AN ESSAY ON DEVELOPMENT OF AN ADF INTEGRATED AIR AND MISSILE CAPABILITY TO COMBAT ADVANCED AIR AND MISSILE THREATS

by Flight Lieutenant Harrison Gray

Introduction

Access to foreign bases has long been a critical enabler of the ADF, and ongoing access will be key to Australia's future security[1]. In the past, these Forward Operating Bases (FOB) were considered relatively secure, however continual improvements to the range and accuracy of missiles acquired by adversarial militaries have made these bases attractive targets, being the seemingly soft underbelly of western militaries.

In order to continue utilisation of FOBs, and to guarantee the safety of deployed forces, the ADF cannot remain idle to the threat of advanced air and missile attacks. As such Australia must look to develop its Air and Missile Defence (AMD) capabilities in order to remain secure in future operations.

The aim of the essay is to discuss a range of AMD design and operating concepts to inform the development of an ADF Integrated AMD (IAMD) capability.

This essay will be structured into four key areas: western nations' historical and future reliance on FOBs to project power; the emerging threat of powerful state and non-state actors; Australia's response to emerging air and missile threats; and, IAMD design and operational concepts in an Australian context.

Australia's Reliance on Foreign Bases

The Australian Government has historically achieved its national interests through the deployment of the ADF overseas[2]. From a RAAF perspective, this has meant a reliance on overseas FOBs to project air power. While deployments to foreign air bases have incurred some risk to RAAF aircraft and their support elements, advancements in aircraft range and air to air refuelling capability has allowed the RAAF to be based

in relatively safe locations away from the battlespace. A notable example is Operations FALCONER, which saw the RAAF project air power into Iraq with little threat of reprisal from the Iraqi Armed Forces[3].

Since the end of the Cold War, western air forces have regularly based in partner nations just outside the reach of adversaries, effectively creating a rear area sanctuary. These rear area sanctuaries have made it difficult even for state based adversaries to attempt to disrupt the generation of air power[4]. However, state and non-state actors' access to a growing number of advanced air and missile technologies threatens to end the era of rear area sanctuaries as these air bases become viable targets.

The RAAF publication 'Beyond the Planned Air Force' recognises that advances in missile propulsion may necessitate the need to operate high value assets from locations further from harm, though this may not always be possible[5]. Suitable basing for these assets may only be available within range of an adversary's missiles, and foreign nations may place restrictions where RAAF aircraft can be operated from. Also, further advances in propulsion and guidance technology may advance to the stage where RAAF aircraft will be in range of attack no matter the distance. Despite the potential issues surrounding foreign air bases, Australia's isolated geography necessitates reliance on their accessibility to effectively project air power[6]. Malcolm Davis' Australian Strategic Policy Institute report further supports this argument, whereby he outlines that if Australia is to respond appropriately to future security challenges, deploying to FOBs in foreign nations will be necessary[7].

Australia does not face this problem alone; the United States (U.S.) military also relies heavily on access to foreign bases to project power[8]. It has been suggested that the U.S. needs to adapt its power-projection concepts to operate under greater threat of attack and treat rear areas as part of the battlespace[9]. With such comparable circumstances affecting the ADF, it should be paramount that the ADF adopts a similar mindset and prepare to defend itself regardless of time or place.

The Escalating Air and Missile Threat

The re-emergence of powerful state actors such as China and Russia are challenging U.S. military dominance, through progressively asserting their authority and influence in flashpoints across the globe (Eastern Ukraine, South China Sea and Taiwan) and challenging the rules based global order[10]. At the centre of increasingly heightened regional tensions are smaller state actors like Iran and North Korea, who show continuous disregard and contempt for the rules based global order[11].

These nations possess large inventories of conventional long range ballistic and cruise missiles as a corner stone of their military strategies, and the advent of global positioning system guided weapons in the 1990's have only increased the capability of their arsenals[12]. Recent technological developments into hypersonic and manoeuvrable re-entry vehicles, stealth, electronic countermeasures, improved guidance systems and decoys have further increased their lethality and difficultly to be defeated[13].

Even the limited application of these technologies has proven to be devastating. One notable incident is the suspected Iranian drone and cruise missile attack on Saudi Arabian oil processing facilities in September 2019. Despite possessing one of the most sophisticated air defence systems in the world, Saudi Arabia failed to intercept the 17 drones and eight cruise missiles launched against it[14].

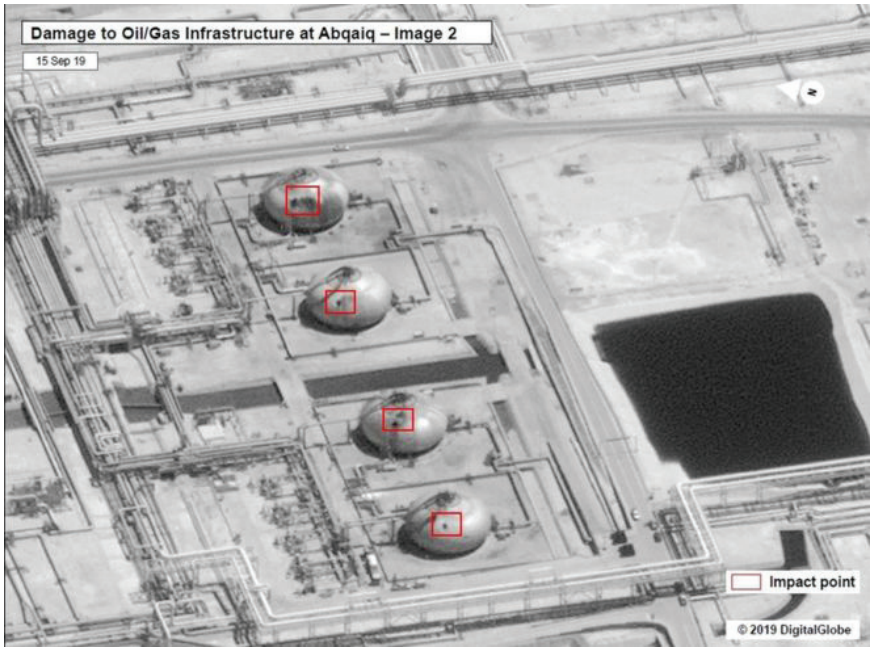

Figure 1 Aftermath of drone and cruise missile attacks on Saudi Aramco's Abaqaiq oil processing facility[15]

As an example of the consequences of a larger attack, a 2010 Research and Development (RAND) Corporation study modelled missile strikes on U.S. air bases near China and estimated that 30–50 theatre ballistic missiles would be sufficient to overwhelm air defences, destroy all parked aircraft and crater runways[16]. As of 2015, China's missile inventory is estimated to contain approximately 1400 ballistic missiles and hundreds of cruise missiles; enough to allow focused and committed attacks to interrupt and cease operations at one or more air bases for an extended period of time[17].

The employment of guided missiles and Unmanned Aerial Vehicles (UAVs) is not limited to state actors. Non-state actors have also gained access to a range of guided missiles through the proliferation of missile technology from state actors and the availability of commercial UAVs, which have enabled their entry into the air domain[18]. The Houthi rebels, in particular, have made extensive use of these technologies throughout the course of the Yemen civil war to great effect. Since 2015, the Houthi rebels have launched more than 250 missiles into Saudi Arabia killing at least 206 people, and have utilised UAVs as a means to conduct Intelligence, Surveillance, and Reconnaissance (ISR) and assassinations[19].

Australia's Response to the Growing Air and Missile Threat

Defence recognises the growing air and missile threat. It is clear in the '2016 Defence White Paper' that Australia must develop capabilities to counter increasingly sophisticated air and missile threats to Australian sovereign territory and deployed forces[20]. The push to expand Australia's AMD capabilities has seen the establishment of AMD focused projects across all three services, which include Air Force's Air 6500, Army's Land 19 Phase 7B and Navy's Sea 4000[21]. However, AVM Blackburn AO (Retd) argues that these projects alone cannot address the complexity of delivering an IAMD capability that can effectively counter the growing threat. He argues further that a quality Australian IAMD capability requires a top-down design approach[22].

Without a top-down approach, Australia risks repeating the U.S.'s past mistakes of bottom-up developed systems, which often lead to single points of failure, limited networking capability and ultimately a stifled

IAMD capability[23]. Additionally, IAMD must not be thought of as an Air Force owned and maintained capability either, as it will require elements from all branches of the Department of Defence. The inherent joint nature of IAMD is best summarised in the US Joint Integrated Air and Missile Defence: Vision 2020. It states that IAMD is, 'where all capabilities—defensive, passive, offensive, kinetic, non-kinetic— are meld into a comprehensive Joint and combined force capable of preventing an adversary from effectively employing any of its offensive air and missile weapons'[24].

Designing an Australian IAMD Capability

To ensure Australia's IAMD capability is designed appropriately, an IAMD vision and CONOPS must be developed to inform the top-down design process[25]. While the scope of an Australian IAMD vision and CONOPS is too vast to be thoroughly examined in this essay, the following sections will discuss a number of concepts to assist in developing an ADF IAMD capability.

Network Centric Framework. A network centric framework is vital to the success of an ADF IAMD capability, as evidenced by Air Force's investment into a Joint Battle Management System (JBMS) as part of Air 6500. The project has the ambitious aim to link ADF land, sea, air, electromagnetic and cyber systems to provide a shared and fused common operating picture and facilitate Integrated Fire Control (IFC)[26].

The challenge of such a project is integrating a vast number of disparate systems that were never designed to communicate with each other. One proposed solution is an open systems architecture design, which would ideally allow both new and old platforms to be rapidly integrated into the ADF IAMD construct and simplify the process of enabling interoperability between ADF and allied platforms[27].

To derive the most benefit from the network centric structure, it is crucial that the systems contributing to the IAMD capability are linked with each other at the lowest possible level to avoid stove piping of information and single points of failure[28]. The U.S. patriot missile system, illustrated in figure two, provides a comprehensive example of the stove piping vulnerabilities that must be avoided. Destroying or disabling a single radar or Command and Control (C2) node in the system will significantly diminish the surveillance and offensive capabilities of the patriot battery[29].

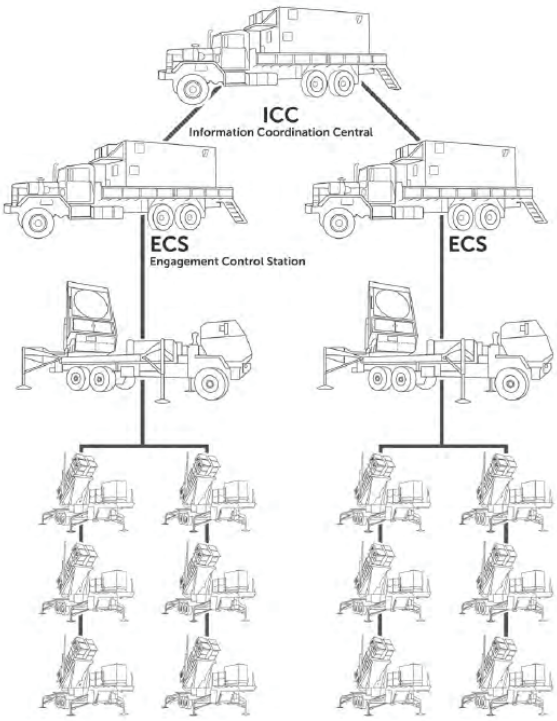

Figure 2 Data transfer stovepipe in current patriot battery configuration[30]

Increasing the links between sensors, shooters, and C2 elements not only provides resilience to attacks on single systems and eliminates information bottlenecks, but enhances the overall lethality of the IAMD system through the flexibility of IFC. IFC enables the best sensor to be linked with the best shooter to engage a target, ensuring a higher probability of kill. Further, it enables the use of weapons outside their own organic sensor range and the continued operation of weapons platforms as ISR contributors even after expending their own weapons[31].

To fully realise Air Force's JBMS, significant changes to ADF C2 structures will be required to leverage the potential of a network centric IAMD capability. According to the 'ADF Concept for Command and Control of the Future Force', currently practiced ADF C2 doctrine, 'emphasises the coordination of action through centralised control of activity'. The issue this creates is a decision-making bottleneck through a centralised controller and a potential single point of failure. If exploited by an adversary this could reduce the ability of IAMD forces to efficiently respond to threats. To circumvent this limitation, it has been suggested that the control aspect of C2 is shifted to focus on collaborative environment. This concept would see multiple force elements work together to achieve missions without needing to defer to a central controller[32].

Figure three outlines how a collaborative control environment would operate for a group of assets assigned to an AMD mission, with a Joint Mobile Operations Centre (JMOC) as the central controller and the primary control relationships coloured purple.

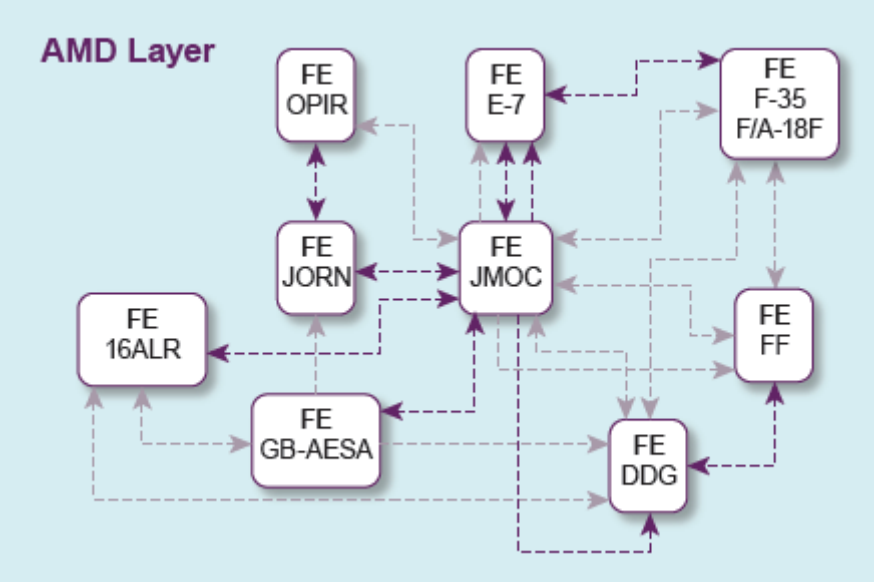

Figure 3 Default control state of an AMD mission[33]

In figure four, the control relationships have been shifted to focus on the Guided Missile Destroyer (DDG) after the loss of the JMOC. This assumes that the DDG would have the greatest situational awareness of the threat, allowing it to become the scene of action controller. As the DDG is closest to the threat and benefits from increased situational understanding over other platforms, it is placed in a unique position to direct other force elements until a more suitable platform becomes available to take control. The role of Command in both these scenarios would be to establish a Command intent and necessary direction to allow the force elements to effectively collaborate with each other, and determine the best mixture of control relationships for the mission and environment[34].

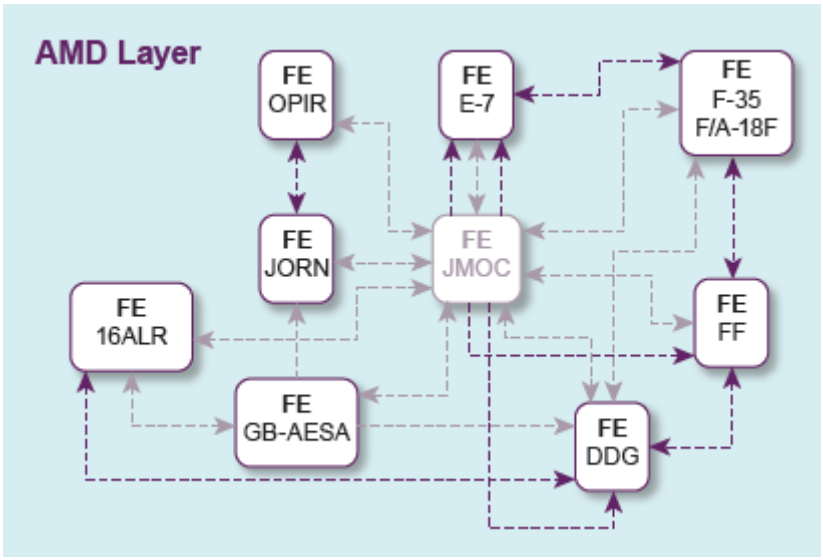

Figure 4 The default control state is shifted to focus on the DDG[35]

The final aspect to enabling network centric warfare is the introduction of Artificial Intelligence (AI). Automation in AMD has existed for some time, however this has always involved a human controller with the ability to intervene in the decision making process, and has also suffered from the previously-mentioned issues with regards to stove piped systems. AI is envisioned to take the vast amounts of information across all warfighting domains available, analyse and fuse it together to increase decision making speed and confidence; essentially, getting inside an adversary's OODA loop. Without AI, this task will likely be in excess

of the capabilities of current C2 structures, and the speed at which decisions need to be made will likely outpace the capability of any human controller. In addition to the significant technical challenges involved with integrating AI into ADF IAMD systems, there are serious ethical concerns surrounding the use of AI in weapon systems which must be addressed[36].

While AI has the potential to be used to enhance autonomous weapon discrimination through analysis of the vast amounts of data available in a networked system, it must be understood that humans will remain responsible for any actions carried out by the system[37]. This is particularly important when considering enemy action through cyber-attacks or Electronic Warfare (EW) could be used to falsify or corrupt data, potentially increasing the likelihood of fratricide[38]. Therefore, the correct balance of human-machine interactions must be found in the decision-making process for kinetic action, more so when considering the broad mission that is AMD[39].

Multi-Mission Shooters and Weapons. The resilience afforded to a network centric IAMD system can be further enhanced by building redundancy into the platforms and the weapons themselves. While most ground based air and missile defence launchers are paired with a specific type of interceptor, a greater emphasis should be placed on the ability for launchers to support a wider variety of weapons[40].

The Mark 41 Vertical Launch System (VLS) installed on the RAN's frigates and destroyers is an example of a launch system capable of supporting multiple weapons, capable of a variety of missions in air defence and strike[41]. The RAAF's planned acquisition of a ground based medium-range air defence capability should be similar in design. For a small defence force like the ADF, an air and road mobile land based system, such as the Mark 41 VLS, would be incredibly beneficial. Air Force would accomplish its goal of acquiring a medium range surface-to-air capability while having the option to expand mission scope to include strike, additionally, costs would be decreased through shared weapon stocks with the RAN.

Figure 5 Patriot launcher multi-mission configurations[42]

The examples described above of integrating offensive strike capabilities into ground based air defence platforms could provide additional assets to contribute to left of launch strategies and a potential counter battery capability[43]. Similarly, this concept could be applied to missile based platforms designed primarily for sur-

face to surface fires (eg. Multiple launch rocket systems) integrating air defence missiles into their available weapons inventory.

Another method of increasing lethality of air defence assets is to build versatility into the missiles. A continued increase in missile ranges and miniaturisation of guidance technology could allow missiles to have an expanded mission set. The RAN's planned acquisition of the SM-6 missile is a prominent example of a weapon that has seen an increasing mission set throughout its life-cycle. Originally based on the SM-2 for ship based air defence, subsequent upgrades have allowed it to target cruise missiles, ballistic missiles and a limited capacity to be used as an anti-ship missile[44].

The drawback of missiles with a broad mission set is that they may not always be the most cost effective option. The previously mentioned SM-6 costs over four times the amount of a single harpoon anti-ship missile[45]. This is not to discredit the inherent flexibility and redundancy provided by such missiles, but to highlight that a one size fits all solution may not be the answer to address the wide range of threats and missions for the RAAF's medium range surface-to-air capability.

Cyber and Electronic Warfare Protection. An Israeli air strike on a Syrian nuclear facility in 2007 highlighted the effectiveness of cyber and EW against air defence systems. While details remain scarce as to how Israel actually achieved the strike, there is speculation that an advanced EW program allowed Israeli operators to infiltrate communication and computer systems associated with the Syrian air defence network to misdirect and blind the Syrian operators to the presence of the Israeli aircraft. Ultimately this allowed non-stealthy strike aircraft to penetrate a comprehensive air defence network and return without harassment[46].

Two lessons can be derived from this event: The first is the line between electronic and cyber warfare is becoming increasingly blurred as EW increases in complexity, producing effects not possible with traditional electronic jamming (producing excessive electronic noise). Secondly, there is a need to prioritise protection of the ADF's future IAMD system against modern cyber and EW threats.

The unfortunate reality is that designing an IAMD system that is completely resistant to cyber espionage or cyber-attack is a near-impossible task due to the inherent size and complexity of a tri-service IAMD system. Instead of trying to stop all threats at all times, Snyder et al suggests that the focus of cybersecurity efforts should be, 'limiting adversary intelligence exploitation to an acceptable level and ensuring an acceptable level of operational functionality even when attacked offensively through cyberspace'[47]. To maintain these acceptable levels of assurance, it is essential that cybersecurity is considered in all phases of the system life-cycle by all stakeholders and is not treated as an afterthought[48].

Blackburn has argued that a bottom-up approach to implementing cybersecurity to an IAMD system is not appropriate and a program-level architecture is required to properly mitigate cybersecurity risks[49]. However, a top-down design approach to cybersecurity not without its own risks. A top-down approach that focuses on achieving cybersecurity through the implementation of generalised solutions could lead to stifling innovative ideas needed to maintain pace with the rapid development of technology and a changing threat environment. The highly technical and complex nature of cybersecurity warrants that decision making on how problems are solved is decentralised to the appropriate level of technical expertise, while senior leadership remain focused on goals and requirements. Achieving an acceptable level of mission assurance of our cyber systems

while under attack should be the preferred outcome, as opposed to simply seeking compliance with policies and directives, which in itself does not guarantee cybersecurity[50].

Passive Defence Measures. While active offensive and defensive elements are critical to an effective IAMD capability, there is a renewed focus on how passive defence measures can contribute to enhancing the IAMD capability. While there have been no recent significant or revolutionary modifications to the concept of passive defence measures, their application among western forces has fallen into disuse in the past few decades[51]. If the ADF wishes to exploit all avenues to possess a credible IAMD capability, the implementation of passive defensive measures must not be overlooked.

Even with the advent of modern air and space based ISR capabilities Camouflage, Concealment and Deception (CCD) can still play an important role in complicating an enemy's ability to effectively target assets and infrastructure. Installation of decoy aircraft shelters, ground support equipment, aircraft and missile defence installations are all methods to complicate the enemy's targeting cycle[52].

Inflatable or metal construct decoys may present a successful deception for some aircraft, vehicles and buildings, but the illusion becomes harder to maintain when an adversary expects equipment to emit distinct infrared and electronic signatures. Karako and Rumbaugh have highlighted the potential for a range of missile systems to be installed in shipping containers to provide visual concealment. These containerised missile systems could be grouped with additional decoy containers that would employ electronic, infrared, electro-optical and logistical decoys to complete the deception[53].

Figure 6 A missile launch system concealed in a shipping container[54]

Dispersal of forces and equipment across a single or multiple bases can reduce the impact that any one missile or bomb can inflict on friendly forces and complicates enemy targeting. However, the ability to appropriately disperse forces during operations may not always be possible. Issues preventing this may include availability of aircraft parking space, the host nation allocating limited parking space or restricting foreign forces entering air bases entirely. Additionally, the burden is placed on security forces, logistical support elements and maintenance personnel to support forces dispersed across a larger area. The increased surviv-

ability attributed to dispersed operations is certainly advantageous, but this needs to be weighed against the logistical efficiencies associated with more concentrated operations[55].

One further passive defensive measure is hardening of air base infrastructure. Air Force has highlighted the need to upgrade and harden it's infrastructure to counter the next generation of threats[56]. The issue is, this goal may only be achievable on Australian soil as opportunities to harden infrastructure overseas are limited. Again, this is not an Australian unique problem, even the U.S. military's ability to construct high quality hardened shelters on foreign soil may not always be practical from an operational, financial and political standpoint[57]. None the less, hardening of key infrastructure should still remain an option when possible as part of a range of considerations in improving airbase resiliency either in Australia or overseas.

Allied Interoperability. A properly designed ADF IAMD has the ability to greatly enhance the lethality of the ADF. However, even with a perfect system, due to the inherent size of Australia's military compared to the vast missile inventories of nations such as China, the ADF will remain at a disadvantage if facing these threats alone[58]. Engagement and cooperation with traditional and regional allies on IAMD will be crucial to protect deployed forces from potential air and missile threats.

Seeking allied engagement on IAMD will predominately serve to provide mass to the AMD forces available to defeat air and missile threats. As our closest and largest military ally, the U.S. will likely be the allied partner of choice to provide equipment and manpower to reinforce ADF AMD deficiencies; although this should not discount other nations from becoming integral contributors to the ADF IAMD mission. A continually improving Defence relationship with Japan will present opportunities for cooperation on IAMD, as this country has signalled in its latest Defence White Paper, plans to integrate and enhance its air and missile defence capability[59]. The Five Powers Defence Arrangement could also provide a platform to explore IAMD cooperation through the Headquarters Integrated Area Defence System.

It is also important to place increased focus on international engagement in IAMD so as to normalise the deployment of ADF IAMD assets in foreign nations. Critical enablers to an ADF IAMD system such as the MC-55A, E-7A, electronic warfare systems and ground based sensors, could potentially be seen as intelligence collection threats to a host nation. This inference could delay or even prevent the deployment of key platforms into theatre, thereby severely degrading an IAMD system. Introduction of Australia's IAMD capabilities to other nations should begin through AMD focused exercises on Australian soil. Australia's vast weapons ranges would serve as valuable testing grounds for the modern missile capabilities of other nations while allowing the ADF to demonstrate its IAMD capabilities[60]. These exercises would serve as a suitable precursor for the ADF to deploy IAMD capabilities on leading regional exercises such as RED FLAG, COPE NORTH, and the BERSAMA series, cementing the normalisation of ADF IAMD assets operating throughout the region.

Conclusion

Australia's requirement for an IAMD capability is being driven by both its need to maintain access to foreign bases to support potential future operations, and to address the increasing threats to these bases from the air and missile capabilities of powerful state actors and hostile non-state actors. FOBs that were once thought of as safe from such threats are now potentially viable targets; which has forced an attitude change in the ADF, appreciating that no element of a deployed force is guaranteed to be safe from enemy action.

The Australian response to this threat has been to pursue a number of AMD related projects across the three services. However, it has been highlighted throughout the numerous references above that, simply pursuing these projects alone will not create an effective IAMD system. In order to enable an efficient and effective IAMD system, a top-down approach underpinned by an ADF-unique IAMD vision and CONOPS is required.

The core concepts underpinning the future ADF IAMD capability should include an AI enabled network centric design, mission versatile weapons and weapon systems, cyber and EW protection, and the adoption of advanced CCD. All of these concepts will contribute to the survivability of the IAMD system and the forces it protects against modern air and missile threats. Furthermore, broad regional IAMD engagement will be needed to offset Australia's comparatively small military. As the ADF looks towards the future, a networked, resilient and interoperable IAMD system will prove to be a critical enabler to the defence of Australian assets and personnel in future operations.

Bibliography

Air Power Development Centre 2018, 'Pathfinder' *Countering Unmanned Aerial Vehicles*, Bulletin, Issue 316, Royal Australian Air Force Air Power Development Centre, Canberra, ACT, viewed 19 January 2019, <http://airpower.airforce.gov.au/APDC/media/PDF-Files/Pathfinder/PF316-Countering-Unmanned-Aerial-Vehicles.pdf>.

Australian Defence Force 2018, 'ADF Concept for Command and Control of the Future Force', Department of Defence, [Canberra].

Blackburn, J 2017, 'Integrated Air and Missile Defence Study' *The Challenge of Integrated Force Design*, Report, The Sir Richard Williams Foundation, viewed 23 January 2019, <http://www.williamsfoundation.org.au/resources/Pictures/WF_IAMD_ReportFinal.pdf>.

Chatham House 2015, 'Challenges to the Rules-Based International Order', Chatham House, The Royal Institute of International Affairs, James's Square, London, viewed 27 July 2019 <https://www.chathamhouse.org/london-conference-2015/background-papers/challenges-to-rules-based-international-order>.

Davis, M 2019, 'Forward Defence in Depth for Australia', Report, Australian Strategic Policy Institute, Barton, ACT, viewed 23 August 2019, <https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-06/SI%20139%20Forward%20defence%20in%20depth.pdf?vfiVknPEa5saKIFEqC_jI_5IFSkwtKvg>.

Department of Defence 2016, '2016 Defence Integrated Investment Program', Commonwealth of Australia, Canberra.

Department of Defence 2016, '2016 Defence White Paper', Commonwealth of Australia, Canberra.

Eberhart, D 2019, 'Drone Attacks Test Saudi Aramco, Deliver Wake Up Call To Global Markets', Forbes, Forbes Media LLC, Jersey City, NJ, viewed 02 December 2019, < https://www.forbes.com/sites/daneberhart/2019/09/16/drone-attacks-test-saudi-aramco-deliver-wake-up-call-to-global-markets/#-167ec2da17b9>.

Gasparre, R B 2008, 'The Israeli "E-tack" on Syria – Part I', Air Force Technology, Verdict Media Limited, London, UK, 9 March, viewed 17 October 2019, <https://www.airforce-technology.com/features/feature1625/>.

Gasparre, R B 2008, "The Israeli 'E-tack" on Syria – Part II', Air Force Technology, Verdict Media Limited, London, UK, 10 March, viewed 17 October 2019, < https://www.airforce-technology.com/features/feature1669/>.

GlobalSecurity.org 2020, 'RIM-174 SM-6 Extended Range Active Missile (ERAM)', GlobalSecuirty.org, Alexandria, VA, viewed 10 January 2020, < https://www.globalsecurity.org/military/systems/munitions/sm-6.htm>.

Heginbotham, E, Nixon, M, Morgan, FE, Heim, JL, Li, S, Engstrom, J, Libicki, MC, DeLuca, P, Shlapak, DA, Frelinger, DR, Laird, B, Brady, K, & Morris, LJ 2015, 'The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power 1996-2017', Report, RAND Corporation, Santa Monica, CA, viewed 24 November 2019, <https://www.rand.org/pubs/research_reports/RR392.html>.

Japan Ministry of Defense, 2019, 'Defense of Japan 2019', Digest, Ministry of Defense, The Government of Japan, Shinjuku-ku, Tokyo, viewed 04 January 2020, <https://www.mod.go.jp/e/publ/w_paper/pdf/2019/DOJ2019_Digest_EN.pdf>.

Joint Chiefs of Staff 2013, 'Joint Integrated Air and Missile Defense: Vision 2020', [United States Department of Defence], [Washington, DC], viewed 24 August 2019, <https://www.jcs.mil/Portals/36/Documents/Publications/JointIAMDVision2020.pdf>.

Karako, T & Rumbaugh, W 2018, 'Distributed Defense' *New Operational Concepts for Integrated Air and Missile Defense*', Report, Centre for Strategic and International Studies, Washington, DC, viewed 23 August 2019, <https://csis-prod.s3.amazonaws.com/s3fs-public/publication/171206_Karako_DistributedDefense_Web_0.pdf?GqH4Iie2m_7aMFqFKMRWu.3vdT18tMdO>.

Kuper, S 2019, 'Enabling the "system of systems" and ADF interoperability with AIR 6500', Defence Connect, North Sydney, NSW, date viewed 14 April 2019, <https://www.defenceconnect.com.au/key-enablers/3617-enabling-the-system-of-systems-and-adf-interoperability-with-air-6500>.

Layton, P 2018, 'Algorithmic Warfare' *Applying Artificial Intelligence to Warfighting*, Air Power Development Centre, Canberra, ACT, viewed 18 August 2019, <http://airpower.airforce.gov.au/APDC/media/PDF-Files/Contemporary%20AirPower/AP33-Algorithmic-Warfare-Applying-Artificial-Intelligence-to-Warfighting.pdf>.

Missile Defense Advocacy Alliance 2019, 'Today's Missile Threat', Missile Defense Advocacy Alliance, Alexandria, VA, viewed 22 February 2019, < https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/>.

Pence, E 2019, 'Iran's Drone and Missile Attack on Saudi Arabia is a Huge Problem', The National Interest, Centre for the National Interest, NW Washington, DC, viewed 29 October 2019, <https://nationalinterest.org/blog/buzz/irans-drone-and-missile-attack-saudi-arabia-huge-problem-90011>.

Royal Australian Air Force 2013, 'AAP 1000–H' *The Australian Experience of Air Power*, Second Edition, Air Power Development Centre, Department of Defence, Canberra.

Royal Australian Air Force 2017, 'Air Force Strategy 2017–2027', Air Power Development Centre, Canberra, ACT, viewed 01 January 2019, <http://airpower.airforce.gov.au/APDC/media/PDF-Files/Air%20Force%20Publications/AF32-Air-Force-Strategy-2017-2027.pdf>.

Royal Australian Air Force 2017, 'Beyond the Planned Air Force Thoughts on Future Drivers and Disruptors', Royal Australian Air Force Air Power Development Centre, Canberra, ACT, viewed 01 January 2019, <http://airpower.airforce.gov.au/APDC/media/PDF-Files/Air%20Force%20Publications/AF34_Beyond-the-Planned-Air-Force.pdf>.

Royal Australian Navy [2019], 'Frigate, Helicopter (FFH)', Navy, Department of Defence, [Canberra], viewed 14 October 2019, < https://www.navy.gov.au/fleet/ships-boats-craft/ffh>.

Snow, S 2019, 'Drone and Missile Attacks Against Saudi Arabia Underscore Need for More Robust Air Defenses', Military Times, Vienna, VA, viewed 29 October 2019, <https://www.militarytimes.com/flashpoints/2019/10/25/drone-and-missile-attacks-against-saudi-arabia-underscore-need-for-more-robust-air-defenses/>.

Synder, D, Powers, JD, Bodine-Baron, E, Fox, B, Kendrick, L & Powell MH 2015, 'Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles', Report, RAND Corporation, Santa Monica, CA, viewed 07 September 2019, <https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1007/RAND_RR1007.pdf>.

United States Navy 2017, 'Harpoon Missile', United State Navy, Washington, DC, viewed 10 January 2020, < https://www.navy.mil/navydata/fact_display.asp?cid=2200&tid=200&ct=2>.

Vick, AJ 2015, 'Air Base Attacks and Defensive Counters' *Historical Lessons and Future Challenges*, Report, RAND Corporation, Santa Monica, CA, viewed 01 January 2019, <https://www.rand.org/content/dam/rand/pubs/research_reports/RR900/RR968/RAND_RR968.pdf>.

Endnotes

1 Royal Australian Air Force, 2013, 'AAP 1000–H' The Australian Experience of Air Power, Second Edition, Air Power Development Centre, Department of Defence, Canberra.

2 Royal Australian Air Force, 2013.

3 Vick, AJ 2015, 'Air Base Attacks and Defensive Counters' Historical Lessons and Future Challenges, Report, RAND Corporation, Santa Monica, CA, p 62, viewed 01 January 2019, <https://www.rand.org/content/dam/rand/pubs/research_reports/RR900/RR968/RAND_RR968.pdf>.

4 Vick, AJ 2015, p 9.

5 Royal Australian Air Force 2017, 'Beyond the Planned Air Force Thoughts on Future Drivers and Disruptors', Royal Australian Air Force Air Power Development Centre, Canberra, ACT, p 23–24, viewed 01 January 2019, <http://airpower.airforce.gov.au/APDC/media/PDF-Files/Air%20Force%20Publications/AF34_Beyond-the-Planned-Air-Force.pdf>.

6 Vick, AJ 2015, p 2.

7 Davis, M 2019, 'Forward Defence in Depth for Australia', Report, Australian Strategic Policy Institute, Barton, ACT, p 10, viewed 23 August 2019, <https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-06/SI%20139%20Forward%20defence%20in%20depth.pdf?vfiVknPEa5saKIFEqC_jI_5IFSkwtKvg>.

8 Vick, AJ 2015, p 2.

9 Vick, AJ 2015, p 64–65.

10 Chatham House 2015, 'Challenges to the Rules-Based International Order', Chatham House, The Royal Institute of International Affairs, James's Square, London, viewed 27 July 2019 <https://www.chathamhouse.org/london-conference-2015/background-papers/challenges-to-rules-based-international-order>.

11 Missile Defense Advocacy Alliance 2019, 'Today's Missile Threat', Missile Defense Advocacy Alliance, Alexandria, VA, viewed 22 February 2019, < https://missiledefenseadvocacy.org/missile-threat-and-proliferation/todays-missile-threat/>.

12 Vick, AJ 2015, p 20.

13 Blackburn, J 2017, 'Integrated Air and Missile Defence Study' The Challenge of Integrated Force Design, Report, The Sir Richard Williams Foundation, p 9–10, viewed 23 January 2019, <http://www.williamsfoundation.org.au/resources/Pictures/WF_IAMD_ReportFinal.pdf>.

14 Pence, E 2019, 'Iran's Drone and Missile Attack on Saudi Arabia is a Huge Problem', The National Interest, Centre for the National Interest, NW Washington, DC, viewed 29 October 2019, <https://nationalinterest.org/blog/buzz/irans-drone-and-missile-attack-saudi-arabia-huge-problem-90011>.

15 Eberhart, D 2019, 'Drone Attacks Test Saudi Aramco, Deliver Wake Up Call To Global Markets', Forbes, Forbes Media LLC, Jersey City, NJ, viewed 02 December 2019, < https://www.forbes.com/sites/daneberhart/2019/09/16/drone-attacks-test-saudi-aramco-deliver-wake-up-call-to-global-markets/#167ec2da17b9>.

16 Vick, AJ 2015, p 23–24.

17 Heginbotham, E, Nixon, M, Morgan, FE, Heim, JL, Li, S, Engstrom, J, Libicki, MC, DeLuca, P, Shlapak, DA, Frelinger, DR, Laird, B, Brady, K, & Morris, LJ 2015, 'The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power 1996-2017', Report, RAND Corporation, Santa Monica, CA, p 48, viewed 24 November 2019, <https://www.rand.org/pubs/research_reports/RR392.html>.

18 Air Power Development Centre 2018, 'Pathfinder' Countering Unmanned Aerial Vehicles, Bulletin, Issue 316, Royal Australian Air Force Air Power Development Centre, Canberra, ACT, viewed 19 January 2019, <http://airpower.airforce.gov.au/APDC/media/PDF-Files/Pathfinder/PF316-Countering-Unmanned-Aerial-Vehicles.pdf>; Missile Defense Advocacy Alliance 2019.

19 Snow, S 2019, 'Drone and Missile Attacks Against Saudi Arabia Underscore Need for More Robust Air Defenses', Military Times, Vienna, VA, viewed 29 October 2019, <https://www.militarytimes.com/flashpoints/2019/10/25/drone-and-missile-attacks-against-saudi-arabia-underscore-need-for-more-robust-air-defenses/>.

20 Department of Defence 2016, '2016 Defence White Paper', Commonwealth of Australia, Canberra, p 96–97.

21 Department of Defence 2016, '2016 Defence Integrated Investment Program', Commonwealth of Australia, Canberra, p 84, 99–100.

22 Blackburn, J 2017, p 11–12.

23 Blackburn, J 2017, p 13.

24 Joint Chiefs of Staff 2013, 'Joint Integrated Air and Missile Defense: Vision 2020', [United States Department of Defence], [Washington, DC], p 1, viewed 24 August 2019, <https://www.jcs.mil/Portals/36/Documents/Publications/JointIAMDVision2020.pdf>.

25 Blackburn, J 2017, p 17.

26 Kuper, S 2019, 'Enabling the "system of systems" and ADF interoperability with AIR 6500', Defence Connect, North Sydney, NSW, date viewed 14 April 2019, <https://www.defenceconnect.com.au/key-enablers/3617-enabling-the-system-of-systems-and-adf-interoperability-with-air-6500>.

27 Blackburn, J 2017, p 13.

28 Karako, T & Rumbaugh, W 2018, 'Distributed Defense' New Operational Concepts for Integrated Air and Missile Defense', Report, Centre for Strategic and International Studies, Washington, DC, p 10, viewed 23 August 2019, <https://csis-prod.s3.amazonaws.com/s3fs-public/publication/171206_Karako_DistributedDefense_Web_0.pdf?GqH4Iie2m_7aMFqFKMRWu.3vdT18tMdO>.

29 Karako, T & Rumbaugh, W 2018, p 11.

30 Karako, T & Rumbaugh, W 2018, p 11.

31 Karako, T & Rumbaugh, W 2018, p 20–21.

32 Australian Defence Force 2018, 'ADF Concept for Command and Control of the Future Force', Department of Defence, [Canberra], p 22–23.

33 Australian Defence Force 2018, p 25.

34 Australian Defence Force 2018, p 25–26.

35 Australian Defence Force 2018, p 26.

36 Layton, P 2018, 'Algorithmic Warfare' Applying Artificial Intelligence to Warfighting, Air Power Development Centre, Canberra, ACT, p 59, viewed 18 August 2019, <http://airpower.airforce.gov.au/APDC/media/PDF-Files/Contemporary%20AirPower/AP33-Algorithmic-Warfare-Applying-Artificial-Intelligence-to-Warfighting.pdf>.

37 Layton, P 2018, p 10.

38 Layton, P 2018, p 67.

39 Layton, P 2018, p 28–29.

40 Karako, T & Rumbaugh, W 2018, p 25.

41 Royal Australian Navy [2019], 'Frigate, Helicopter (FFH)', Navy, Department of Defence, [Canberra], viewed 14 October 2019, <https://www.navy.gov.au/fleet/ships-boats-craft/ffh>.

42 Karako, T & Rumbaugh, W 2018, p 30.

43 Karako, T & Rumbaugh, W 2018, p 30.

44 Karako, T & Rumbaugh, W 2018, p 32.

45 GlobalSecurity.org 2020, 'RIM-174 SM-6 Extended Range Active Missile (ERAM)', GlobalSecuirty.org, Alexandria, VA, viewed 10 January 2020, < https://www.globalsecurity.org/military/systems/munitions/sm-6.htm>; United States Navy 2017, 'Harpoon Missile', United State Navy, Washington, DC, viewed 10 January 2020, < https://www.navy.mil/navydata/fact_display.asp?cid=2200&tid=200&ct=2>.

46 Gasparre, R B 2008, 'The Israeli "E-tack" on Syria – Part I', Air Force Technology, Verdict Media Limited, London, UK, 9 March, viewed 17 October 2019, <https://www.airforce-technology.com/features/feature1625/>; Gasparre, R B 2008, "The Israeli 'E-tack" on Syria – Part II', Air Force Technology, Verdict Media Limited, London, UK, 10 March, viewed 17 October 2019, < https://www.airforce-technology.com/features/feature1669/>.

47 Synder, D, Powers, JD, Bodine-Baron, E, Fox, B, Kendrick, L & Powell MH 2015, 'Improving the Cybersecurity of U.S. Air Force Military Systems Throughout Their Life Cycles', Report, RAND Corporation, Santa Monica, CA, p 2, viewed 07 September 2019, <https://www.rand.org/content/dam/rand/pubs/research_reports/RR1000/RR1007/RAND_RR1007.pdf>.

48 Snyder, D et al 2015, p 5.

49 Blackburn, J 2017, p 14.

50 Snyder, D et al 2015, p 13–14.

51 Vick, AJ 2015, p 9.

52 Vick, AJ 2015, p 40–43.

53 Karako, T & Rumbaugh, W 2018, p 34–38.

54 Karako, T & Rumbaugh, W 2018, p 40.

55 Vick, AJ 2015, p 53–54.

56 Royal Australian Air Force 2017, 'Air Force Strategy 2017–2027', Air Power Development Centre, Canberra, ACT, p 32, viewed 01 January 2019, <http://airpower.airforce.gov.au/APDC/media/PDF-Files/Air%20Force%20Publications/AF32-Air-Force-Strategy-2017-2027.pdf>.

57 Vick, AJ 2015, p 53.

58 Heginbotham, E et al 2015, p 48.

59 Japan Ministry of Defense, 2019, 'Defense of Japan 2019', Digest, Ministry of Defense, The Government of Japan, Shinjuku-ku, Tokyo, p 18, viewed 04 January 2020, <https://www.mod.go.jp/e/publ/w_paper/pdf/2019/DOJ2019_Digest_EN.pdf>.

60 Davis, M 2019, p 7.