Australia's Offset and A2/AD Strategies

Ian Langford

ABSTRACT: This article discusses the competencies Australia's political and military leaders selected to pursue offset strategies and anti-access/area denial capabilities.

Australia's physical security is in large part achieved as a function of its geography. As the world's largest island sitting astride the Pacific, Indian, and Southern Oceans, Terra Australis Incognita and its inhabitants have traditionally sought comfort in being located "at the bottom of the world."[1] Australians were jolted out of this false notion and realized their physical vulnerability when Japan suddenly captured Singapore in 1942. Since then, Australian security planners have emphasized the importance of possessing the military capability to operate across the sea-air gap to the north of the continent. The *Australia in the Asian Century* white paper elevated this issue: "As the global centre of gravity shifts to our region, the tyranny of distance is being replaced with the tyranny of proximity."[2]

The Australian Defence Force focuses much of its effort on developing the means to operate in major theaters of conflict as well as to maintain regional access and engagement as part of a layered approach to national security, including continental defense. This approach also acknowledges Australia's reliance on its most important security treaty—the ANZUS Pact (1951).[3] One of this alliance's most interesting challenges is ensuring the continuity of global commerce systems in the Asia-Pacific, which requires common access to realize the potential benefits. This aspect has underpinned the region's stability for at least the past 70 years. Today, however, access across the global commons is increasingly problematic due to political, environmental, and diplomatic issues. To guarantee continued common access and security in the region, the Australian Defence Force is expanding its network of parties who likewise value developing capabilities and concepts to defeat adversarial anti-access/area denial (A2/AD) threats.

1 For more on Australia's Maritime culture, see Michael Evans, "The Third Way: Towards an Australian Maritime Strategy for the Twenty-first Century," in *2013 Chief of Army History Conference: Armies and Maritime Strategy*, ed. Peter Dennis (Canberra: Big Sky Publishing, 2013), 327–58.

2 Department of the Prime Minister and Cabinet (PM&C), *Australia in the Asian Century*, White Paper 1 (Barton, Australia: PM&C, 2012), 105. The white paper also detailed six key drivers for developing Australia's security environment through 2035: the roles of and relationship between the United States and China; competitive states' challenges to the stability of the rules-based global order; terrorist threats; state fragility resulting from economics, crime, social factors, environment, governing, and climate change; military modernization; and complex, nongeographic threats such as cyber.

3 The Australia, New Zealand, United States Security (ANZUS) Pact initially bound the parties to cooperate on security matters in the Pacific Ocean region. Today the treaty relates to conflicts worldwide: an armed attack on any of the three parties would be met as a common threat.

Colonel Ian Langford, a career special forces officer in the Australian Defence Force, specializes in future warfare.

Anti-Access/Area Denial

Anti-access challenges—geographic, military, and diplomatic—are designed to prevent, delay, or degrade the ability of military forces to enter an operational area and establish bases farther away from preferred locations.[4] Limiting an opponent to an inland operational area, for example, creates great distance from ports and usable airfields, presenting a geographic challenge.[5] In other cases, anti-access challenges are diplomatic or political matters, such as when a nation in a region prohibits or limits the ability of a military operation to deploy joint task forces into its sovereign territory or to fly through its airspace.

Area denial refers to actions designed to restrict freedoms of maneuver, which are characterized by an adversary's ability to obstruct the actions of military forces once they have deployed. Land forces deployed to Afghanistan in 2001, for example, encountered no significant military area denial threats though forces deployed to the region later in the conflict regularly faced severe area denial threats such as improvised explosive devices. In the maritime domain, sea mines and other defensive measures effectively deny access to and use of maneuver corridors (straits), harbors, and beach-landing sites.

The types of A2/AD threats the Australian Defence Force could encounter in future operations will vary considerably. At the low-end of the spectrum of conflict, insurgent forces such as the Taliban in Afghanistan or the Islamic State in Iraq and Syria have limited anti-access capabilities and a small number of modern weapons. These forces could still pose a considerable area denial 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, hybrid opponents can employ irregular or guerrilla-type tactics, but are reasonably well-armed with modern weapons. Examples of these opponents, who can simultaneously fight in a conventional manner, include the pairing of irregular Viet Cong and regular North Vietnamese forces during the Vietnam War and the Hezbollah forces that Israel fought in southern Lebanon in 2006.[6]

At the high end of the threat spectrum, armed forces of nation-states 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. In World War II, Nazi Germany's submarine force provided a potent, long-range anti-access capability that threatened allied shipping routes across the North Atlantic Ocean. Similarly, during the Cold War, a major mission of the Soviet navy's submarines was to interdict the movement of North Atlantic Treaty Organization reinforcements from the United States to Europe.

---

4 John Gordon IV and John Matsumura, *The Army's Role in Overcoming Anti-Access and Area Denial Challenges* (Washington, DC: RAND Corporation, 2013), 21–23.

5 US Army Capabilities Integration Center (ARCIC) and US Marine Corps Combat Development Command, *Gaining and Maintaining Access: An Army–Marine Corps Concept* (Fort Eustis, VA: ARCIC, 2012), 3.

6 Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly* 52 (1st Quarter 2009).

Offset Strategy

Australia has, in comparison to other regional military forces, a numerically modest capability to provide security over a significant geographic area. To deter effectively and to provide military responses to threats, the Australian Defence Force must compensate for its size disadvantage by developing a competitive, asymmetrical strategy capable of generating an advantage over potential adversaries. This type of strategy usually centers on engineering cross-domain and technological capabilities that effectively offset quantitative inferiority in regions dominated by larger, more potent forces.

In its simplest form, an offset strategy is a competitive long-term concept that generates and sustains strategic advantage.[7] While not an exclusively technological approach, the strategy does tend to have a robust technical focus. Offset strategies strive for an appropriate 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 multipliers that can generate the military effects required to protect Australia and her national interests.

Force-on-force attrition is the end point of warfare, the least desired operational scenario for military forces. The Australian Defence Force seeks to generate operational outcomes by employing asymmetric effects; it relies on tactics, technologies, personnel, and alliances—its inventory of offset capabilities—to generate its military operations.

Offset Capabilities for Asia-Pacific Access beyond 2020

To retain access and to defeat area denial systems in the Asia-Pacific, the Australian Defence Force offset strategy concentrates on eight core tactical competencies and concepts that, when combined with cross-domain synergy, gives Australian and allied joint forces the edge necessary for future military contests for access. These competencies are at the heart of short-notice, rapid-response force success.

Competency 1: Electromagnetic Maneuver Warfare

Modern military ships, aircraft, and ground forces cannot effectively operate without using the electromagnetic spectrum and have not been able to do so for about a century. At a very minimum, communication via radio—notwithstanding runners, pigeons, and easily cut telephone cables—is necessary even in an emissions-controlled environment. Today's Australian forces constantly transmit and receive intelligence, operational plans, and asset locations via wireless networks and other communication and control systems. These systems must be protected while their platforms and their sensor suites simultaneously deny the electromagnetic spectrum from being used by any potential adversary.

---

7 Robert Martinage, *Toward a New Offset Strategy: Exploiting U.S. Long-Term Advantages to Restore U.S. Global Power Projection Capability* (Washington, DC: Center for Strategic and Budgetary Assessments, 2014), 14–20.

8 Wing Commander Phil Arms, "The U.S. 3rd Offset Strategy: An opportunity for the ADF," Australian Army, July 28, 2016, http://www.Army.gov.au/Our-future/Blog/Articles/2016/07/Third-Offset-Strategy.

Electromagnetic maneuver warfare is the concept of creating an electromagnetic battle management system, where all individual platforms collect data on and inform the network of enemy signals while managing their own emissions to defeat, deceive, or deny the adversary through offensive kinetic and nonkinetic operations. By unifying and asserting positive control inside the electromagnetic spectrum—indeed maneuvering inside the spectrum—numerically inferior forces have an antedote for an adversary's military forces. Moreover, electromagnetic maneuver warfare does not only focus on the adversary, it also guarantees access to the electromagnetic spectrum for joint forces' command and control, detection, force protection, and frequency management capabilities. Supporting the ability for forces to maneuver across all domains—air, maritime, land, space, cyber—as well as to control the spectrum through denial, deception, and destruction, electromagnetic maneuver warfare provides joint forces opportunities to operate without attribution, which protects sensitive capabilities and maintains operational security.

Competency 2: Technologically Intensive, Human Focused Decision-Making

Effective decision-making is critical to success in war. Colonel John Boyd's Observe, Orient, Decide, and Act (OODA) Loop was designed as an organizing principle for strategy that anticipated and embraced ambiguity and uncertainty, which he perceived as inherent features of man and nature. The randomness of the outside world, he felt, played a large role in uncertainty. Boyd further argued the inability of military commanders to properly make sense of a constantly changing reality is a bigger hindrance. Thus, he called for continuously updating mental concepts by using both man and machine to deal with a constantly changing reality.

Boyd's OODA Loop emphasizes alertness—the ability to *observe* the changing situation and environment. A follow-on focus of the changing character of the situation allows a person to *orient* to the situation. Armed with this perspective, one can *decide* to *act* based upon action alternatives that inform subsequent OODA Loops via a continuous learning process. While modern technology collects critical information to inform the loop, the interpretation of such information remains an essential human skill founded on the decision-maker's personal experience and prior preparation to understand the situation and the enemy. Boyd emphasized an additional need for the commander's intent to unify a force's purpose and preference for decentralized execution to ensure redundancy in action, thereby increasing the chances of mission success.[9]

As a component of an offset strategy, decision-making is critical. Embracing the OODA Loop allows the military to harness technologies that support decision-making, which is emphasized during the observe and orient phase, while preserving the human aspects of the decide and act component.

The observe and orient focus within an offset strategy generates superior situational understanding for commanders and joint forces to ensure their ability to execute the key warfighting functions—know,

9 For more on John Boyd, see Robert Coram, *Boyd: The Fighter Pilot Who Changed the Art of War* (New York: Bay Back Books, 2002).

shape, strike, shield, sustain, and adapt.[10] To achieve this perspective and the ability to defeat complex systems such as an adversary's A2/AD capability, focus must be maintained on key intelligence, surveillance, and reconnaissance capabilities, which include electronic warfare, electronic attack, persistent surveillance, supercomputing, autonomous systems, and unmanned systems, as well as decision support systems such as geoimagery, synthetic simulation, artificial intelligence, and computer learning systems. Analytical technologies that determine the alertness and character of problem-solving as well as analytical functions such as data management and data analysis are also critical: they enable processed and analyzed data to be presented as information appropriately formatted for military forces to apply to the next phase of the decision cycle—decide and act.

The decide and act function as part of an offset strategy requires a centralized command and control system that emphasizes human-to-human interconnectedness and integrates Generation 5 capabilities such as those being introduced into military service over the next decade. Coupled with increased data processing technologies, including accelerated analytics, the decide and act function is likely to rapidly deliver patterns and correlations that were previously unidentified. A more accurate and detailed data set would maximize the use of limited capabilities such as low-density/high-demand intelligence, surveillance, and reconnaissance systems as well as optimize the use of scarce resources such as aviation and logistics. High performance analytics also present an opportunity to derive value from big data, solve complex operational problems, and deliver timely, high-quality insights for making decisions.

Competency 3: Integrated Air and Missile Defense Systems

An effective integrated air and missile defense system detects, tracks, identifies, and monitors airborne objects, such as aircraft, helicopters, unmanned aerial vehicles, and ballistic missiles, and if necessary, intercepts them using surface-based or airborne weapons systems. Integrated air and missile defense systems are key enablers for joint force operations and encourage a system of cooperative engagement emphasizing a fully integrated targeting network that designs kinetic and nonkinetic solutions in an all-informed networked environment.

The systems' capabilities provide effective air policing with a deterrent effect in peacetime as well as preserve the actions necessary to nullify or reduce the effectiveness of air and missile threats during times of crisis and conflict. Integrated air and missile defense systems provide a highly responsive, time-critical, persistent capability to achieve a desired or necessary level of air control that allows joint forces to conduct full-range missions. They integrate a network of interconnected national and battle command systems comprised of sensors, command and control facilities, and weapons systems.

---

10 The combat and warfighting functions of know, shape, strike, shield, sustain, and adapt, which were articulated by the Australian Army, in *The Fundamentals of Land Warfare*, Land Warfare Doctrine (LWD) 1 (Canberra, ACT, Australia: Australian Army, 2008), were removed in the 2014 version of the doctrine, but an oblique reference to these functions, which excludes strike, remains in the following: Australian Army, *Operations*, LWD 3-0 (Laverton, Victoria: Defence Publishing Service, 2015).

A theater-level system is capable of combining sensor data in real time to create a detailed, integrated picture of aircraft and missile threats in the air that can be shared on an allied network to give friendly ships, aircraft, and land mobile systems the ability to create an integrated air defense. This capability is especially important for managing the threat level of an A2/AD environment where the simultaneous targeting of a multitude of anti-access systems is critical to overwhelming and defeating the enemy network.

The advent of cheap, mass-produced, autonomous drones, which have no centralized system but are capable of generating thousands of air vectors that can overwhelm the processing power of an integrated air and missile defense system, has become an emerging arms race. The need for adaptive refresh capabilities and the avoidance of block or system obsolescence will be essential to ensuring the systems remain capable and effective.

Given the myriad of capability priorities for modern military forces, including the Australian Defence Force, the development of an interoperable, robust integrated air and missile defense system must be seen in the context of cost-consciousness. System inceptors should therefore be simple, relatively inexpensive, and employ a network approach to engagement: the active defense versus missile attack cost ratio should be reversed. System procurement should be managed through a development process that allows organizations, including the Australian Defence Force, an opportunity to leap to the end-state, thereby leveraging the defense industry and Australia's alliance frameworks.

Competency 4: Manned and Machine Teaming

Unmanned systems are changing the way all militaries operate and protect forces. Exploration and expansion of these capabilities must be continued while militaries remain conscious of low-technology threats, such as drone technology, that effectively act as autonomous rounds of ammunition. 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 emphasizes this progression whether it occurs as tactical surveillance in a war zone, support of a humanitarian operation, or movement of supplies in a convoy.

The Australian Defence Force must invest additional resources and effort in developing manned-machine systems that enhance image-capture and sensor systems, positioning and navigation systems, targeting and decision-support systems, and advanced simulation systems. Advanced computing capabilities now allow systems to communicate with teams of humans and other systems. Improvements in affordable, portable, and long-lasting power sources also improve system mobility and accelerate processing ability. Technologies on and off any teamed platform will also help unmanned systems understand tasks and how to respond to obstacles, weather conditions, and other unknown interferences.

Competency 5: Defended and Defending Communications Networks

The Australian Defence Force relies heavily on cyberspace to enable its military, intelligence, and logistics operations, including the movement of personnel and matériel and the command and control of the full spectrum of military operations. Exploitation of cybervulnerabilities could undermine the force's ability to operate, thereby threatening national security and competitiveness. Recent government investments in cybersecurity have improved the posture of networks, systems, and data by reducing attack surfaces and improving control over information access. Results include enhancements in cybersecurity measures and situational awareness, such as monitoring for intrusions, mitigating vulnerabilities, improving identity management and authentication, and central collection of incident data; however, cyberthreats are increasing and adversaries are becoming more skilled, sophisticated, and strategically minded. The Australian Defence Force must ensure it does not overlook the vulnerability of cyberassets.

To meet the challenges expected between now and 2020, transformational changes to cyberculture, workforce, technology, policy, and processes of the Australian Defence Force are required. The results of this strategy will enable the organization to continue to operate effectively in cyberspace, as well as actively defend against adversarial cyberactions. This strategy should emphasize establishing a resilient defense posture, transforming the management of all deployments and operations, enhancing all situational awareness assets with a specific focus on network integrity, and increasing assurance and survivability against highly sophisticated attacks against core systems.[11]

To support these efforts, the Australian Defence Force will work more closely with its interagency partners, the private sector, and international partners toward collective cyberdefense. Most importantly, the Australian cyberspace workforce will have to be fully trained, equipped, and prepared for defending the cyberinterests of not only the military but also Australian society in general. Although not addressed as a critical element, each focus area will require development of related policy, oversight, and compliance mechanisms to be successful.

Competency 6: Dark Systems

Survivability in a highly contested A2/AD environment demands capabilities that can operate below adversaries' detection threshold, in other words, the capability to "go dark." The Australian Defence Force should develop stealth-like systems that include air, maritime, and land platforms with the following design characteristics: acoustic design features that reduce operating noise emissions and thermal masking through equipment insulation, low emissivity paint, and radar absorbent materials that reduce the probability of interception, as well as metamaterial concealment and nonmagnetic construction materials.

Of significant note is the requirement to reduce a platform's electronic signature, use low-probability intercept transmissions, as well as develop and implement mathematical and statistical algorithms for allied and adversarial radio frequency signal detection, characterization,

11 US Department of Defense (DoD), *DoD Strategy for Defending Networks, Systems, and Data*, (Washington, DC: DoD, 2013).

and localization with a particular emphasis on wideband, multichannel, and distributed sensors. This capability will not only help the Australian Defence Force mask its communication signals but also improve its ability to detect other signals within the operating environment.[12]

Competency 7: Anti-Position Navigation Timing Protection and Disruption Systems

There is a growing awareness among modern militaries of the major disruption risks to operations and capabilities that rely on GPS as the only means of position determination and precision timing. Developed in the 1970s by the US Department of Defense, GPS was created for military navigation and is widely credited with America's military dominance during the Persian Gulf War (1990–91). Since that time, the capability has become absolutely critical to military operations and weapons systems as well as international commerce, which is critical to the global economy. Thus, the Australian Defence Force must possess both the ability to operate within a GPS degraded environment and to deny effectively the use of the same system to an adversary. This ability should increase space resiliency, hedge against the loss of space-based enablers, and develop counterspace capabilities accordingly.

As part of its offset strategy, the Australian Defence Force should pursue a robust and cost-effective solution to protect military capabilities from GPS interference: high-performance GPS antijamming devices that allow GPS receivers to acquire and track satellite signals so the Australian Defence Force can retain the ability to determine accurate battlefields positions.[13] Alternatively, Australia may need to choose a less direct approach such as ensuring systems can operate on multiple systems such as an adversary's primary Glonass or Beidou systems, which would be less likely to be jammed.[14] This redundancy in position determination and precision timing capabilities does not currently exist.

Spoofing, a process of replacing correct GPS readings by creating a false signal that leads devices to display incorrect times or locations, could potentially disrupt power grids or hijack systems including weapon platform and key maneuver systems.[15] As an offensive capability, the ability to deny GPS signals to an adversary would be an important maneuver and attack tool, especially in a highly decentralized and long-range targeting conflict such as an A2/AD environment with unmanned systems and attack munitions whose core functions rely on the signal.[16]

Competency 8: Directed Energy Systems

With the groundbreaking test of a laser weapons system aboard the USS *Ponce* in 2014, directed energy systems have never been closer to

---

12 "Spectrum Sensing and Shaping," Australian Department of Defence Science and Technology, http://www.dst.defence.gov.au/capability/spectrum-sensing-and-shaping (accessed August 18, 2016).

13 NovAtel, *Mitigating the Threat of GPS Jamming: Anti-Jam Technology* (white paper, Alberta, Canada: NovAtel, 2012).

14 Philip G. Mattos and Fabio Pisoni, "Quad Constellation Receiver: GPS GLONASS, Galileo, BeiDou," *GPS World*, January 1, 2014.

15 "The increasing risk of GPS systems," Homeland Security NewsWire, November 22, 2011, http://www.homelandsecuritynewswire.com/dr20111122-the-increasing-risks-of-gps-systems.

16 "China Unveils Anti-Drone Laser Weapon Able to Shoot Down 'Small Aircraft' within 5 Seconds," RT, 2 November 2014, https://www.rt.com/news/201795-china-drone-defense-laser/.

becoming integrated as fully operational military systems.[17] An effective capability that can block adversaries' electronics and communications, protect maritime and ground convoys in high risk zones, and protect critical land, maritime, and airborne assets is crucial in defeating future threats. Electromagnetic rail guns and directed energy missile technologies are now fielded capabilities in some countries. Once developed and deployed, these systems, such as the Tomahawk cruise missile and the Javelin antitank missile, are relatively inexpensive.

While size, weight, interoperability, and lethality are factors, other concerns, which mostly involve environmental extremes, limit directed energy weapons. Traditional assault rifles are reliable in extreme tropical, desert, and arctic conditions. They operate effectively in rain, snow, dust, and fog. They can generally be immersed in water and covered in mud without degrading their performance, and unlike directed energy systems, assault rifles are not negatively affected by solar flares or electromagnetic pulses.

A directed energy weapon relies on a sophisticated electronic circuit to generate an energy beam, which can be isolated and shielded from outside influence but not without adding weight and sophistication. Clouds, fog, rain, and snow are all enemies of directed energy. Today's powerful antimissile airborne systems simply burn their way through targets, but lower-energy man-portable systems will not have similar sustained power nor are they likely to be as reliable in extreme battlefield environments. Notwithstanding these caveats, directed energy weapons will continue to evolve and potentially offer a significant technology advantage against a peer adversary, especially against area denial systems such as integrated air defense networks and hypersonic antiship ballistic missiles.

Conclusion

As our forward-looking document, *Australia in the Asian Century* states, "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."[18] In a region that is increasingly dependent on its maritime, air, and land 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 in addition to maintaining regional access and engagement as part of a layered approach to global and regional security as well as continental defense. This amplification will require the Australian Defence Force to develop strategies and concepts for defeating adversaries' A2/AD capabilities as part of its core mission set. And, the well-defined, resourced, and balanced series of offset strategies mentioned here are important components to defeat any such mechanism.

A critical question must be: how will Australia afford an offset system such as that proposed in this paper? What legacy systems may have to be sacrificed in order to afford such a system? Whether it is all or part of the offset capabilities proposed, it is clear that Australia's

17 "US Navy Deploys Laser Weapon to Persian Gulf for First-Ever Combat Mission," RT, November 14, 2014, https://www.rt.com/news/205711-us-laser-weapon-persian/.

18 PM&C, *Australia in the Asian Century*, 1.

traditional "technology edge" within the Asian region is deteriorating—and quickly. And given its relatively small military force, the Australian government must either decide to leap to a technology end state that reasserts a technology edge or face a loss of global access and influence due to degraded military capabilities.