The horses went 56 hours without water, while the men spent 44 hours in the saddle with only one water bottle for 35 hours. In 24 hours, they rode 80 kilometres and then fought mounted and dismounted 40 kilometres from water. There was classic insubordination to boot by a Brigadier, who ignored Chauvel's order to withdraw, which turned the tide and for which Chauvel later expressed his gratitude.

The subsequent battle for Rafa was almost given up for lack of water and, again, a NZ Brigade disobeyed orders to withdraw and charged. By comparison, after the decisive victories at Romani, El Arish, Magdhaba and Rafa, the first battle of Gaza was one of the worse-led battles of the desert campaign, plagued by poor communications and Generals too far from the action. The second attack on Gaza was a suicidal advance by infantry, which the British War Cabinet likened to a second Gallipoli, after which the EEF spent five months facing off the Turks in constant reconnaissance.

The battle for Beersheba, which was part of the third battle of Gaza, was a stunning victory and turning point in the battle for Palestine. The Light Horse traversed desert sand in a night march over 40 kilometres and the horses went 48 hours without water. An infantry attack from the west and south enabled the Light Horse to advance from the east, supported by British artillery. It was an incredible assault by 1000 men over seven kilometres, commencing at the trot, then canter, then a charge over the last two and a half kilometres in which 31 men and 44 horses were killed, just as the wells were about to be poisoned and blown up. Interestingly, Chauvel reckoned that it was continual movement and not speed that won the day.

10 Light Horse was the first of the EEF to enter Jerusalem in December 1917 and the first Christians in six centuries. They encountered difficult terrain north of the Dead Sea around Jericho and were thrice defeated after crossing the Jordan River at Es Salt and Amman. Then, by the time a troop from 10 Light Horse took a short cut to be the first of the EEF to ride into Damascus, much to the chagrin of Lawrence of Arabia, Chauvel commanded four Divisions and the largest cavalry force in history. Some of the Light Horse were even issued swords late

in the campaign. The EFF encountered a lot of diseases towards the end, leading up to the final battle at Aleppo.

My only minor criticism is that I would have liked to have read more about the roles of the Australian Service Corps in sustaining the force. However, the focus of this book is on the diaries, letters and photos of brave young Australian men, whose service and sacrifice shaped several nations. This easy-to-read book is a welcome addition to any Australian library.