Offset Strategies and Anti-Access Area Denial capabilities

By

Colonel Ian Langford, DSC and Bars

> *"Machines don't fight wars. Terrain doesn't fight wars. Humans fight wars. You must get into the minds of humans. That's where the battles are won."*
>
> John Boyd[1]

Introduction

Australia's physical security is in large part achieved as a function of her geography. As the world's largest island sitting astride the Pacific, Indian, and Southern Oceans, *Terra Australis* and her inhabitants have always sought comfort in being located 'at the bottom of the world'[2]. The realisation of the seriousness of the Japanese threat to Australia's physical security, most spectacularly demonstrated with the sudden capture of Singapore in 1942 jolted Australia out of this false notion.

Since that time, Australian security planners have sought emphasise the importance of military capability capable of operating across the 'sea-air' gap to the north of Australia. The October 2012 *Australia in the Asian Century White Paper* headlined this issue with the statement, '…as the global centre of gravity shifts to our region, the tyranny of distance is being replaced with the tyranny of proximity…'[3] It is in this context that the Australian Defence Force now focuses much of its efforts on developing the means to conduct 'expeditionary operations' as well as maintain regional access and engagement as part of a layered approach to global and regional security, as well as continental defence. [4] This also requires the Australian Defence Force to develop strategies and concepts for defeating adversary Ant-Access / Area Denial (A2/AD) capabilities as part of this core mission set.

[1] Grant T Hammond, *The Mind of War: John Boyd and American Security* (Smithsonian Books: Washington DC), 2004.

[2] For more on Australia's Maritime culture, see Michael Evans, The Third Way, in *2013 Chief of Army History Conference: Armies and Maritime Strategy,* Ed: P. Dennis, (Big Sky Publishing: Canberra), 2013, pp 327-358.

[3] Department of the Prime Minister and Cabinet, *Australia in the Asian Century White Paper*, 1, 105.

[4] This 2016 Defence White Paper details six key drivers that will shape the development of Australia's security environment out to 2035. Briefly, these drivers are:

1. The roles of the United States and China and the relationship between them, which is likely to be characterised by a mix of cooperation and competition.
2. Challenges to the stability of the rules-based global order, including competition between countries and major powers trying to promote their interests outside of the established rules.
3. The enduring threat of terrorism, including threats emanating from ungoverned parts of Africa, the Middle East and Asia.
4. State fragility, including within our immediate neighbourhood, caused by uneven economic growth, crime, social, environmental and governance challenges and climate change.
5. The pace of military modernisation and the development of more capable regional military forces, including more capable ballistic missile forces.
6. The emergence of new complex, non-geographic threats, including cyber threats to the security of information and communications systems.

A2AD- a definition and an understanding [5]

Anti-access (A2) challenges prevent or degrade the ability to enter an operational area. These challenges can be geographic, military, or diplomatic.[6] For example, an operational area could be very far inland, a great distance from ports and usable airfields. That would be a geographic challenge. In other cases, diplomatic or political issues can pose an A2 challenge when one or more nations in a region prohibit or limit the ability of the Australian Defence Force to deploy forces into their sovereign territory or to fly through their airspace.

Area denial (AD) refers to threats to forces within the operational area. As they relate to land forces, AD threats are characterised by the opponent's ability to obstruct the actions of land forces once they have deployed. Importantly, there are far more potential opponents that could pose significant AD challenges than there are opponents with major A2 capabilities. For example, when land forces deployed to Afghanistan in 2001–2002, there was not a significant military A2 threat, although there were initially diplomatic challenges to overcome with regard to nearby countries, and the geography of the region required a long-distance deployment far from the sea and existing bases. However, once land forces began operating in Afghanistan, they faced numerous and, at times, severe AD threats, such as the increasingly common use of Improvised Explosive Devices (IEDs) that caused casualties and imposed constraints on the mobility of land and other coalition forces.

The types of A2/AD threats that the military could encounter in future operations will vary considerably. At the *low end* of the conflict spectrum, there could be guerrilla-type forces, like the Taliban in Afghanistan, with very limited A2 capabilities and a small number of modern weapons. These forces could still pose a considerable AD challenge due to their ability to operate among the local population and employ irregular tactics to strike land forces at times and places of their choosing.

In the *middle* of the spectrum are so-called "hybrid" opponents, which can employ irregular or guerrilla-type tactics but are reasonably well armed with modern weapons. Hybrid opponents can therefore simultaneously fight in a conventional manner. Examples include the irregular Viet Cong and regular North Vietnamese forces during the Vietnam War and, more recently, the Hezbollah forces that Israel fought in southern Lebanon in 2006.[7]

At the *high end* of the threat spectrum are the armed forces of nation-states that tend to employ conventional tactics and weapons. Even at this end of the spectrum, the level of A2/AD capability can vary considerably. As with the hybrid threat, this challenge is not new to the military. In the case of the Second World War, Nazi Germany had a potent, long-range A2 capability in its submarine force (the U-boats) that threatened Allied shipping routes that carried troops and supplies across the

[5] John Gordon IV, John Matsumura, *The Army's role in overcoming anti-access and area denial challenges* (RAND Corporation: Washington DC, USA), 2013, pp 21-23.

[6] U.S. Army and U.S. Marine Corps, *Gaining and Maintaining Access: An Army–Marine Corps Concept*, version 1.0, March 2012, p. 3.

[7] Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly*, No. 52, 1st Quarter, 2009.

Atlantic. Similarly, during the Cold War, a major mission of the Soviet Navy's submarines was to prepare to interdict the movement of NATO reinforcements to Europe.

In many cases, the Australian Defence Force will have to employ a system of joint capabilities to overcome A2/AD challenges. This observation is based on both the insights gained in the scenarios that were examined as part of this research and an examination of how operations were actually conducted in the post–Second World War era in which a range of air, land, and naval capabilities were required to gain and maintain access. In some situations, air and maritime power will be the primary capabilities required (at least in the initial phases of an operation) to overcome significant A2 threats. In other situations, the role of ground forces will dominate or could come to do so as an operation progresses.

What is an Offset Strategy?

Countries such as Australia and its principle allies have identified the ability to gain access to areas of its choosing, whether opposed or unopposed, as a strategic imperative; tactically, The Australian Defence Force prepares its joint task forces to be ready to seize, hold, and build lodgements to enable follow on combat and peace support operations. This kind of operational access comprises numerous physical and shaping operations that together enable forcible entry, thus bridging the strategic imperative and tactical mission accomplishment.

Force-on-Force attritional conflict is the end-point of warfare; it is the least desired operational scenario for military forces. The Australian Defence Force of the future aims to generate operational outcomes employing asymmetric effects; it relies on its tactics, technologies, personnel, and alliances to generate its military operations. The development of 'offset' strategies seeks to do this.

So what is an offset strategy? In its simplest form, it is part of a long-term competitive strategy that aims to generate and sustain strategic advantage. While not solely about technological approaches, they do tend to have a powerful technological focus. Offset strategies are about finding the right combination of technology and operational constructs to achieve decision advantage, and in doing so bolster conventional deterrence[8]. For the Australian Defence Force, who by any regional comparison will always be a numerically small military, technology and military alliances represent the most important 'combat multiplier' when it comes to generate the type of military effects required to protect Australia and her national interests.

Offset Capabilities needed to maintain access beyond 2020 in the Asia-Pacific region

To achieve access as well as defeat area denial systems, the 'Offset strategy' the Australian Defence Force requires is drawn from 10 core tactical competencies and concepts that, when combined with cross-domain synergy, will help give Australian and other allied joint forces the necessary edge in the current and future fight for

[8] WGCR Phil Arms, The U.S 3rd Offset Strategy: An opportunity for the ADF (http://www.army.gov.au/Our-future/Blog/Articles/2016/07/Third-Offset-Strategy) *Land Power Forum,* 28 Jul 2016 (accessed online: 11 Aug 16).

access. These competencies are at the heart of what our short notice, rapid response forces must possess if they are to be effective in achieving their future assigned missions.

Electro-magnetic Manoeuvre Warfare

It is an agreed fact that modern military ships, aircraft, and ground forces *cannot* effectively operate without using the electromagnetic spectrum. They haven't been able to do so for about a century. At a very minimum, communication via radio (unless we go back runners, pigeons, and easily cut telephone cables), is necessary, even in an 'EMCON' environment. ADF forces today are constantly transmitting and receiving via wireless networks, downloading intelligence from satellites, sharing plans, checking their position on GPS, as well as other line of sight communication and control systems.

Electromagnetic Manoeuvre Warfare (EMW) is the concept of creating an electromagnetic battle management system, where all individual platforms collect data on enemy signals to inform the network while simultaneously managing up and down their own emissions in order to defeat, deceive or deny the adversary through offensive kinetic and/or non-kinetic operations.

EWM seeks to unify and assert positive control inside the electro-magnetic spectrum; this ability to directly control, indeed, to *manoeuvre* inside the spectrum, is a precise antidote to being numerically inferior to an adversary's military forces. EWM does not only focus on the adversary however, it also seeks to guarantee access for our Joint Forces to the electro-magnetic spectrum in support of command and control, detection, force protection and frequency management, support the ability for forces to manoeuvre across all domains (air, maritime, land, space, cyber), as well as allow own forces the ability to control the spectrum through denial, deception, and destruction EWM operations. EWM also provide joint forces with the opportunity to operate without attribution, which provides protection for sensitive capabilities as well as maintains operational security.

OODA= OO that is technologically intensive, DA that is human focused

"When circumstances change, we often fail to shift our perspective and instead continue to try to see the world as we feel it should be. We need to shift what Boyd calls our existing "mental concepts" – or what I like to call "mental models" – in order to deal with the new reality"[9].

So said John Boyd, in his unpublished work on military decision making. According to Boyd, ambiguity and uncertainty are inherent features of man and nature. While the randomness of the outside world plays a large role in that uncertainty, Boyd argued that the inability of military commanders to properly make sense of a constantly changing reality is a bigger hindrance. Boyd called for the continuous update of existing "mental concepts" in order to deal with the new reality.

[9] Grant T Hammond, *The Mind of War: John Boyd and American Security* (Smithsonian Books: Washington DC), 2004, pp 22-23.

Effective decision making is critical to success in war. Boyd's Observe, Orient, Decide, and Act (OODA) Loop was designed as an organising principle for strategy that anticipates and embraces ambiguity and uncertainty. The *Loop*, emphasised *alertness* (Observe) to the changing situation and environment, *character* (Orient) of the situation**,** the *decision among action alternatives* (Decide) generated from the Orientation phase, and lastly the *test* (Act), which focuses on the Action applied informing subsequent OODA Loops via a continuous learning process. It is generally accepted that most deliberate military planning processes in western countries today acknowledge and apply the logic of Boyd's work.

As an important component of an Offset strategy, decision making is critical. Embracing the OODA Loop allows for the harnessing of military technologies capable of supporting decision making- emphasizing the intensive use of military technology during the *OO* phase, while preserving the *DA* component for human processes represents the potential for superior fusion between the *Ends/Ways/Means* processes of military planning and execution.

OO (Observe/Orient) focus within an Offset strategy looks to generate superior situational understanding for commanders and their joint forces to ensure their ability to execute their key war fighting functions[10] (Know, Shape, Strike, Shield, Sustain, Adapt). A focus on key ISR capabilities (Electronic Warfare, Electronic Attack, persistent surveillance, super-computing, autonomous systems, unmanned systems) and decision support systems (geo-imagery, synthetic simulation, artificial intelligence) in an environment that is complex and ever-changing is essential in defeating complex systems such as an adversary A2/AD capability. Analytical technology is also critical in determining the alertness and character of problem-solving. Functions such as data management and data analysis using various analytic techniques and results that are surfaced or visualised in a format most appropriate for military forces is also essential to enabling the next phase of the decision cycle- decision and action.

DA (Decide/Act) functions as part of an Offset Strategy requires a centralised Command and Control system that emphasises human-to-human interconnectedness and is capable of integrating future 'Generation 5' capabilities such as those being introduced into the ADF over the next decade. Coupled with 'accelerated analytics' (derived from OO phase), the DA function rapidly delivers patterns and correlations that were previously unidentified and maximises the use of limited capabilities such as low-density/high-ISR demand assets, or optimises the employment of valuable resources such as airlift. High-performance analytics also give you an opportunity to derive value from big data, solve complex operational problems and deliver timely, high-quality insights for making decisions. This of course, supports commanders and their decision making in a way that generates superior tempo to the adversary, ensuring the ADF maintains a cognitive edge at all times.

[10] Note that the Combat / War-fighting Functions (Know, Shape Strike, Shield, Sustain, Adapt), which were articulated in LWD-1, The Fundamentals of Land Warfare (2008) were removed in the updated version of LWD-1 The Fundamentals of Land Power (2014). There remains an oblique reference to the Functions in the most current LWD 3-0 (Operations, 2015), however Strike is NOT included nor defined.

IAMD- Integrated Air and Missile Defence

The system known as the Integrated Air and Missile Defence System detects, tracks, identifies and monitors airborne objects (for instance aircraft, helicopters, unmanned aerial vehicles and ballistic missiles), and – if necessary – intercepts them using surface-based or airborne weapons systems. IAMD as a key enabler for joint force operations and encourages a system of ‘cooperative engagement’, which emphasises a fully integrated targeting network that designs kinetic and non-kinetic solutions in an ‘all-informed’ networked environment.

Integrated Air and Missile Defence capabilities can provide an effective ‘air policing’ deterrent effect in peacetime as well as preserving the actions necessary to nullify or reduce the effectiveness of air and missile threats during times of crisis and conflict. IAMD provides a highly responsive, time-critical, persistent capability in order to achieve a desired or necessary level of control of the air to allow joint forces the ability to conduct the full range of its missions. It integrates a network of interconnected national and battle command systems comprised of sensors, command and control facilities and weapons systems.

IAMD is a centralised ‘enabler’ for joint operations, and as such, should come under the authority of the theatre commander. A theatre-level IAMD is capable of providing a detailed single integrated air picture of aircraft and missile threats that is able to be shared amongst the friendly network resulting giving all ships, aircraft, and land mobile systems the ability to create an integrated air defence network and share sensor data in real time. This is especially important when reducing the level of threat in an A2 / AD environment where the simultaneous targeting of a number of A2 systems is critical to overwhelming and defeating the enemy network through superior tempo.

Given the myriad of capability priorities for the ADF, the development of an interoperable, robust IAMD system must be seen in the context of a ‘cost-consciousness’ that seeks to achieve real value for money. IAMD inceptors should be simple, low-cost and employ a network approach to engagement. The procurement of such a system should be managed through a process of development that allows the ADF to ‘leap to the end-state’, leveraging defence industry and Australia’s alliance frameworks accordingly.

Manned and Machine Teaming

Unmanned systems are changing the way all militaries operate and protect forces. The success of an unmanned system in any domain is best demonstrated by the way it integrates with manned activity and serves as a combat multiplier, rather than a simple swap. Human-machine teaming emphasises expanding capabilities, whether it be tactical surveillance in a war zone, dousing forest fires in a humanitarian operation, moving supplies in a convoy or inspecting undersea communications pipelines.

The ADF must invest additional resources and effort in developing manned-machine systems that enhance image-capture and sensors systems, sense and navigation systems, targeting and decision support systems, and advanced simulation systems. Incredible computing capabilities now allow systems to communicate with teams of humans and other systems. Advances in affordable, portable and long-lasting power sources help the system to improve mobility and speed up processing ability. Technologies on and off the platform help the unmanned system to understand its task and how to respond to obstacles, weather conditions and other unknown interferences.

Defended Communications Networks / We must defend our 'own' network – prevent high hacking of own systems.

The ADF relies heavily on cyberspace to enable its military, intelligence, and logistics operations, including the movement of personnel and material, and the command and control of the full spectrum of military operations. Exploitation of cyber vulnerabilities could undermine ADF's ability to operate and threaten national security and competitiveness. Recent investments by the Australian Government in cyber-security have improved the security posture of networks, systems, and data by reducing attack surfaces and improving control over information access. Results include enhancements in cyber-security measures and situational awareness, such as monitoring for intrusions, mitigation of vulnerabilities, improved identity management and authentication, and central collection of incident data. However, the cyber threat is increasing, and adversaries are becoming more skilled, sophisticated, and strategically-minded.

To meet the challenges expected between now and 2020, transformational changes to the ADF's cyber culture, workforce, technology, policy, and processes are required. The results of this strategy will enable the ADF to continue to operate effectively in cyberspace, as well as actively defend against adversarial cyber actions. By pursuing the following strategic efforts, the ADF will greatly improve its cyber defences. These initiatives will capitalize on down payments that have been made in each area, yet the current fiscal climate will further challenge the Department to make smart investment choices. These four focus areas and their critical elements are necessary to achieve our cyber mission now and in the future:

1) Establish a Resilient Defence Posture,
2) Transform Defence Operations,
3) Enhance Situational Awareness,
4) Assure Survivability against Highly-Sophisticated Attacks. [11]

In these efforts, the ADF will work more closely with interagency, private sector, and international partners toward collective cyber defence. Most importantly, the ADF cyberspace workforce will have to be fully trained, equipped, and prepared for cyber defence of the ADF and Australia more broadly. Although not addressed as a critical element, each focus area will require development of related policy, oversight, and compliance mechanisms.

'Dark' systems

Survivability in a highly contested A2 / AD environment demands capabilities that possess the ability to operate below the adversary 'detection threshold' by being able

[11] http://dodcio.defense.gov/Portals/0/Documents/DoD%20Strategy%20for%20Defending%20Network%20Systems%20and%20Data.pdf (accessed 18 August 2016).

to ‘go dark’. The ADF should develop systems capable of operating ‘stealth-like’. In order to do so, major air, maritime, and land platforms should possess the following design characteristics: Acoustic design features that reduce operating noise emissions; Thermal masking through equipment insulation and low emissivity paint, and the use of radar absorbent materials that reduce the probability of interception as well as meta-material concealment, and an emphasis on non magnetic materials.

Of significant note is the requirement to reduce a platforms electronic signature; the use of low probability intercept transmissions, as well as undertake mathematical and statistical algorithms development and implementations for own force and adversary RF signal detection, characterisation and localisation, with a particular emphasis on wideband multichannel and distributed sensors. This will assist in understanding our own ability to mask communication signals as well as improve our ability to detect others in the operating environment.[12]

Anti-Position Navigation Timing Protection and Disruption systems

There is a growing awareness amongst modern militaries of the risks associated with the Global Positioning System (GPS) being the only means of position determination and precision timing. Modern day militaries rely significantly on GPS and the loss of this system represents a major disruption risk to operations and military capabilities. The Australian Defence Force must possess the ability to both operate within a GPS degraded environment as well as be able to effectively deny the use of the same system to an adversary.

Developed in the 1970s by the US Department of Defense, the GPS was created for military navigation and is widely credited with helping the US achieve military dominance during the 1991 Gulf War. Since that time, this capability has become absolutely critical to military operations and their critical weapons systems; notably, GPS is also now critical to global commerce and trade, the continuity of which is critical to the continuity of the global economy.

As part of its Offset Strategy, the ADF should seek to develop a robust and cost-effective solution to protect military capabilities from GPS interference. High-performance GPS anti-jamming devices that nullifies jamming signals and allows GPS receivers to acquire and track satellite signals are necessary to ensure the ADF retains the ability to determine accurate battlefields positions. [13]

Spoofing is the process of creating a false GPS signal which replaces correct readings, leading devices to display incorrect times or locations. Spoofing could potentially be used to disrupt power grids or by criminals under house arrest looking to fool monitoring devices.[14] As an offensive capability, the ability to deny GPS to an adversary would be an important manoeuvre and attack tool, especially in a highly de-centralised and long-range targeting conflict such as an A2 / AD environment. This

[12] http://www.dst.defence.gov.au/capability/spectrum-sensing-and-shaping (accessed 18 August 16).

[13] http://www.novatel.com/assets/gajt/pdf/gajt-white-paper.pdf (accessed 18 Aug 16)

[14] http://www.homelandsecuritynewswire.com/dr20111122-the-increasing-risks-of-gps-systems (accessed 18 Aug 16).

would be an important capability especially against adversary unmanned systems and attack munitions, which rely on GPS as part of their core functions.[15]

Directed Energy Systems

With the groundbreaking testing of a Laser Weapons System aboard the USS Ponce, directed energy systems have never been closer to becoming integrated as fully operational military systems.[16] The potential for the capabilities of the ADF to block adversary electronics and communications, protect convoys in high risk zones, and protect critical land, maritime and airborne assets is crucial in preparing for future threats, and is quickly becoming incorporated into the vision of nations with active programmes. Active denial systems and other non-lethal DES applications for police and civil enforcement remains a controversial topic, whilst also seeing vast investment and research in the area. Challenges surrounding power supply, size and weight remain elemental in the research and development stage, whilst ruggedisation remains a key inhibitor to real-world deployment.

While size, weight, interoperability and lethality are factors, there are other concerns that limit directed energy weapons and they involve environmental extremes. Today's bullet launching assault rifles are reliable in all extremes ranging from tropical, to desert, to arctic conditions. They work in rain, snow, dust and fog. You can generally immerse them and they'll still shoot given a few seconds for the water to drain. They can be covered in mud and they shoot. Solar flares and EMP make no difference – they still work. A directed energy weapon relies on a sophisticated electronic circuit to generate the energy beam. While it can be isolated and shielded from outside influence, that adds weight and another level of sophistication. There is always some sort of lens to calumniate (focus) the beam and that, in most cases is optical. That lens must be kept unobstructed and clean to function properly which is a difficult expectation in many environments. Water vapor mitigates directed energy. Clouds, fog, rain and snow are all enemies of directed energy. Today's powerful anti-missile airborne systems simply burn their way through, but lower energy man-portable systems won't have that sort of sustained power and will likely be unreliable in some of these unpredictable battlefield environments.

Conclusion

The October 2012 *Australia in the Asian Century White Paper* opened with the comment that "predicting the future is fraught with risk, but the greater risk is in failing to plan for our destiny. As a nation, we face a choice: to drift into our future or to actively shape it"[17] In a region that is becoming increasingly dependent on its maritime access as a key element to support national sovereignty, the Australian Defence Force must now focus significant effort on developing the means to conduct 'expeditionary operations' as well as maintain regional access and engagement as part of a layered approach to global and regional security, as well as continental defence. [18] This will require the Australian Defence Force to develop strategies and concepts

[15] See https://www.rt.com/news/201795-china-drone-defense-laser/ (accessed 18 August 2016)

[16] https://www.rt.com/news/205711-us-laser-weapon-persian/ (accessed 16 August 2016).

[17] Department of the Prime Minister and Cabinet, *Australia in the Asian Century White Paper*, 1.

[18] This 2016 Defence White Paper details six key drivers that will shape the development of Australia's security environment out to 2035. Briefly, these drivers are:

for defeating adversary Ant-Access / Area Denial (A2/AD) capabilities as part of this core mission set. A well defined, resourced, and balance series of ‘Offset Strategies”, are an important component to any A2 / AD capability.

Colonel Ian Langford, DSC and Bars is a career Army officer with nearly 20 years service in Special Operations Command. He is currently the G5 (Plans, Modernisation, and Concepts) at Headquarters Forces Command in Sydney, Australia. The views represented in this paper are his own.

- The roles of the United States and China and the relationship between them, which is likely to be characterised by a mix of cooperation and competition.
- Challenges to the stability of the rules-based global order, including competition between countries and major powers trying to promote their interests outside of the established rules.
- The enduring threat of terrorism, including threats emanating from ungoverned parts of Africa, the Middle East and Asia.
- State fragility, including within our immediate neighbourhood, caused by uneven economic growth, crime, social, environmental and governance challenges and climate change.
- The pace of military modernisation and the development of more capable regional military forces, including more capable ballistic missile forces.
- The emergence of new complex, non-geographic threats, including cyber threats to the security of information and communications systems.