Advanced Technology and Strategy
Team Phoenix

New technologies provide options for the protection of Australia that we have not had before. What might this mean in particular for a long range strike capability? In particular, in the context of the 21st century, what does “long range”, “strike” and “strategic” actually mean and what are the range of options we might have for a 21st century deterrent built around long-range strategic strike?
EXECUTIVE SUMMARY

In a degraded geostrategic environment, strategic long-range strike is fundamental to Australia's defence through the provision of deterrence. In the Australian context, deterrence is best achieved by exploiting power asymmetry, ensuring an adversary actions are costlier than any perceived benefit. This paper will argue that long-range strategic strike is a system that encompasses the entire targeting cycle (D3A), and examine how advanced technologies will increase credibility and achieve deterrence in the face of increasingly sophisticated anti area axis denial (A2AD) capabilities.

As part of a strategic long-range strike system, detection needs to be considered a critical component of strategic strike capabilities as we face threats beyond traditional kinetic strike in a complex threat environment. Reduced warning of escalation in an increasingly volatile environment means early detection is essential to providing context and strategic warning to decision-makers. This is best achieved through a cohesive, multi-disciplined approach. An integrated system would overcome information access/sharing delays, and fluidly engaged integration of detection and decision-making processes supported by AI-augmented sensor integration can enable rapid tipping and cuing of sensors, early warning, timely decision-making and execution of directives.

AI-enabled decision making will be central to the 'Decide' phase of an Australian Long-Range Strike System. The System will still rely on personnel, with AI augmenting contemporary staff systems. The Decide phase will similarly be enhanced by the fidelity of AI advice based on superior quantitative and qualitative analysis.

The crux of deterrence and the long-range strike system is delivery. Future systems will use kinetic and non-kinetic effects, synchronised and orchestrated to achieve complex effects against adversary systems. Such future systems will include EMP, Hypersonic, Swarming weapons, and Autonomous systems, all enabled by space and cyber capabilities. The layered systems provide kinetic and non-kinetic effects to the AI system to present as options to achieve desired effects on Adversary systems.

Finally, the assess phase will leverage the elements of the detect and decide capabilities to determine the efficacy of the long-range strike system. Investment in advanced battle damage assessment is a component of the assess phase, with sophisticated AI-enabled analysis of adversary decision making and response, being calculated to determine, not only physical effect but the compounding effect on adversary offensive systems.

This paper has argued that long range strategic strike is a system that encompasses the entire D3A, and has examined how advanced technologies will increase Australia's credibility and achieve modern deterrence in the face of increasingly sophisticated A2AD capabilities. Strategic long-range strike and deterrence must evolve with the changing nature of Australia's adversaries. Modern and future A2AD systems provide Australia's adversaries with a technological advantage, however, Australia is well postured to adopt a whole of government strike system to further enhance the ADFs ability to protect Australia and its national interest.
INTRODUCTION

The future consists of a high degree of uncertainty; however, it also presents a unique opportunity to shape future capability. Through the application of the ‘D3A targeting cycle’ within a fictitious future threat scenario, this paper will outline Australia’s future protection capability (2040-2050) through the acquisition of a long-range strategic strike system. To achieve this, it will demonstrate the practical application of an Australian Long-Range Strike system, demonstrating its relevance to modern conventional deterrence from a revisionist perspective. Furthermore, in the analysis of the problem set Long-Range Strategic Strike was viewed as a system of systems that encompasses the D3A targeting cycle, this was done for three reasons. Firstly, significantly enhanced future defences will require a holistic approach to ‘strike effects.’ Secondly, Australia’s middle power status and the boutique nature of our ADF requires mass to be replaced by superior decision-making. Finally, the abundance of sensor capabilities that the ADF seeks to employ ultimately need to be synchronised and orchestrated into a coherent strategy that enables said ‘strike effects.’

This paper will argue that long-range strategic strike is a system that encompasses the entire D3A, and examine how advanced technologies will increase credibility in the face of increasingly sophisticated A2AD capabilities, and achieve deterrence. This paper will achieve this by discussing future technology in the context of a future threat scenario, demonstrating the technologies involved in deterrence, long-range strike as part of a system. Firstly, it will outline the general background. Secondly it will discuss the specifics of the targeting cycle, progressing through Detect, Decide, Deliver, and Assess. During the Targeting Cycle specific technologies will be highlighted with the key impacts of each phase, and the essential systems links being articulated.

AUSTRALIAN SECURITY 2040-2050

As Australia approaches 2050, key regional geostrategic security actions through the period 2040-2050 require examination at the unclassified level. With the Great Energy Crisis of the 2030s and resultant global hostilities Australia must position itself to defend its national interests particularly the Southern Ocean regional energy production zone.v

A critical turning point in history was the significant enhancement of deep water ocean technology in the 2020s along with the ratification of the Antarctic treaty reaffirming Australia’s claims and maintenance of Antarctic regional preservation.vi This technological development enabled significant land reclamation of the South West Pacific nations under threat from the rising sea levels resulting from climatic changes. Deep water ocean technology facilitated the dredging and enhancement of Southern Ocean channels which enabled not only land reclamation but also enhanced the strength of the Antarctic circumpolar currents. A critical by-product of the altered Coldwater currents increased the South West Pacific and Southern Ocean marine stocks through improved breeding grounds and migratory zones.

The increased strength and intensity of the Antarctic Circumpolar currents, indicated in Figure 1, enabled the creation of multiple Marine Hydrokinetic power generation plants located in several fields within the Southern Ocean which utilised the strength of ocean currents for mass energy production. This technology enabled Australia, New Zealand, and South West Pacific nations to protect themselves from the impact of the Great Energy Crisis which occurred during the 2030s resulting from the depletion and, in several regions, complete exhaustion of fossil fuels.
Whilst Australia maintains stable regional alliances, and existing historical alliances and agreements between the North and South Americas, Canada and most European nations there is an ongoing risk of global instability and threats to Australian national interests. As one of the principal energy providers in the Indo-Pacific rim, the key geostrategic national interest is the maintenance and security of the Southern Ocean Regional Energy Production Zones. To achieve this, Australia must continue positioning itself to defend and deter hostilities through decision, detection, delivery and assessment of threats. Due to the global nature of potential threats including cyber and space it is essential to ensure deterrence through the development and maintenance of a long-range strike system as was indicated in the 2048 conflict with Kamaria.

An additional key technological development directly impacting Australia’s capability was the development of ‘Nulla-Nulla’ an Artificial Intelligence (AI) Process, Exploitation and Dissemination (PED) program. Nulla-Nulla linked vast quantities of data generated through the systems of ADF sensors and expedited military staff functions. Nulla-Nulla was the progeny of Project Maven, AlphaGo and Data61.

**DETECT**

Leading into the conflict, Defence Intelligence Group (DIG) analysts noted a marked drop in communications/signals intelligence of key Kamarian decision-makers, including consistent periodic outages of personal monitoring system data collection.\(^\text{vii}\) Review of satellite imagery of known primary working locations for these individuals revealed vehicular parking patterns inconsistent with routine business over the period. Australian owned AI-augmented satellites were subsequently tasked to track vehicle\(^\text{ix}\) and signals movements, specifically, to track available individual-associated signals of interest, determine a point of culmination for these key Kamarian members, image the location, initiate visual vehicle tracking, and ultimately image and scan the final destination. This identified a new heavily secured, command and control capable underground bunker.

Nulla-Nulla rapidly reviewed available databases, determining there had been an increase in activity at this location, following the break-down in Kamarian-AUS engagement. This new information increased Nulla-Nulla’s assessed likelihood of further escalatory action to 90% certainty. Tasked with identifying any related activity in Kamaria over the defined period, Nulla-Nulla scanned databases and open source resources (including social media). Nulla-
Nulla determined it was probable that personnel were being prepared for KMS 1 and KMS 2, with facial recognition confirming which naval Commanders were in the area. Additionally, based on the number of personnel and support staff detected at that location it was determined that there was at least one fighter wing now stationed at Woody Island. Nulla-Nulla also flagged increased activity detections at an anti-satellite site in Laeg and near the Mimbe submarine base. Satellite monitoring of each of these locations was increased, Joint Operations Command (JOC) commenced preparations for reduced notice to move as well as preparations for the deployment of networked Automated Underwater Vehicles (AUV) to monitor territorial boundaries at sea.

Imagery analysis identified a naval task group comprising 3 Frigates and 2 support tankers, had departed Port Preparatory. Nulla-Nulla initiated satellite tracking procedures and essential workforce call out, however surveillance coverage was sporadic and ineffective. Diplomatically Kamaria insisted they were conducting routine naval exercises. Based on recorded historical tracking data and the decision-preference profiles of the onboard commanders, Nulla-Nulla identified the three most likely locations for incursion of the AUS Area Of Responsibility (AOR) and Exclusive Economic Zone (EEZ).

Within hours AUVs were deployed to these locations, their placements along the boundary enabling persistent sensor monitoring for any approaching underwater or surface vessels. Reduced notice to move orders were issued, to be enacted if any Kamarian vessels veered off-course and crossed AUS trip-lines. Broad area infra-red satellite monitoring was tasked, with Nulla-Nulla programmed to trigger urgent warning to DIG analysts in the National Operations 24-hour Monitoring Centre of any anomalous detections for trip-line confirmation. A cyber team was also assembled to monitor and prepare to disrupt power to the anti-satellite site should any further preparations be detected from the location. Following several false positive returns, an urgent infra-red detection was received by Defence Intelligence analysts, with Nulla-Nulla identifying a 63% probability of a match to the vessels which had deployed from Port Preparatory. DIG analysts conducted a visual analysis, reviewed the details of the detection, and confirmed it met the trip-line threshold.

Upon receiving confirmation Nulla-Nulla commenced JOC contingency protocols, notifying Command Joint Operations (CJOPS) immediately of the confirmation, and standing by for approval to issue orders. CJOPS reviewed the notification, activated the contingency plan, approved and issued orders before commencing the return to work. This initiated the contingency response – Nulla-Nulla simultaneously issued updated orders to the respective service heads and commanders and contacted the members of the Crisis Response Team and the War Cabinet. Nulla-Nulla established and disseminated access to a Common Operating Picture for the response, informed by all streams of relevant data Nulla-Nulla had been utilising to this point and enabling interactive engagement. Nulla-Nulla also fed the updated information to the deployed AUVs enabling extended range monitoring at the assessed most likely location of incursion.

The contingency plan saw the (1) rapid deployment of UAVs to provide visual confirmation, monitoring and, if required, disruption of the surface vessels, (2) preparation of AUS Strike assets inclusive of supporting autonomous weapons system swarms, (3) rapid deployment of submarines and supporting AUVs to defend the Marine Hydrokinetic power generation plants, (4) preparation of autonomous missile defence and coastal defence cruise missile sites, (5) immediate recall of remainder of the cyber capability in anticipation of disruption requirements, and (6) re-tasking of satellites for infra-red and change detection warnings at Woody Island and Kamarian bomber and long-range missile sites. Enabled by Nulla-Nulla and an integrated AUS national security system, this was achieved within 15 minutes of receiving
the initial urgent infra-red detection. Joint AUV/UAV patrols using a combination of on-board AI and centralised Nulla-Nulla control, maintained active surveillance of Kamarian assets, however AUVs were receiving active signal interruption with a 75% certainty of jamming, providing the information to the AUS COP and DIG signals, prior to losing contact.

A notification from the UAV was received in the COP, with cross-referenced object detection confirming that it had observed the Kamarian vessels approaching. The War Cabinet requested a warning be issued for the vessels to redirect. CJOPS instructed Nulla-Nulla to issue the warning message via the UAV. The UAV was tasked to maintain observation and provided immediate notification of incursion into AUS EEZ to the CRT and War Cabinet. Connection was re-established with the forward deployed AUVs and the video feed confirmed at least two Kamarian submarines had been deployed to the area, based on speed and time from location Nulla-Nulla estimated underwater incursion of AUS EEZ from this secondary approach in one hour. The CRT instructed Nulla-Nulla to re-task the AUVs to detect and track the submarines from a distance that would not disrupt connectivity, feeding their location immediately into the COP. Less than two hours after the AUS fighters were deployed notification was received of satellite change detection at Woody Island, imagery revealing that Kamaria had commenced preparations to deploy their long-range fighters. UAV footage confirmed the Kamarian surface vessel formation had crossed into the AUS EEZ.

**Recommendations and Linkages**

- Facing threats beyond traditional kinetic strike in a complex threat environment, detection needs to be considered a critical component of strategic strike capabilities.
- Reduced warning of escalation in an increasingly volatile environment makes early detection critical in providing context and strategic warning to decision-makers.
- Early detection is best achieved through a cohesive, multi-disciplinary approach.
- Detection and timely decision-making enabled by an integrated operating system would overcome information access/sharing delays and facilitate efficient systems of cross-cuing of collection across sensors and platforms.
- New technologies can act as a force multiplier, mitigating challenges of detection across the expansive geography Australia is responsible for defending.
- Engaged integration of detection and decision-making processes supported by AI-augmented sensor integration can enable rapid tipping and cuing of sensors, early warning, rapid decision-making and dissemination of updates or orders.

**DECIDE**

The tools and products used during military planning prior to the proliferation of AI would see radical transformation in the face of deep learning and quantum computing. This was reflected in the roles of the Staff Officers embedded to JIATF 001 Joint Fires and Effects Cell in the conflict with Kamaria in 2042.

In understanding the conflict with Kamaria and the ADF’s success it is essential to understand not just the effectiveness of Deep Strike assets and the detection systems used, but also the processes that led to expediting the targeting of Kamarian high-value targets and support regional actors provided in enabling this to occur. Therefore, this short reflection summarises how AI enabled kinetic effects on Kamarian forces and highly conducive policy work with Non-Aligned nations within the region during the inter-war period. It will be argued that AI, specifically the CSIRO built Nulla-Nulla construct, enabled superior decision-making for both lethal and non-lethal outcomes.
Nulla-Nulla’s predictive modelling allowed for traditional Military Appreciation Process\textsuperscript{xxii} products such as the Enemy Situation Template,\textsuperscript{xxiii} Attack Guidance Matrix\textsuperscript{xxiv} and Intelligence, Surveillance and Reconnaissance plans\textsuperscript{xxv} to be developed with such effectiveness that the co-ordination of Strike effects were without historical precedent. The use of AI reduced the errors associated with the subjective analysis of the JIATF – JFECC Staff Officers and the speed at which it derived options would unhinge the larger Kamarian Vanguard as well as the Kamarian Government. Nulla-Nulla incorporated large amounts of data built over the preceding inter-war period, with substantial information on weapon effects obtained freely from Military Industry. This enabled optimised Strike effects on targets and a highly accurate predictive model of Kamarian movements. When this was overlaid with the confirmatory intelligence derived from the ADF’s complement of sensors it meant two things in the opening stages of the conflict.

Firstly, that the Kamarian public rhetoric could be disproven with relative ease noting the abundance of sensors and, secondly, that Nulla-Nulla provided targeting options for the JIATF almost instantaneously. The speed at which this was done even surprised the most ardent staff officer in the TF, particularly noting many were veterans of recent low intensity regional conflicts. Though intended for deterrence, the AI-enabled ability to take a first Strike approach ultimately set the conditions for victory. Nulla-Nulla enabled a smaller comparative force to qualitatively Observe, Orientate, Decide and Assess within a faster cycle than the Kamarians.

It is worth noting how Nulla-Nulla also predicted the behaviours of both the Kamarian Government, its military and citizens, and that of other Non-Aligned and supportive actors within the Indo-Pacific. Often captured within an Intelligence Officers subjective assessment of the dimensions of PMESII\textsuperscript{xxvi}, understanding what other regional stakeholders were likely to do was done almost instantaneously and far more comprehensively than a traditional Intelligence Cell ever could. Nulla-Nulla automatically interrogated open source information available on Twitter, Facebook, Instagram, Weibo and LINKEDIN as well as official government statements. When it compared this data to the histories of both principal decision makers and the history of each nation it allowed for an understanding of the regional responses to ADF military action. In turn this allowed a level of Australian Governmental risk understanding to occur if the response was negative or allow exploitation if the response was positive. The work of many dozens of Intelligence Analysts driven and shaped by an experienced Intelligence Officer was now truly accurate and automated.

The use of Nulla-Nulla had confirmed the hypothesis that many of the Non-Aligned nations were fearful of taking sides in a conflict, in part due to their strong economic ties with Kamaria but were equally concerned about a uni-polar environment within the Indo-Pacific. Nulla-Nulla had determined that many nations would remain independent until such time as a victor could be determined, thus elevating the importance of an initial decisive victory. It remains unclear whether it was completely the AI or the staff at the JFECC, but a consensus was generated that if the ADF were to use its arsenal of land, air, sea, and cyber based Strike options\textsuperscript{xxvii}, it needed to do so quickly and decisively.

This segues to the use of AI during the inter-war period. Specifically, how its ability to discern public opinion within the Indo-Pacific, guided political rhetoric for the Australian Government (AUSGOV). Nulla-Nulla had provided recommendations on talking points during key Indo-Pacific forums, such as APEC and ASEAN, ultimately creating favourable security agreements with India and Indonesia and enabling an effective Information Operations campaign across the region, promoting AUSGOV trade and agenda items. So successful were these discussions that the Five Powers Defence Agreement was ratified to the Seven Powers Defence and Peace Agreement in 2030. Of principal note was the sharing of mensurated\textsuperscript{xxviii} data obtained from
the various sensors of each nation. As access was granted to Nulla-Nulla, this meant the AI was able to incorporate every feed in the region to generate near perfect real time understanding of what was happening. Multi-national co-operation was free from the friction of interpersonal interactions underscored by cultural and political differences. The process was algorithmic, it was science rather than art.

AI was essential to the victory against the Kamarians. The ability to fuse nationally-sourced data and allied data allowed the JIATF to Decide which targets to Strike quickly. Just as importantly, AI assessments guided policy discussions during the inter-war period allowing a comprehensive understanding of second and third order effects of said kinetic activities. While the investments in long-range Strike assets made post-COVID-19 would cause the destruction of Kamaria's military force, the AI enabled a small but capable military to out-think a larger force.

### Recommendations and Linkages
- Detection and decision are intimately linked, with ISR providing necessary information, and AI enabling higher fidelity assumption-based planning
- Defence is a part of the whole of government decision-making cycle
- Artificial intelligence will aid in the decision-making cycle by improving fidelity and speed of decision-making
- Artificial intelligence will not be a ‘win button’ due to the enduring nature of war; friction, uncertainty and chance.

### DELIVER

### Long Range Strike Background

Nulla-Nulla-enabled ISR assets layered with an interconnected all-round defence of meshed underwater Hypersonic Scramjet missiles\(^{\text{xxix}}\) formed the backbone of Australia's deterrent standoff long-range strike capability. Miniaturised hypersonic missile pods (12 missiles) (annex 1) are small and manoeuvrable and have replaced previous land-based rocket systems such as HIMARS. This makes them difficult to track and are now the long-range weapon of choice for most nations, both on land and at sea.\(^{\text{xxx}}\) The hypersonic revolution has resulted in the demise of aerial platforms as airborne assets are now easily trackable and interceptable due to predictable flight paths and relative slow speeds (less than Mach 5), making them susceptible to targeting by hypersonic platforms worldwide. Nations no longer rely upon air superiority, which dominated the 20th century, as relatively inexpensive hypersonic missile technologies dominate any traditional aircraft capabilities. Space borne weapon systems and directional Electro Magnetic Pulse (EMP)\(^{\text{xxxi}}\) ensure that specific aircraft can be shot down moments after take-off almost anywhere in the world from any middle or major power. Evolution has resulted in the obsolescence of aircraft as main strike weapons, favouring unidentifiable underwater systems and eye in sky space weapon systems.

### Context

The threshold for engagement of the Kamarian advance guard was discussed and the Australian War Cabinet made a strategic decision to conduct ‘Long-Range Strike on Kamarian expeditionary force in order to abandon their territorial expansion into the Australian EEZ at a scale that would not result in war.’ The premise was that a pre-emptive engagement in a conflict short of triggering war, would assert Australia’s sovereign claims, and demonstrate globally that Australia would not be coerced out of its legally owned resources.
JIATF's challenge was striking sufficiently to force Kamarians to desist their operations without triggering an escalation that would result in mainland attacks on Australian territory. The options developed, were integrated to predict any retaliation and counter any hostile responses. The Kamarian expeditionary force (KMS1 and KMS2) consisting of six frigate-destroyer class vessels and their supporting autonomous vessels was identified as the primary target. AI calculated that rendering two vessels combat ineffective would achieve the end state of denying options of continuing their expeditionary pursuit but not inflict so much destruction of the formation that the Kamarians would be forced to escalate. The expeditionary advance force could affect the rescue of their own personnel and return to Kamarian waters without extreme political embarrassment. This engagement would be conducted by integrated D3A process focusing on long-range strike assets.

Nulla-Nulla generated attack options based on the set parameters including lethality, redundancy, attribution, likelihood of retaliation and geography. The basis for making the decision like any previous Military Appreciation Process was based on Feasibility, Acceptability, Sustainability. The AI ran thousands of options instantly with integrated access into the logistics and combat systems. This increase in the tempo of operations driven by AI running options based on percentage of success enabled a rapid targeting cycle and a prediction of second and third order effects. These predictions allowed for narratives to be developed and weaponised in response post-kinetic engagement.

**Convergence Window**

It was vital to establish a kinetic and non-kinetic convergence window in time and space for the engagement sequence to enable the delivery of effects with minimum disruption for an attack to be successful. Commencing in the 2020s, the increase in disruption technology throughout the entire electromagnetic spectrum, coupled with highly potent strike weapon systems mean unsynchronised and indiscriminate systems are easily countered. Therefore, unlike in the early part of the 20th Century, Strike is no longer a single shot capability but rather necessitates layering of multiple assets and concurrent execution to enable a ‘converge window’ for one or more of these effects to succeed. Counter-measures to long-range strike are readily available and require strike redundancy in the magnitude of 4 to 1 to have a reasonable chance of success. Therefore, Australia required a multi-layered response spanning the electromagnetic spectrum and including deception to maximise the anticipated success percentage, with four times the Kinetic ordnance delivered to achieve the destruction of two Surface vessels to achieve mission success.

**Cyber space**

Offensive and defensive cyber was layered throughout the engagement sequence to enable the kinetic strike and control the post-strike narrative. Integrated space disruption of communications at the time of the strike was paramount. Australia had the means available to destroy Kamarian dual use space capabilities through land based hypersonics however Nulla-Nulla predicted 91% of magnified retaliation by Kamaria (due to the dual use civil nature of Kamarian satellites) if this option was selected, which is outside the acceptable AUSGOV risk threshold.

Nulla-Nulla advised the best option was to disrupt Kamarian integrated space communications through geographic EMP which could be focused at specific layers of the atmosphere to disrupt strategic downlinks from space and radar from the surface fleet. This temporary disruption (over destruction) was cheaper and reduced the expected severity of retaliation down by 72%. This disruption was targeted at two specific links rather than the forces
themselves. The first link was between the Kamarian expeditionary force and their external communications reducing their ability to coordinate with higher headquarters. The second link was navigational between mainland Australia and mainland Kamaria to remove accuracy and time synchronization between potential mainland coordinated strategic responses which could then be countered (shot down) in a more piecemeal fashion. This disruption was to be layered over the top of kinetic targeting from H-5 minutes through to H+24 hours from a mixture of space based and ground based EMP options.

The offensive cyber layer was controlling the narrative post-strike. This involved disrupting the links between Kamarian and mainland news networks and an insertion of the Australian narrative of 'conducting legitimate defence of legally recognised sovereign waters by painting the picture of a Kamarian invasion.' This disruption window would allow offensive information campaigns to be executed while controlling the strategic narrative, highlighting that Australia's sovereignty was being threatened and by law Australia needed to respond.

Layered Strike options

Once Nulla-Nulla had confirmed the effectiveness of the EMP disruption, the conditions for kinetic strike within the D3A process could proceed. Layered long-range strike from multiple platforms were readied. This included manoeuvring Australia’s main strike asset of integrated mesh of kinetic hypersonic Underwater Autonomous Weapon Systems (UAWS). Australia largely replaced their manned submarine fleet in 2040 with UAWS as the vulnerability and redundancy in technology and capability made UAWS a more cost effective capable and continuous threat. The UAWS fleet are fully integrated in Australia’s AI defence and are distinguished by their ability to, once activated, select and engage targets without further intervention by a human operator. Nulla-Nulla calculates the data it is receiving from satellites, meteorological conditions, secondary underwater sensors and sends encrypted initiation sequences to selected platforms. This communication link has multiple levels of redundancy such as, satellite, sonar, HF seismographic.

Once activated the UAWS rises from an underwater seafloor ambush location and can manoeuvre underwater undetected to an optimum firing position normally within 300km radius of their original ambush position. UAWS has multiple kinetic options including hypersonic missiles effective range (10000km), directional EMP (3000km) and Direct Energy Weapon (DEW) focused on LOS anti-aircraft and self-protection. The UAWS system is tasked with a set of human-approved operational parameters, within which it may seek out and attack targets as its AI sees fit, with no need for direct supervision at any point between the generation of the mission data and the system’s return to base (or, in the case on an expendable munition, its own destruction upon execution of an attack). Indeed this level of autonomous trust is seen culturally as a natural extension of mission command.

Engagement sequence

The kinetic engagement sequence lasted 34 minutes from JIATF authority to strike, Nulla-Nulla execution programming, movement of UAWS systems, to striking surface vessels. Two UAWS platforms provided the primary hypersonic salvos. Layered secondary strike options of land-based hypersonics from Australia's West coast including small concealed highly deployable hypersonics were ready and online but were not required due to integral BDA achieved through AI. These secondary hypersonic options also acted as potential interceptors from any Kamarian based kinetic counterattack or defensive measures directed at Australian mainland.
Post-engagement from two separate UAWS platforms in the Southern Ocean each firing four hypersonic salvos synchronized in time and with defensive and offensive cyber directed at two command vessels, they achieved decisive effects. Aimed at the stern of the ship, to minimise casualties but maximize ship damage, reduced the expected retaliation percentage by 31%. Five salvos appear to have been intercepted from unknown onboard self-defence capabilities, likely hypersonic interceptors, reinforcing the 4 to 1 overmatch required for successful kinetic strike. The UAWS systems engaged post-engagement sequences, sinking back into the depths of the Indian Ocean and Southern Ocean and reposition remaining poised to receive and execute future missions.

The kinetic strike was executed relatively easily, however, controlling the post-strike narrative was the centre of gravity which involved the most strategic risk and could be easily weaponised through disinformation and a counter-narrative painting Australia as an unprovoked aggressor. Controlling the non-kinetic targeting took days to setup and weeks to counter the disinformation claims post-strike.

Recommendations and Linkages
- Engagement is a single component of the ‘strike system’ and is unachievable without the Detect phase, and is unlikely to nest operational outcomes within strategic objectives without an effective Decide phase.
- Defence needs to invest in multiple redundancy ‘engage’ systems, kinetic and non-kinetic, to increase survivability and options for decision-makers.

ASSESS

Australia's Kinetic and non-kinetic strike in defence of its territory was a resounding success. Nulla-Nulla automatically fused BDA data from satellite tracking, UAWS weapons data, and adversary communications providing real-time updates to the JIATF TOC. Two enemy vessels were disabled, demonstrating Australia's resolve, forcing Kamaria to withdraw its forces to its own territory.

Throughout, Australian Government messaging, enabled by Nulla-Nulla and the reduction in Kamarian capability owing to the EMP Strike, allowed AUSGOV to control the strategic narrative. Australian Detect and Strike capabilities were once again able to return to their principal role of deterrence.

Recommendations and Linkages
- Assessment is intimately linked to efficacy of engagement, and relies on the detect phase for confirmation and speed of decision-making in the decide phase to complete further required action nested to operational and strategic objectives.

CONCLUSION

This paper has argued that long range strategic strike is a holistic system that encompasses the entire D3A, and has examined how advanced technologies will increase Australia’s credibility in the face of increasingly sophisticated A2AD capabilities, achieving modern deterrence. This paper has discussed future technology in the context of a future threat scenario, demonstrating the technologies involved in deterrence and long-range strike as part of an effective system. It outlined the general background. It then went through the specifics of the targeting cycle, progressing though Detect, Decide, Deliver, and Assess. During the cycle it demonstrated the
linkages between the various components of the D3A cycle and the key future technologies required to enable it.

Strategic long-range strike and deterrence must evolve with the changing nature of Australia’s adversaries. Modern and future A2AD systems provide Australia’s adversaries with a technological advantage. Australia is well postured to adopt a modern whole of government strike system to further enhance the ADF’s ability to protect Australia and its national interest.

This paper was completed by Ray Brin, Theresa Cunningham, Christina Dubej, Simon Frewin, and Michael Smith. Ray and Simon have extensive experience in the RAA and Michael in the RAE within training, operations and staff appointments. Christina has diverse GEOINT experience across national security and joint defence environments. Theresa has extensive service in the RAN with a focus on Training and Capability.
BIBLIOGRAPHY


Top Strike System Technologies

<table>
<thead>
<tr>
<th>Technology</th>
<th>Capability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Space-based ISR: Large area monitoring</td>
<td>“Observing surface water is essential for ecological and hydrological studies. This paper reviews the current status of detecting, extracting, and monitoring surface water using optical remote sensing ... It was found that pixel unmixing and reconstruction, and spatio-temporal fusion are two common and low-cost approaches to enhance surface water monitoring. Remote sensing data have been integrated with in situ river flow to model spatio-temporal dynamics of surface water. Recent studies have also proved that the river discharge can be estimated using only optical remote sensing imagery. This will be a breakthrough for hydrological studies in ungauged areas. Optical sensors are also easily obscured by clouds and vegetation. This limitation can be reduced by integrating optical data with synthetic aperture radar data and digital elevation model data ... Enhanced global or regional water monitoring in the future requires integrated use of multiple sources of remote sensing data.” [Ref: Huang et al., &quot;Detecting, extracting, and monitoring surface water from space using optical sensors: A review,&quot; p.333. Huang, Chen, Zhang, and Wu, 'Detecting, extracting, and monitoring surface water from space using optical sensors: A review,' p.333]</td>
</tr>
<tr>
<td>Space-based ISR: Infra-red capability</td>
<td>“Since the late 1990s, remotely sensed night-time lights (NTL) satellite imagery has been shown to correlate with socioeconomic parameters including urbanization, economic activity, and population. More recent research demonstrates that multitemporal NTL data can serve as a reliable proxy for change over time in these variables whether they are increasing or decreasing.” [Ref: Bennett and Smith, &quot;Advances in using multitemporal night-time lights satellite imagery to detect, estimate, and monitor socioeconomic dynamics,&quot; p.176. Bennett and Smith, 'Advances in using multitemporal night-time lights satellite imagery to detect, estimate, and monitor socioeconomic dynamics,' p.176]</td>
</tr>
</tbody>
</table>

“In October 2011, the launch of NASA/NOAA's Suomi National Polar-orbiting Partnership satellite, whose Visible Infrared Imaging Radiometer Suite (VIIRS) sensor has a Day/Night Band (DNB) specifically designed for capturing radiance from the Earth at night, marked the start of a new era in NTL data collection and applications.” [Ref: Bennett and Smith, "Advances in using multitemporal night-time lights satellite imagery to detect, estimate, and monitor socioeconomic dynamics," p.176. Bennett and Smith, 'Advances in using multitemporal night-time lights satellite imagery to detect, estimate, and monitor socioeconomic dynamics,' p.176]

“Finally, future directions for NTL research are suggested, particularly in the areas of determining the fundamental causes of observed light and in leveraging VIIRS' superior sensitivity and spatial and radiometric resolution.” [Ref: Bennett and Smith, "Advances in using multitemporal night-time lights satellite imagery to detect, estimate, and monitor socioeconomic dynamics," p.176]
**Space-based ISR: Automated item or change detection**

“The data from remote sensing satellites provide opportunities to acquire information about land at varying resolutions and has been widely used for change detection studies. A large number of change detection methodologies and techniques, utilizing remotely sensed data, have been developed, and newer techniques are still emerging … The importance of the exponential increase in the image data volume and multiple sensors and associated challenges on the development of change detection techniques are highlighted. With the wide use of very-high-resolution (VHR) remotely sensed images, object-based methods and data mining techniques may have more potential in change detection.” [Ref: Hussain et al., "Change detection from remotely sensed images: From pixel-based to object-based approaches," p.91. Hussain, Chen, Cheng, Wei, and Stanley, 'Change detection from remotely sensed images: From pixel-based to object-based approaches,' p.91]

“In this paper, we propose a context-sensitive technique for unsupervised change detection in multitemporal remote sensing images. The technique is based on fuzzy clustering approach … Since the ranges of pixel values of the difference image belonging to the two clusters (changed and unchanged) generally have overlap, fuzzy clustering techniques seem to be an appropriate and realistic choice to identify them (as we already know from pattern recognition literatures that fuzzy set can handle this type of situation very well) … Results are compared with those of existing Markov random field (MRF) and neural network based algorithms and found to be superior. The proposed technique is less time consuming and unlike MRF does not require any a prior knowledge of distributions of changed and unchanged pixels.” [Ref: Ghosh, Mishra, and Ghosh, "Fuzzy clustering algorithms for unsupervised change detection in remote sensing images," p.699. Ghosh, Mishra, and Ghosh, 'Fuzzy clustering algorithms for unsupervised change detection in remote sensing images,' p.699]

“A new algorithm for Continuous Change Detection and Classification (CCDC) of land cover using all available Landsat data is developed. It is capable of detecting many kinds of land cover change continuously as new images are collected and providing land cover maps for any given time. … The land cover map with 16 categories resulting from the CCDC algorithm had an overall accuracy of 90%.” [Ref: Zhu and E.Woodcock, "Continuous change detection and classification of land cover using all available Landsat data," p.152. Zhu and E.Woodcock, 'Continuous change detection and classification of land cover using all available Landsat data,' p.152]

**Laser**

“Still, that kind of directed energy can be very useful on the battlefield. Enough heat can detonate explosive payloads on rockets and ignite chemical fuels in drones or small boats, popping off lethal payloads in the air and shooting down drones. Battlefield lasers can keep on shooting as long as troops have diesel to run the generators.” [Ref: Hecht, "A “Star Wars” Sequel? The Allure of Directed Energy for Space Weapons,” p.167. Hecht, 'A “Star Wars” Sequel? The Allure of Directed Energy for Space Weapons,' p.167]

“Yet lasers might serve an important military purpose in space, doing something they already do very successfully in ground-based factories: cutting metals and other materials. NASA and DARPA have been trying to develop robotic repair spacecraft for many years. Ostensibly, the goal is to repair malfunctioning satellites like space shuttle astronauts repaired the Hubble Space Telescope. Approach the satellite slowly, dock with it, fix the problem, and fly off to the next repair mission.” [Ref: Hecht, "A “Star Wars” Sequel? The Allure of Directed Energy for Space Weapons,” p.168. Hecht, 'A “Star Wars” Sequel? The Allure of Directed Energy for Space Weapons,' p.168]

“AI systems will allow autonomous decision-making by networked computer agents, enabling extremely rapid sequential action, even in uncertain operating environments.” [Ref: Payne, "Artificial Intelligence: A Revolution in Strategic Affairs?,” p.9. Payne, 'Artificial Intelligence: A Revolution in Strategic Affairs?,' p.9]

“autonomous and intelligent platforms will be able to manoeuvre faster and employ force with more precision than those operated by humans. Already, an AI system can outperform an experienced military pilot in simulated air-to-air combat.6 Autonomy and networking, along with other technologies, including nano, stealth and bio, will offer sophisticated tactical war-fighting capabilities on land and sea, and in the air.” [Ref: Payne, "Artificial Intelligence: A Revolution in Strategic Affairs?,” p.9. Payne, 'Artificial Intelligence: A Revolution in Strategic Affairs?,' p.9]

“Strategic-level AI operating as an ‘oracle’ for decision-makers will be able to test accepted wisdom, discarding spurious associations, rejecting...

“a third-party actor might attempt to use AI-driven adversarial inputs, data-poisoning attacks, and audio and video manipulation to create escalatory effects between nations. While other early-warning systems would eventually discredit the spoof, it would still create high levels of uncertainty and tension in a short period of time. … Collecting and processing the intelligence would take precious time during an escalatory crisis in which AI algorithms were urging immediate response actions.” [Ref: Mark Fitzpatrick, "Artificial Intelligence and Nuclear Command and Control," Survival 61, no. 3 (2019): p.83, https://doi.org/10.1080/00396338.2019.1614782. Mark Fitzpatrick, 'Artificial Intelligence and Nuclear Command and Control,' Survival 61, no. 3 (2019): p.83]

“Deep fakes by third parties can be magnified by AI capabilities that fall into the wrong hands and are used to generate false positives.” [Ref: Fitzpatrick, "Artificial Intelligence and Nuclear Command and Control," p.84. Fitzpatrick, 'Artificial Intelligence and Nuclear Command and Control,' p.84]

“Once the operation of AI systems is triggered, humans are unable to monitor the systems’ decision calculus in real time.” [Ref: Fitzpatrick, "Artificial Intelligence and Nuclear Command and Control," p.85. Fitzpatrick, 'Artificial Intelligence and Nuclear Command and Control,' p.85]

“The background papers for the exercise had noted how data poisoning attacks introducing skewed inputs into the training dataset for an AI machine-learning process can distort an AI system’s output by degrading its ability to distinguish between good data and bad data.” [Ref: Fitzpatrick, "Artificial Intelligence and Nuclear Command and Control," p.85. Fitzpatrick, 'Artificial Intelligence and Nuclear Command and Control,' p.85]

“while disinformation is a long-standing intelligence and strategic problem that pre-dates the cyber age, the integrity of AI systems is especially vulnerable to it. The combination of reliance on AI and its appropriation by malevolent actors could seriously amplify the disruptive effects of disinformation campaigns.” [Ref: Fitzpatrick, "Artificial Intelligence and Nuclear Command and Control," p.91. Fitzpatrick, 'Artificial Intelligence and Nuclear Command and Control,' p.91]

“The key forces driving this evolution include: (1) the exponential growth in computing; performance; (2) expanded datasets;4 (3) advances in the implementation of machine learning techniques and algorithms (especially in the field of deep neural networks); and above all, (4) the rapid expansion of commercial interest and investment in AI” [Ref: Johnson, "Artificial intelligence & future warfare: implications for
This article argues that military-use AI is fast becoming a major potential source of instability and great power strategic competition. Towards this end, the paper makes three inter-related central arguments: (1) At its current development stage, AI in isolation has few genuinely strategic effects; rather it is a potential power force multiplier and enabler for several high-tech domains – including cyberspace, autonomy and robotics, and guided missiles; (2) the uncertainties and risks surrounding the proliferation and diffusion of dual-use AI technology could worsen international security in several ways: exacerbate existing threats, transform the nature and characteristics of these threats, and introduce new (and potentially accidental prone and unsafe) threats to the security landscape; and (3) the concomitant pursuit of AI technology by great and rising powers (especially the U.S. and China) will create additional incentives for strategic competition and distrust, which has potentially profound implications for international security.” [Ref: Johnson, "Artificial intelligence & future warfare: implications for international security," p.148]

<table>
<thead>
<tr>
<th>AI Cyberattacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;The most dangerous feature of an AI cyberattack is that it may target civilian infrastructure as well as military targets.” [Ref: Sharikov, &quot;Artificial Intelligence, Cyberattack, and Nuclear Weapons — A Dangerous Combination,&quot; p.371]</td>
</tr>
<tr>
<td>&quot;It is easier for potential attackers to find these vulnerabilities, and harder for the government to guarantee security. Artificial intelligence together with big data analysis may be used to figure out the most vulnerable infrastructure, or choose the best timing to make an attack most catastrophic.” [Ref: Sharikov, &quot;Artificial Intelligence, Cyberattack, and Nuclear Weapons — A Dangerous Combination,&quot; p.371]</td>
</tr>
<tr>
<td>&quot;The whole process of ensuring cybersecurity is very dynamic. Unlike conventional and even nuclear weapons, cyberoffense is constantly changing, and hence the defense against it also must be constantly developing. A robust cyberdefense is the one that can adjust to the constantly changing environment.” [Ref: Sharikov, &quot;Artificial Intelligence, Cyberattack, and Nuclear Weapons — A Dangerous Combination,&quot; p.371]</td>
</tr>
<tr>
<td>&quot;cyberthreats as well as cybervulnerabilities are asymmetrical, which means that no parity can be reached.” [Ref: Sharikov, &quot;Artificial Intelligence, Cyberattack, and Nuclear Weapons — A Dangerous Combination,&quot; p.371]</td>
</tr>
</tbody>
</table>
“Several U.S. national security officials have posited that AI and machine learning will have a transformative influence on cyber domain, as force multipliers for both defensive and offensive cyber weapons. The line between AI-augmented cyber-offense and cyber defence will likely remain an obscure one, however. As a result, effective defence against attacks by sophisticated autonomous AI systems (such as a bot) will require increasingly innovative (and self-learning) solutions.” [Ref: Johnson, "Artificial intelligence & future warfare: implications for international security," p.154. Johnson, 'Artificial intelligence & future warfare: implications for international security,' p.154]

**Ineffective as a deterrent:** “if a cyberweapon is actually demonstrated, then the enemy may create a remedy and the offender would lose superiority. Hence, the idea of cyberdeterrence is nearly unfeasible, as RAND corporation expert Martin Libicki noted in 2009.” [Ref: Sharikov, "Artificial Intelligence, Cyberattack, and Nuclear Weapons — A Dangerous Combination," p.371. Sharikov, 'Artificial Intelligence, Cyberattack, and Nuclear Weapons — A Dangerous Combination,' p.371]

### Robotics
Isaac Asimov’s Three Laws of Robotics:
“A robot may not injure a human being or, through inaction, allow a human being to come to harm. A robot must obey orders given it by human beings except where such orders would conflict with the First Law. A robot must protect its own existence as long as such protection does not conflict with the First or Second Law.” [Ref: Sharikov, "Artificial Intelligence, Cyberattack, and Nuclear Weapons — A Dangerous Combination," p.372. Sharikov, 'Artificial Intelligence, Cyberattack, and Nuclear Weapons — A Dangerous Combination,' p.372]

### UAVs/ UAWs
“In the maritime domain, UUVs, USVs and UAVs – supported by AI-enabled intra-swarm communication and ISR systems – could be deployed simultaneously in both offensive and defensive ASW operations to saturate an enemy’s defences and locate, disable and destroy its nuclear-armed or non-nuclear attack submarines.” [Ref: Johnson, "Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare," p.9. Johnson, 'Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare,' p.9]

(as noted above in AWS) “Eschewing these risks, China and Russia plan to incorporate AI into UAVs and unmanned underwater vehicles (UUVs) for swarming missions infused with AI machine-learning technology. Chinese strategists have reportedly researched data-link technologies for ‘bee-swarm’ UAVs, emphasising network architecture, navigation and anti-jamming military operations, in particular, to target US aircraft carriers.” [Ref: Johnson, "Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare," p.5. Johnson, 'Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare,' p.5]

(as noted above in AWS) “Recent advances in sensor, communication and processing technologies (especially big-data analytics and machine learning) could become disruptive, transformative technologies in future ASW and undersea support platforms (for example, UUVs, unmanned
Autonomous Weapons Systems

“The real innovation behind contemporary drone warfare is the construction of high-capacity data links that allow the drone to stay in contact with its human ‘pilot’. This communication network, not to mention the drone itself, is fragile; it is unlikely that the system could function in a non-permissive environment featuring modern air-defenses, electronic jamming, or cyber warfare. The systems also require intelligence ‘queuing’.” [Ref: Johnson et al., "An INS Special Forum: Intelligence and Drones/Eyes in the Sky for Peacekeeping: The Emergence of UAVs in UN Operations/The Democratic Deficit on Drones/The German Approach to Drone Warfare/Pursuing Peace: The Strategic Limits of Drone Warfare/Seeing but Unseen: Intelligence Drones in Israel/Drone Paramilitary Operations Against Suspected Global Terrorists: US and Australian Perspectives/The ‘Terminator Conundrum’ and the Future of Drone Warfare," pp.433-34.Johnson, Dorn, Webb, Kreps, Krieger, Schwarz, Shpiro, Walsh, and Wirtz, 'An INS Special Forum: Intelligence and Drones/Eyes in the Sky for Peacekeeping: The Emergence of UAVs in UN Operations/The Democratic Deficit on Drones/The German Approach to Drone Warfare/Pursuing Peace: The Strategic Limits of Drone Warfare/Seeing but Unseen: Intelligence Drones in Israel/Drone Paramilitary Operations Against Suspected Global Terrorists: US and Australian Perspectives/The ‘Terminator Conundrum’ and the Future of Drone Warfare,' pp.433-434]  

“Field experimentation also has revealed that the performance of fully autonomous drones will probably exceed the performance of their human-piloted counterparts in counter-terror missions: today’s autonomous drones equipped with narrow AI seem to do at least as well as humans in discriminating between threats and harmless civilians.” [Ref: Johnson et al., "An INS Special Forum: Intelligence and Drones/Eyes in the Sky for Peacekeeping: The Emergence of UAVs in UN Operations/The Democratic Deficit on Drones/The German Approach to Drone Warfare/Pursuing Peace: The Strategic Limits of Drone Warfare/Seeing but Unseen: Intelligence Drones in Israel/Drone Paramilitary Operations Against Suspected Global Terrorists: US and Australian Perspectives/The ‘Terminator Conundrum’ and the Future of Drone Warfare," p.434.]

“Autonomy offers benefits. Swarms of low-priced, autonomous drones can operate in a hostile environment, because they can be collectively programmed to undertake all types of emergent behavior (search, swarm to attack, relay information, spook surveillance systems) and to select what type of behavior is most appropriate without human intervention, thereby eliminating the need to communicate with human operators. In other words, drones might fulfill their military potential by actually operating as an autonomous collective.” [Ref: Johnson et al., "An INS Special Forum: Intelligence and Drones/Eyes in the Sky for Peacekeeping: The Emergence of UAVs in UN Operations/The Democratic Deficit on Drones/The German Approach to Drone Warfare/Pursuing Peace: The Strategic Limits of Drone Warfare/Seeing but Unseen: Intelligence Drones in Israel/Drone Paramilitary Operations Against Suspected Global Terrorists: US and Australian Perspectives/The ‘Terminator Conundrum’ and the Future of Drone Warfare," p.434.]

“a new generation of artificial intelligence (AI)-augmented and -enabled autonomous weapon systems (AWS), most notably drones used in swarming tactics, could have a significant impact on deterrence, nuclear security, escalation and strategic stability in future warfare.” [Ref: Johnson, "Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare," p.1.]

“new Iterations of AI-augmented advanced conventional capabilities (such as cyber weapons, precision munitions and hypersonic weapons) will compound the risk of military escalation, especially inadvertent and accidental escalation.” [Ref: Johnson, "Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare," p.2.]

“Conceptually speaking, autonomous systems will incorporate AI technologies such as visual perception, speech, facial recognition and decision-making tools to execute a range of core air interdiction, amphibious ground assaults, long range strike and maritime operations independent of human intervention and supervision.” [Ref: Johnson, "Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare," p.3.]

“Loitering attack munitions (LAMs)… pursue targets (such as enemy radar, ships or tanks) based on pre-programmed targeting criteria, and launch an attack when its sensors detect an enemy’s air-defence radar. … LAMs use AI technology to shoot down incoming projectiles faster than a human operator could, and can remain in flight (or loiter) for far longer periods than human-operated munitions.” [Ref: Johnson, "Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare," p.3.]

“Hundreds of AI machine learning autonomous drones in a swarming sortie may potentially evade and overwhelm an adversary’s sophisticated defence capabilities even in heavily defended regions such as China’s eastern and coastal regions. Moreover, stealth variants of these systems, along with miniaturised electromagnetic jammers and cyber-weapons, may be used to interfere with or subvert an adversary’s targeting sensors and communications systems, undermining its multi layered air defences in preparation for drone swarms and long-range stealth-bomber offensive attacks.” [Ref: Johnson, "Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare," p.3.]

“Manned F-35 fighters developed by the US will soon be able to leverage AI to control small drone swarms in close proximity to the aircraft performing sensing, reconnaissance and targeting functions, including countermeasures against swarm attacks.” [Ref: Johnson, "Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare," p.4.]

“Eschewing these risks, China and Russia plan to incorporate AI into UAVs and unmanned underwater vehicles (UUVs) for swarming missions infused with AI machine-learning technology. Chinese strategists have reportedly researched data-link technologies for ‘bee-swarm’ UAVs,

“Recent advances in sensor, communication and processing technologies (especially big-data analytics and machine learning) could become disruptive, transformative technologies in future ASW and undersea support platforms (for example, UUVs, unmanned surface vehicles (USVs) and UAVs) to locate and attack submarines in real time, and enhance the stealth and endurance of submarines and their attendant weapon systems.” [Ref: Johnson, "Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare," p.6. Johnson, ‘Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare,’ p.6]

“AI applications will likely enhance the delivery system targeting and tracking, and improve the survivability of drone swarms against the current generation of missile defences. For example, technological advances in hypersonic boost-glide weapons – especially deployed in conjunction with cruise missiles and missile-defence capabilities, and supported by drone swarms – could target an adversary’s high-value assets such as radars, anti-satellite weapons, mobile missile launchers, C3I systems and TELs used to undergird both nuclear and conventional missiles.” [Ref: Johnson, "Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare," p.8. Johnson, 'Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare,' p.8]

“the dependency of swarms on these systems (similar to cyber defences, discussed below) could make them more vulnerable to attack, for example, from spoofing, manipulation, digital jamming and electromagnetic pulses. To Reduce these vulnerabilities, sensor drone swarm formations could apply AI augmented ISR to bolster intelligence collection, intra-swarm communication and analysis, widening the geographical range of its operations and monitoring for potential threats to the swarm, thereby leaving the remainder of the swarm unfettered to perform its offensive activities.” [Ref: Johnson, "Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare," p.8. Johnson, ‘Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare,’ p.8]

“Drone swarms might be armed with cyber or electronic warfare (EW) capabilities (in addition to anti-ship, anti-radiation, or regular cruise and ballistic missiles) to interfere with or destroy an adversary’s early warning detection and C3I systems, in advance of a broader offensive campaign.” [Ref: Johnson, "Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare," p.8. Johnson, 'Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare,' p.8]

“advances in mobile sensing platforms could enable drone swarms to locate submarines through chokepoints (or gateways) as they emerge from
<table>
<thead>
<tr>
<th>Anti-satellite capabilities</th>
<th>“On 27 March 2019, the Indian Government destroyed one of its own satellites with a missile interceptor, reminding the world that States consider “counterspace capabilities” to be an essential part of a modern military and are actively developing such weapons.” [Ref: Porras, &quot;Anti-satellite Warfare and the Case for an Alternative Draft Treaty for Space Security,&quot; p.142. Porras, 'Anti-satellite Warfare and the Case for an Alternative Draft Treaty for Space Security,' p.142]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>“Some observers lamented the 400-plus pieces of debris that were generated, with several objects being tracked at altitudes of up to more than 1,000 kilometers, or about 621 miles. (To put this in perspective, the International Space Station orbits at an altitude of about 400 kilometers, or 249 miles.) Others, however, noted that the test was carried out at a relatively low altitude, and the debris should fall out of orbit in a short amount of time – a matter of weeks or months – posing a minimal risk to other objects or persons in Low Earth Orbit.” [Ref: Porras, &quot;Anti-satellite Warfare and the Case for an Alternative Draft Treaty for Space Security,&quot; p.142. Porras, 'Anti-satellite Warfare and the Case for an Alternative Draft Treaty for Space Security,' p.142]</td>
</tr>
<tr>
<td></td>
<td>“The technology to engage in electronic or cyber counterspace operations is much cheaper and more widely available, and its attributes make it much easier to plausibly deny its use. Some of this technology is already being used in the battlefield, such as in Syria and Ukraine. However, unlike destructive counterspace technology, there seems to be some tolerance for temporary, non-destructive capabilities. There is little-to-no outcry calling for the cessation of electronic warfare in space.” [Ref: Porras, &quot;Anti-satellite Warfare and the Case for an Alternative Draft Treaty for Space Security,&quot; pp.143-44. Porras, 'Anti-satellite Warfare and the Case for an Alternative Draft Treaty for Space Security,' pp.143-44]</td>
</tr>
<tr>
<td>Hypersonics</td>
<td>“Hypersonic flight occurs at velocities five times above the speed of sound (Mach 5 = 6,174km/hr), and current research into hypersonic propulsion is focusing on the Mach 5 to Mach 10 (12,348km/hr) realm based around supersonic combustion ramjets, or ‘scramjet’ engines.” [Ref: <a href="https://www.aspistrategist.org.au/to-mach-5-and-beyond-the-age-of-high-speed-warfare/">https://www.aspistrategist.org.au/to-mach-5-and-beyond-the-age-of-high-speed-warfare/</a>]</td>
</tr>
<tr>
<td></td>
<td>“hypersonic weapons reduce time of response for defenders to the point where a viable anti-ship missile defence with the traditional layered approaches becomes largely impossible. Instead, naval forces will need new and more responsive technologies like directed energy weapons, electromagnetic railguns or defensive hypersonic missile systems”. [Ref: <a href="https://www.aspistrategist.org.au/to-mach-5-and-beyond-the-age-of-high-speed-warfare/">https://www.aspistrategist.org.au/to-mach-5-and-beyond-the-age-of-high-speed-warfare/</a>]</td>
</tr>
</tbody>
</table>
Hypersonic weapons will depend on an effective and resilient ‘kill chain’ to function effectively. That means a state that invests in hypersonic weapons must also invest in advanced sensor systems that can detect and track a specific target, and have secure data links from the sensor to the decision-maker and then to the ‘shooter’. It’s not just about faster missiles—it’s about the technologies that come together to either use such weapons or defeat them. [Ref: https://www.aspistrategist.org.au/to-mach-5-and-beyond-the-age-of-high-speed-warfare/]

**EMP**

Australia's Defence Science and Technology Organisation (DSTO) has built an experimental reusable high-power radio frequency weapon with an impact zone of 20-30m (65-100ft) as part of ongoing research into electromagnetic-pulse armaments able to destroy electrical and electronic systems. [Ref: https://www.flightglobal.com/australia-reveals-electromagnetic-pulse-weapon/45504.article]
ENDNOTES


ii For this paper Long Range strike no longer means dropping ordnance on an enemy's homeland. The concept has evolved due to range being irrelevant, with the proliferation of space based and energy directed weapons. Long Range Strike now means having the ability to render an enemy capability redundant in the electromagnetic spectrum by creating a convergence window to execute desired kinetic and or non kinetic effects.

iii Strategic means "the use of engagements for the object of the war". Principally it will be used in the context of the employment of all aspects of national security against an adversary for the purpose of war.

iv Finally deterrence can be viewed in “two primary forms of deterrence are deterrence by denial and deterrence by punishment”. Simplistically, deterrence seeks to impose a high cost relative to the political benefit on an Adversary, with punishment seek to impose a higher transactional cost relative to any political gain.

v The Southern Ocean Regional Energy Production Zone encompasses all Marine Hydrokinetic power generation fields located between Australia, New Zealand and Antarctica states.

vi Whilst the ratification of the Antarctica treaty imposed increased Australian Southern Ocean protection commitment it enabled the research and development of Marine Hydrokinetic capability.


Teresa Umali, (Open Gov Asia, 2020). CSIRO released an AI roadmap in 2019, though it did not include a Defence component it is offered that this would mark a reasonable start point for Defence AI research and Development.

NULLA-NULLA – a wooden club used by indigenous Australians, a hypothetical name for an Australia AI construct.

The Military Appreciation Process is the ADF methodology for both understanding and generating a solution to a problem.

The Attack Guidance Matrix provides military planners an understanding of what weapon system can be used on a particular target for best effect.

The ISR Plan indicates where an adversary may be and allocates sensors to that location.

The Enemy Situation Template is a visualization of an adversary’s movement and likely and most dangerous predicted behaviors. This is based on the subjective analysis of the doctrinal norms of an adversary reflecting their assessed objectives, their capabilities and environmental factors.

PMESSII - Political, Military, Economic, Social, Information, Infrastructure – a tool typical used by the Intelligence community to focus an understanding of a nations capability.
The STRIKE options made mentioned include those such as long-range fires, cyber options and the provision of RAAF F-35. Australian Government: Department of Defence. *2020 Defence Strategic Update*. Canberra: Commonwealth of Australia, 2020.

**Mensuration** is the process of measurement of a feature or location on the earth to determine an absolute latitude, longitude, and elevation. Mensuration consists of geometric measurements from monoscopic and stereoscopic imagery, under a variety of acquisition conditions. National Geospatial-Intelligence Agency. *Mensuration*. 10 Jul. Accessed Jul 16, 20.

[https://www.nga.mil/ProductsServices/PrecisePositioningandTargeting/Pages/Mensuration.asp](https://www.nga.mil/ProductsServices/PrecisePositioningandTargeting/Pages/Mensuration.asp)

**Scramjets** use a rocket to attain high speeds, then an air-breathing engine to sustain the speed.


**Electro Magnetic Pulse** (EMP) and direct energy weapons will evolve into small mobile platforms that can be launched from a range of sea-based and land-based sites. *Vision of Future Warfare*


**Hypersonic** vehicles from 2040 (those exceeding Mach 5) are capable of global strike operations that could put any target on Earth or within earth's orbit within reach in less than an hour of decision and launch. They are effective at penetrating defences due to their ability to manoeuvre and change altitude at flat trajectory to avoid defences. O’Hanlon, Michael. "Forecasting change in military technology, 2020-2040." *Military Technology* 2020 (2018): 2040.


**Autonomous Weapon Systems and Strategic**

**Directed Energy Weapons**