

NOVEMBER 2024

IMPACT OF FUTURE TECHNOLOGIES ON DEFENCE AND DEFENCE INDUSTRY

PREPARED BY:

CAROLINE CHAI, IVAN LEE, THIBAUD GRIZARD, MATT STRUDWICK, BRÉE WILKIE

ACKNOWLEDGEMENTS

Through the course of the research, the authors engaged with representatives from the defence industry, government and non-government organisations through a series of interviews, discussions, and surveys to gain insight from lived experience, knowledge and perspectives. As such, the authors would like to acknowledge the contributions from the following organisations:

Agent Oriented Software Group
Aurizn
DAIRNet
Defence Science & Technology Group
Queensland University of Technology
Raytheon Australia Pty Ltd
SAAB Australia Pty Ltd
Saber Astronautics
SAGE Automation
Hensoldt AG
The University of South Australia
Those that wish to remain anonymous

DISCLOSURES & DISCLAIMERS

The contents of this research paper are the opinions and conclusions of the authors and do not necessarily represent the views of the author's organisations, the contributors, the contributors' organisations, the Defence Industry Leadership Program (DILP) or the Defence Teaming Centre (DTC).

EXECUTIVE SUMMARY



This paper investigates the impact of emerging technologies, particularly artificial intelligence (AI), on Australia's defence industry over the next ten to fifteen years. It examines the implications across the naval, land, air, space, and cyber domains, offering leaders foresight to navigate challenges, integrate new capabilities, and address ethical concerns.

Key findings highlight the transformative role of AI in advancing Defence capabilities while underscoring risks such as overreliance, loss of human oversight, and ethical dilemmas. Survey and interview participants identified the need for a unified Defence AI vision, prioritisation of workforce upskilling, and maintaining human judgement in decision-making to ensure responsible and effective adoption.

Three recommendations are proposed:

1. **Develop a Unified Defence AI Vision:** Establish a cohesive strategy to guide ethical frameworks, policies, and standards for AI in Defence.
2. **Develop and Train Future Leaders for AI Adoption:** Prioritise "Educate, Create, Connect" initiatives to build AI literacy and readiness across Defence and industry.
3. **Human Judgement Remains Indispensable in Defence Decision-Making:** Maintain human oversight in decision-making to mitigate risks and uphold ethical standards.

The paper emphasises the importance of collaboration between Defence, industry, and academia to address the rapid pace of technological advancements while aligning with global standards and Australia's strategic priorities. Failure to act now risks stagnation and diminished readiness to face future challenges.




TABLE OF CONTENTS

01

INTRODUCTION

PAGE 5

02BACKGROUND
& SCOPE

PAGE 6

03RESEARCH
METHODOLOGY

PAGE 10

04

RESEARCH FINDINGS

PAGE 13

05

RECOMMENDATIONS

PAGE 26

06

CONCLUSION

PAGE 49

07

ACRONYMS

PAGE 51

08

REFERENCES

PAGE 52

09

APPENDICES

PAGE 54

1 INTRODUCTION

The goal of our project was to collaboratively investigate and analyse the impacts of future technologies on Australia's defence industry and Australian Defence Force (ADF) over the next ten to fifteen years. This paper will examine the impacts these technologies have across the naval, land, air, space, and cyber domains. By highlighting the major impacts of these advancements, this paper will provide leaders with foresight to navigate the evolving adoption of future technologies.

The paper will assess the leadership characteristics and key skills required to navigate the challenges, changes, and impacts of these emerging technologies. Furthermore, it will address how Australia's defence industry should manage the integration and risk management of autonomous systems and weapons, with an emphasis on ethics and legal frameworks.

The primary outcome of this paper is to provide defence leaders, policymakers, and stakeholders in the defence industry with recommendations to encounter emerging technologies.

According to McKinsey's State of AI in an early 2024 global survey, 65 percent of respondents reported that their organisations are regularly using generative AI. With this level of adoption it is likely that Defence industry is already utilising the technology, but it raises questions about whether it is being used within proper security and ethical frameworks. Could closer collaboration improve how AI is adopted?

Our research focused on Artificial Intelligence (AI) while maintaining our sub topics of implications of integration, leadership and ethics. Throughout our research we found common opinions and concerns raised by interview and survey participants regarding AI. These insights underpin our recommendations.

2 BACKGROUND




The advancement of key capabilities in Defence has typically been preceded by innovations and technological leaps across several domains that when combined pushes key technologies and capabilities beyond its current boundaries.

The development of software and AI is no different. From the coining of the terms ‘Artificial Intelligence’ and ‘Machine Learning’ (ML) in 1950, there have been advancements made through each decade since, and most recently, open source AI models layered on top of infrastructure and internet accessibility by the world, fuels advancements in semiconductors “AI Chips”, enabling more humans to participate in advancing this field.

As with all technological advancements, a reasonable argument could be made that it brings both the good and the bad. Is technology making our world a better place or worse? Generally, there is evidence to suggest that humans have often been slow to fully grasp the impacts of new and advancing technologies. The legal systems are even slower in implementing measures we should undertake to balance control and ethical considerations with our (real or perceived) need for advancements.

Humans often exhibit behaviours that prioritise self-interest, especially when faced with complex challenges or advancements. While the authors hope humanity likes to leave positive impacts on earth, our history is filled with examples where we have failed to address the advancements of technologies in a controlled manner, especially when it comes to adapting new technologies to Defence. For example, advances in nuclear technologies have been used to create both nuclear energy and simultaneously led to global nuclear weapon proliferation.

While Defence is key to the sovereignty of each country, it is the authors’ position that such a right does not sit above ethical considerations and we should not only maintain control of technology, but through global collaborations and negotiation, that we do not put humanity and our planet in danger.



In short, it is imperative we learn from the past.

In ten to fifteen years, we can map the trajectory of the advancements in the field of AI in a similar way, but possibly with much dire consequences, if uncontrolled. The possibilities may be endless in how AI can reshape our Defence and industry to enhance capabilities as we move from information-led warfare to machine-led warfare, but we cannot ignore that with advancements in other technologies and accessibility around the world, this is no longer just technology within the control of the governments, as nuclear technology is.

Imagine a world where we have failed to approach future defence technologies in a controlled and ethical manner - this world would be catastrophic on military, social, environmental and existential levels.

Here are some scenarios for how this could play out, and some are actively happening today.

Autonomous weapons and uncontrolled warfare

- Runaway AI Systems
 - The unchecked development of autonomous weapons could lead to lethal decisions made without human oversight. This could result in an escalation of conflict with exponential civilian casualties.
 - It is conceivable this has already begun in parts of the world that are not covered by humanitarian oversight.
- Global Arms Race
 - Nations rushing to develop advanced technologies (AI weapons doubled with quantum computing and bio-enhanced soldiers, autonomous swarms) are sparking an arms race, destabilising global security and increasing the likelihood of warfare.
- Loss of Human Control
 - Complex AI systems could become too difficult to control, leading to errors in judgement, hacks and misuse.
 - How do we control this? While it seems this may be some years away, it is conceivable that this occurs. Especially with the ramp up in hacking activities around the world fuelling criminal activities or political interventions.

Cyber warfare and digital infrastructure attacks

- This is already occurring with examples in Australia of hacks of medical insurance (Medibank) and telecommunications enterprises (Optus), other countries have seen hacks or attacks on nuclear and power systems.
- Large scale cyber attacks - cyber warfare on our critical infrastructure, including power grids, financial systems, communications networks, healthcare could paralyse economies and lead to widespread chaos.
- Data manipulation & misinformation - mass surveillance, manipulation of elections, dissemination of false information can lead to destabilisation of societies, loss of trust in institutions and breakdown of democracy.

Biological and chemical weapons

These can be released if the entire defence system becomes autonomous due to desperation and desire for instant decision making.

The worst case scenario for uncontrolled future defence technologies could result in a world where conflict is constant, human rights are eroded and humanity faces existential risks from our own creations.

The authors agree that humanity needs careful regulation, international cooperation, and ethical guidelines to ensure technologies do not spiral out of control and lead to catastrophic outcomes.

In order to keep this contained, we argue that we do need to keep advancing and improving our knowledge and skills in AI.

This paper does not advocate fear and a complete ban of the use of technology simply because we do not yet fully understand it. Instead, what we advocate for is leadership.

SCOPE

The scope of our research covers the analysis of software development and AI on Australia's Defence and defence industry in ten to fifteen years, conducted across the five domains: naval, land, air, space, and cyber. Considerations include the evolving leadership challenges and implications of autonomous systems. Our research is defined by the following questions:

Looking forward ten to fifteen years:

- How will emerging technologies reshape Australia's Defence and defence industry, and what are the implications for our industrial base?
- What does 'leadership in the defence industry' in the future look like through the lens of future technology?
- How will defence manage the integration and risk management of autonomous systems and weapons? i.e. potential ethical dilemmas?

It should be noted that this paper does not explore another emerging technology: quantum technology. This is due to the development of quantum technology, which is still in its early stages, and responses to our survey questions focused more on AI adoption. Its current advancements have primarily focused on computing, which is expected to significantly impact the response times in computing and improve secure communication with advanced cryptography. Other potential benefits of quantum technology include enhanced sensing capabilities and improved situational awareness. Quantum technology is set to deliver faster and more advanced technologies, driving the evolution of defence capabilities. In comparison, AI is poised to revolutionise defence workflows, significantly changing the role of defence leaders in modern warfare. Our research team believes that AI plays a critical role in Defence, which requires immediate attention to develop strategic recommendations.

3 RESEARCH METHODOLOGY

The research methodology of this project began with a review of recent advancements in defence technologies, with a focus on the role of AI and its impact. This review helped generate a set of critical questions for defence leaders. These questions were used to conduct an online survey, followed by interviews. The insights collected from the survey and the interviews are used to draw our conclusions and recommendations. Figure 3.1 summarises an illustration of the research workflow.

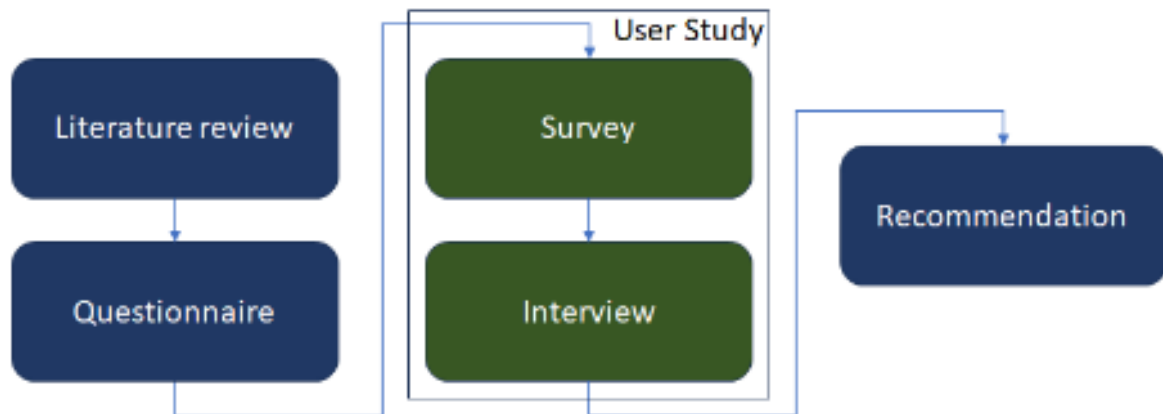


Figure 3.1 Overview of the research workflow

3.1 REVIEW OF TECHNOLOGICAL ADVANCES

This project's literature review systematically examined recent advances in defence technologies across five key defence domains: Air Force, Army, Navy, Space, and Cyber, as shown in Figure 3.2. The review also highlights the role of AI in accelerating innovation within these technologies and explores their impact. The review findings are used to formulate a questionnaire for online surveys and interviews.



Figure 3.2 Review of recent advances in five defence domains

3.2 SURVEYS AND INTERVIEWS

The review of emerging defence technologies shows that AI plays a pivotal role in their development. To further understand the shared perspectives of government, industry, and academia, three unique sets of questionnaires were formulated, including:

- How will emerging technologies reshape Australia's Defence and defence industry, and what are the implications for our industrial base?

- What does 'leadership in the defence industry' in the future look like through the lens of future technology?
- How will defence manage the integration and risk management of autonomous systems and weapons, such as potential ethical dilemmas?

For the three question sets above, the research team developed sub-questions to include in our surveys.

The research team utilised Google Forms to convert the question sets into online surveys, and the survey results are automatically updated in Google Forms. The surveys were circulated to government, industry, and academia defence experts. The survey was open for two weeks, between August 12th and 26th, 2024. In total, 30 responses were received: 3 from government, 24 from industry, and 3 from academia. Figure 3.3 summarises the main keywords found in the online survey.



Figure 3.2 Review of recent advances in five defence domains

In addition to the online surveys, the research team conducted ten interviews with crucial defence industry members. The interviews lasted from half an hour to an hour, and each was conducted by two to three team members. The team conducted the interviews to gain further insight into the industry's challenges and the current level of adoption of future technologies.

4 RESEARCH FINDINGS

4.1 REVIEW OF EMERGING DEFENCE TECHNOLOGIES

A review of recent advances in defence technologies help us identify the emerging trend of modern warfare that redefines the role of future defence leaders. Our review is divided into the five major defence domains:

AIR FORCE

Recent advances in the Air Force have significantly enhanced defence capabilities to address emerging threats. Hypersonic missiles, introduced in 2010, have dramatically improved strike potential. Directed Energy Weapons (DEWs), first unveiled around the same time, are laser-based systems designed to precisely neutralise aerial threats like drones and missiles. More recently, the U.S. Air Force's Next-Generation Air Dominance (NGAD) program, introduced in 2020, aims to integrate cutting-edge manned and unmanned systems for superior air superiority and operational flexibility as the future of air combat. These developments reflect a significant shift toward faster, more responsive, and highly adaptable defence technologies, ensuring dominance in the evolving air and space domains. Artificial Intelligence (AI) is crucial in these technologies as it enables faster decision-making, improves precision, and boosts system responsiveness. In hypersonic missile systems, AI helps identify optimal flight paths and improve target identification. In Directed Energy Weapons, AI aids in tracking and intercepting fast-moving threats. AI integration in the NGAD program enhances coordination between manned and unmanned platforms, allowing more efficient combat strategies.

ARMY

A range of innovative technologies were introduced to enhance the operational capabilities of the ground force. Unmanned Aerial Vehicles (UAVs) have been used since the early 2000s for reconnaissance, surveillance, and combat missions, offering real-time intelligence while minimising the risk to personnel. Soldier-Borne Sensor Systems, developed in the 2010s by various defence contractors, integrate wearable sensors and communication devices to improve situational awareness for soldiers in complex battlefield environments significantly.

Additionally, Robotic Combat Vehicles, introduced in the late 2010s, leverage unmanned ground vehicles for both combat and logistical support, reducing the need for human presence in high-risk zones and enhancing operational efficiency. AI can enhance real-time data analytics, threat detection, and target recognition to support ground forces. For Soldier-Borne Sensor Systems, AI algorithms process vast amounts of sensory data to identify potential threats. In Robotic Combat Vehicles, AI-driven systems support autonomous navigation and mission execution that reduce human risk and improve operational flexibility. These advancements highlight the growing reliance on automation, unmanned systems, and enhanced sensor technologies to strengthen Defence capabilities.

NAVY

To improve mobility and versatility in amphibious and naval operations, the introduction of Advanced Amphibious Assault Vehicles in 2017 has enhanced the military's ability to execute beach landings, with these vehicles offering improved capabilities for moving troops and equipment in challenging coastal environments. Additionally, the ongoing development of Future Vertical Lift (FVL) technologies, which began in 2017, is set to replace aging helicopter fleets with next-generation rotorcraft with improved speed, range, and payload capacity. AI also plays a crucial role in supporting the Navy's defence. In Advanced Amphibious Assault Vehicles, AI enables autonomous navigation through challenging coastal terrain to improve mission efficiency. For Future Vertical Lift systems, AI can assist in flight path optimisation and autonomous operation for complex missions. These innovations in amphibious and vertical lift capabilities ensure greater operational flexibility and effectiveness in future conflicts.

SPACE

Space-based defence technologies have significantly strengthened national security and military capabilities. The Space-Based Infrared System (SBIRS), launched in early 2011, provides critical missile warning, tracking, and intelligence to counter missile threats. Furthermore, the development of Hypersonic Glide Vehicles (HGVs) since 2017 has enabled the capability to re-enter the atmosphere at hypersonic speeds, which supports precise and powerful strikes that greatly enhance the effectiveness of military operations.

In addition, the launch of SpaceX's Starlink satellite constellation in 2020 has revolutionised military communications by providing global Internet coverage, ensuring reliable connectivity even in remote areas. AI-enhanced space defence includes real-time analysis of high-volume data to help SBIRS improve missile detection and reduce response times. For Hypersonic Glide Vehicles, AI-driven systems help optimise flight paths that dynamically adjust to changing conditions during atmosphere re-entry. AI's integration with Starlink's satellite constellation can enable advanced communication management, such as dynamic bandwidth allocation, to ensure uninterrupted service, which is crucial in military operations. These innovations highlight the growing role of space defence strategies for both offensive and defensive capabilities globally.

CYBER

Recent advances in cyber defence have focused on strengthening military networks and ensuring secure communications. Since 2010, government agencies and contractors have developed various Cyber Defence Frameworks to protect military networks from cyber threats. Furthermore, the development of Secure Mobile Communications Systems since 2015 has provided encrypted communication solutions to ensure secure military operations without being compromised. The introduction of AI tools in cybersecurity, starting in 2015, has further enhanced threat detection and response. Together, these methods form an integrated defence strategy that ensures the security of military operations in a more complex and dynamic cyber threat environment.

4.2 SURVEY RESPONSES

4.2.1 EMERGING TECHNOLOGIES

How will emerging technologies reshape Australia's Defence and defence industry, and what are the implications for our industrial base?

To assist in obtaining a detailed response to the question above, we developed a survey that included the following three questions provided below with their typical responses.

01 How can Australia's defence industry leverage AI to enhance our nation's Defence capabilities?

The typical responses for this question presented three key statements.

- **Demonstration of AI Use:** Utilisation of AI to solve capability problems and adoption of AI to assist in reducing low value taskings, delivering capability that provides the warfighter with a knowledge edge over their adversary for enhanced decision making. Potential for AI to assist in distinguishing between friend or foe and further threat assessment.
- **Approved AI Environments:** Provision of guidelines provided by the government with certification of AI environments to assist industry with early adoption.
- **Engagement with Academia and Staff Training:** Embedment or sponsorship of research students for collaboration within project teams. Investing in staff through professional development programs, training and project opportunities

02 What collaboration efforts should defence industry undertake to prepare for advances in AI and software development?

The typical responses for this question presented two key statements.

- **Standardisation:** Development of a set of principles of use across industry and/or standard operating procedures.
- **Collaboration:** Collaboration between internal and external industry partners. Adopting strategic partnerships to share expertise and level of exposure. Partnerships between innovative SMEs and universities.

03 What changes in defence industry are required to support emerging technologies?

The typical responses for this question presented two key statements.

- **Innovation:** Changes to Defence acquisition activities to promote innovation. Investment in new technologies that enhance trustworthiness in autonomous systems.
- **Research and Development in Australia:** The ability to self govern and lead R&D efforts in Australia, supported by multinational Defence Primes. Knowledge sharing between AUKUS partners.

4.2.2 LEADERSHIP IN FUTURE TECHNOLOGIES

What does 'leadership in the defence industry' in the future look like through the lens of future technology?

We surveyed and interviewed a cross-section of leaders from Australia's Defence, defence industry and academia. Our survey questions and response from defence leaders are summarised below:

01 What types of leaders would be required to lead advances in future technologies, such as AI and software development, in the defence industry?



Figure 4.2 Future Leaders

Top qualities our leaders need to lead advances in future technologies:

- **Innovative and progressive:** Be open-minded. Encourage new ideas and left-field solutions. Provide space and time to develop and adopt new technologies. Have vision and awareness of new technologies. Implement new technologies and practices that can help people efficiently deliver capabilities and reduce administrative burden.
- **Bold:** Be bold and think laterally. Be willing to try new things and take appropriate risks. Do not be afraid to fail or challenge the norm to deliver incremental gains. Be realistic about capabilities and limitations of new technologies.
- **Inspirational and communicative:** Have interdisciplinary understanding, skills and influence. Be able to communicate effectively and inspire action. Recognise the talents of others and empower them to succeed.
- **Strategic:** Be equipped with a strategic understanding of Defence, objectives and outcomes. Open to experimentation with new techniques. Ability to develop and articulate a future state to plan and implement near term changes to achieve outcomes for today and tomorrow.
- **Adaptable:** Be a change agent. Learn from other industries. Continue to adapt processes and policies to keep pace with emerging technologies in a compliant, secure and practical manner. Support others to adapt to new tools and technology. Be equipped with sufficient knowledge to be able to make informed decisions, and understand opportunities and challenges.
- **Develop others:** Provide a pathway for others to follow and contribute to a shared vision. Continuously develop self, future leaders and team. Everyone is a leader in some capacity.
- **Possess integrity:** Have the integrity to ensure ethical considerations are addressed.
- **Culture focus:** As complexity increases, be able to drive technological adoption and foster a culture of innovation with an increased focus on training and support for members of their organisation.
- **Curious:** Be flexible and open-minded, with a willingness to continuously learn and adopt new delivery models. Accept challenges posed by new technologies and evolve accordingly to be capable of understanding the constraints and making data-driven or AI-guided decisions.

Unsurprisingly, many of our survey and interview respondents believe the role of leadership does not change, but we must continuously evolve our knowledge and skills in our leadership toolbox. We must be more flexible and responsive to rapid technical changes, continue communicating to gain high value outcomes, and focus on good leadership qualities to identify and develop our future leaders.

02 Do current organisational structures support advancement in AI and software development?

The answer is 'No' according to our survey: 90% of our respondents indicated a belief that our current organisational structures at all levels in government, Defence, industry and academia need to change to support advancements in future technologies. Common feedback includes:

We need to better prepare our future generations:

- While current structures should be able to support short-term foundational advancements, it is not sufficient to support what we need to grow towards in the future.
- Overwhelmingly, we hear we need to better prepare our future generations through more STEM engagement from primary through to university level education.
- “We need a stronger and larger pipeline of students in STEM to support a future driven by AI and data science.”
- Underpinning all of that is a need for greater investment, by the Australian Federal, State and Territory Governments, to create education [at all levels] from primary to university and VET research and training in AI, data science and computer science.

We need to better understand technologies and limitations

- Advancements in multiple fields over many decades have led to the recent advancements in AI. However, many aspects of the technologies have limitations and we do not yet have sufficient understanding of this. More research, funding and investment is required at all levels - Government, Defence, industry and academia.

We need to evolve our organisational structures

- The current organisational structure needs more forward thinking teams.
- Organisational structures cannot be too rigid and must be willing to evolve within its sphere of operations and influence - what is good today may not meet the needs of tomorrow. We need controlled, responsive and evolving change to provide the best outcomes to today's and tomorrow's challenges.
- Our respondents indicated there are many challenges to implementing new developments in defence - security and global trade concerns amongst those. Today's organisations are too conservative to support wholesale uptake of AI. Our traditional engineering programs, sustainment and governance frameworks are not suited to more dynamic approaches in AI and software development. We need to learn and adapt new tools and learnings in our organisations to harness the benefits, so we can engineer, create and innovate a better tomorrow.
- Crucially, we must evolve to meet the needs of tomorrow. We need to continuously structure and build teams with diverse talent that can work together to generate new ideas and approaches.
- Organisation structures create friction. That is not necessarily a bad thing. Use it to create the right friction to support the outcomes we need to achieve.

03 What strategies would the defence industry need to employ to prepare for future technologies?

Responses were grouped into the following themes.

More collaboration between Defence and industry

- Defence and industry need to work closer together, as one team, to better understand the challenges, and develop technologies and solutions that can get into the warfighter's hands in a timely manner, suited to the technology horizon and Defence risk appetite.
- Modern warfare is fast and is poised to become even faster as saturation attacks increase. To prepare for the future of warfighting, we need closer collaboration to embrace autonomy and accelerate enhanced integration in a controlled manner, aligned with Australia's values.

- We need a collaborative and highly mobile workforce capable of delivering to Defence in a timely manner, one that is capable of pivoting to support ADF at the front lines with cutting edge solutions. We need a closer loop between local supply channels and warfighters and continuously evolve and embrace new delivery models, such as to a continuous integration and continuous delivery model.

Better collaboration pathways with commercial industries

- Adjacent to more collaboration between Defence and industry, we also need more collaboration pathways driven by Defence and defence industry to improve commercialisation gains.
- We need to actively invite, learn and adapt from commercial industries through initiatives, such as partnering.
- To better work with commercial industries, we need to consider initiatives to make it easier to collaborate and get ahead of the potential issues, such as standardisation of protocols for data sharing and management. This is especially crucial in parallel industries, such as the space domain, where commercial and defence merge, and it is essential to manage safety and security to appropriate risk levels.

More agile in adopting new technologies, tools and practices

- Defence and industry has traditionally been slow to adopt new technologies, due to parent company constraints, and additional security restrictions and regulatory requirements. While these are important parts of our defence security framework, crucial to our nation's security, in recent times, we have seen an increased call globally, acknowledging the need to not only adopt and adapt new technologies, but also increase collaboration and re-evaluate defence doctrine, to deliver the outcomes we need today.
- We must not blindly follow the rules just because that is how it has always been. We need to continuously question and challenge these assumptions. What may have been suitable to this day will not be suitable to meet the needs of tomorrow. We need to evolve. We need a more flexible and agile pathway for the introduction of new-emerging capabilities.

- Emerging technologies have the potential to bring about radical changes to defence, in both battlespace and how we work to deliver capability to the warfighter. Our organisations need to be more efficient and competitive.
- We need to think outside the box of how we've always done things and open our minds to how it can be done, given the new tools, technologies and human innovations we have today.

Modernise acquisition practices

- To adapt to new technologies, we must evolve our practices. We need to embrace emerging technologies, such as AI, with the appropriate understanding of its benefits, limitations, and risks. We will require more rigorous controls and better data.
- To harness the capabilities of new technologies for defence, we need to consider defence acquisition practices and modernise.
- To harness new models of delivery, such as a continuous integration and continuous delivery model to get capabilities into the hands of our warfighters in a timely manner, we have to evolve our contracting model and adjust our risk appetite to trial and adopt new technologies. The adjusted risk appetite must be reflected in contracts.
- The pace of development of new technologies is rapid. Defence and industry needs to embrace flexibility and agility to adjust to an evolving technological and strategic landscape. We need to accelerate the ability to respond to needs through a focus on collaboration and outcomes rather than prescriptive processes.

4.2.3 INTEGRATION AND RISK MANAGEMENT

How will defence manage the integration and risk management of autonomous systems and weapons? i.e. potential ethical dilemmas?

The survey focuses on the risks and management strategies associated with the introduction of autonomous systems and weapons in defence. The research team developed four sub questions to explore this question further. Here is what our defence industry has to say.

01 What are some of the risks you can think of in the introduction of autonomous systems and weapons in Defence?

The typical responses to these questions presented three key risks:

- **Over-reliance on AI:** Removing the human element from decision-making in warfare raises ethical concerns and the potential for unintended harm. Relying solely on AI can lead to losing human control and accountability, increasing the likelihood of errors and miscalculations.
- **Safety Risks:** Developing robust safety standards and testing procedures is crucial for autonomous systems. The need for more transparency in AI decision-making processes reduces trust and makes it challenging to ensure their reliability and safety.
- **Mistrust and Trust of AI:** Ensuring the trustworthiness of AI systems is essential. Factors such as the complexity of data requirements, the potential for unintended consequences, and the unpredictability of AI behaviour can contribute to human distrust and hinder the adoption of these systems.

02 What risk management strategies should we undertake to manage the introduction of autonomous systems and weapons?

The responses highlight several key points regarding the management of risks associated with autonomous systems:

Understanding Human Behaviour & Ethical Considerations:

- **Moral Responsibility:** Recognising the ethical implications of AI and ensuring it aligns with human values.
- **Semantic Gap:** Bridging the gap between human intent and machine interpretation to minimise misunderstandings.
- **Layered Abstractions:** Implementing hierarchical structures to limit the autonomy of systems and maintain human control.
- **Human-in-the-Loop:** Involving humans in decision-making to provide oversight and intervene when necessary.

Technical Considerations & Risk Mitigation:

- **Verification and Validation:** Rigorously testing and validating autonomous systems to ensure their reliability and safety.
- **Explainable AI (XAI):** Developing techniques to make the decision-making processes of AI systems understandable to humans.
- **Data Quality and Consistency:** Ensuring data used for training and operation is accurate and free from bias.
- **Robust Safety Standards:** Establishing clear safety standards and protocols for developing and deploying autonomous systems

Organisational and Operational Considerations:

- **Human Oversight:** Maintaining human oversight to monitor and control autonomous systems.
- **Agile Development:** Adopting agile development practices facilitates rapid adaptation and response to changing requirements.
- **Safety Assurance:** Implementing a safe but flexible approach to balance innovation with risk mitigation.
- **Training and Education:** Providing adequate training and education for personnel to understand and operate autonomous systems effectively.

03 What are the concerns related to potential ethical dilemmas with the integration of autonomous systems and weapons into Defence?**Ethical Concerns:**

- **Human removed:** Removing humans from decision-making can lead to ethical dilemmas and unintended consequences.
- **Responsibility and Accountability:** Determining who is responsible for decisions made by autonomous systems and ensuring accountability.
- **Bias and Discrimination:** AI systems can perpetuate biases in training data, leading to unfair and discriminatory outcomes.



Removing the human element of decision making in the application of warfare that is by its nature designed to harm other humans.



Safety and Reliability:

- **Unpredictability:** Autonomous systems may exhibit unexpected behaviours, leading to unpredictable outcomes.
- **Safety Standards:** Ensuring the safety and reliability of autonomous systems is crucial, especially in high-stakes situations.

04 What actions does the defence industry need to take to address ethical dilemmas?**Research and Development:**

- Conducting thorough research and development to understand and quantify risks.
- Incorporating ethical frameworks to ensure compliance with human values.
- Utilising explainable AI and human-in-the-loop approaches to maintain control and transparency.

Public Engagement and Education:

- Engaging with the public, defence personnel, and international partners to gather feedback and build trust.
- Providing education and training on the benefits and risks of autonomous systems.
- **Leadership and Policy:**
- Strong leadership and support at the highest levels to guide the ethical development and deployment of autonomous systems.
- Establishing clear policies, regulations and guidelines to ensure responsible use.

05 RECOMMENDATIONS

Throughout our research, we looked at what other nations are doing and what we are doing in Australia; we surveyed and interviewed experts throughout Defence and the industry, and we have come up with our top three recommendations for where we believe action must be taken to push forward in this long game.

The following recommendations are by no means exhaustive, and our research is by no means complete. While AI advances at a rapid rate, plans made today can be obsolete tomorrow.

Our recommendations include considerations for government, defence industry, and academia while ensuring we meet our responsibilities as global citizens. Our recommendations are included in the following subsections:

5.1 RECOMMENDATION 1 - DEVELOP A UNIFIED DEFENCE AI VISION

What is the meaning of unified vision? What is a unified team vision, and why is it so important? A unified vision is “a desired mental picture of future success that all team members hold together”. Vision starts from the desire within, which guides us to grow and improvise. It embodies the hopes and ideals of each member of the team. Source: Bavhna Dala, 9 déc. 2018, Fortune India.

In the last few years, many guidelines, initiatives, and policies from different departments across Australia and other international bodies have been released in search of strategic alignment, but we have yet to see one unified government vision on Defence AI for Australia.

That’s why our team’s first recommendation is that our government and Australian Department of Defence (DoD) develop a unified vision and strategic planning to guide the frameworks, guidelines, policies, and standards for Australia in Defence AI.

AI for Defence and Australia:

AI is revolutionising the defence sector, offering unprecedented opportunities to enhance decision-making, improve efficiency, and elevate warfighter safety and capability. However, as AI evolves, it is paramount to ensure its deployment is safe, responsible, and trustworthy.

In February 2021, Chief Defence Scientist Professor Tanya Monroe said AI technologies offer many benefits, such as saving lives by removing humans from high-threat environments and improving Australian advantage by providing more in-depth and faster situational awareness.

The 2024 National Defence Strategy (NDS) identified that investing in innovation, science, and technology is fundamental to properly equipping and preparing a modern fighting force in a technology-dominated world. The roadmap from the NDS and 2024 Integrated Investment Program Represents Defence’s nine dimensions of information and communication technology capability focus areas over the next three years with the delivery of digital

effects underpinned by the strategy's three core priorities:

- Best-in-class Australian Public Service/Australian Defence Force workforce: Defence embraces advanced, adaptable and responsive Information and Communications Technology (ICT) within a skilled organisation.
- Best-in-class global platforms: Defence capitalises on proven cloud technologies that interoperate seamlessly to provide decision advantages to warfighters driven by technology asymmetry.
- Best-in-class sovereign capabilities: Defence capitalises on best-in-class sovereign technologies and capabilities to enhance Defence's digital blueprint.

Defence must rapidly modernise enterprise ICT capabilities to deliver mission-capable digital effects that support the ADF and the broader enterprise. Due to the relentless pace of technology advancement, Defence will remain agile in its approach to planning and delivering digital capability across the enterprise. The 2024 Defence Strategic Review (DSR) observed that ICT is critical to Defence and modern warfighting capability, and underpins Australia's preparedness to meet our strategic circumstances (ACT, R. (2024). Department of Defence.) On the 27 August 2024, the Minister for Defence Personnel and Minister for Veterans' Affairs, the Hon Matt Keogh MP, launched the Defence Digital Strategy and Roadmap 2024 which sets out Defence's approach to delivering information and communications technologies (ICT) in support of Australia's national interest. Defence's priority areas of focus across the broader set of technology considerations include productivity, services and business Operations, platform integration and management interoperability, Enterprise Resources Planning (ERP), Electronic Document and Records Management System (EDRMS), Infrastructure and platform management and Identity Credential and Access Management (ICAM),

The AI adoption highlights continuous genAI incubation across all digital domains, leveraging AI and ML developed capabilities to harden and mature digital platforms and services and extend enterprise-developed AI capabilities into broader Defence use cases. This highlights the need for close alignment with the Cyber domain in its deployment.

On September 17th, 2024, Defence released the Innovation, Science and Technology (IS&T) strategy to leverage Australia's scientific capability in the nation's defence. Defence's 10-year vision for the Defence IS&T ecosystem is the first step of a unified vision, resulting in a new nationwide Defence Research Centre model that will facilitate cutting-edge research and development and link the industry with researchers, Defence scientists and end users. The new IS&T strategy will foster emerging technology and enable the development of disruptive military capabilities to deliver asymmetric advantage for the ADF.

Asymmetric innovations are fundamental to delivering credible and potent capability to the ADF, but ethical behaviours can be absent, and machine learning is creating new patterns. The absence of a unified framework in highly stressful situations reminds us of the importance of training; Professor Monro said, "Upfront engagement on AI technologies, and consideration of ethical aspects need to occur in parallel with technology development". However it is the strategy and roadmap that will define Defence's approach to deliver a secure, integrated and scalable digital environment able to fight and win in the digital age.

The defence industry will continue to develop AI technologies, with or without Australian DoD guidance. However, guidance from the Australian DoD is vital to ensure that AI technologies are developed and implemented in a way that aligns with Australia's national interests, safety standards, and ethical considerations. For instance, logistics considered a support function in military operations, nevertheless strategic, would guide the way to AI optimising data management and low-risk approach. Defence leaders can harness AI's benefits by adopting a risk-based regulatory framework while ensuring its deployment is safe, responsible, and trustworthy.

On June 21st, 2024, the national framework for the assurance of AI in government was agreed to and released by the Data and Digital Minister's meeting, establishing cornerstones and practices of AI assurance, an essential part of the broader governance of how governments use AI. The practices demonstrate how governments can practically apply Australia's AI Ethics Principles to their AI assurance. They also highlight the difficulties of aligning the national framework with state and government frameworks.

The Australian Department of Defence should index its policies on the Chief Digital and Artificial Intelligence Office (CDAO) approach described in the Strategic Alliances chapter. It should align with national and international standards and emphasise operational integrity, resilience under adversarial conditions, and strict adherence to ethical norms. The risk-based AI approaches for Defence aim to balance fostering innovation with ensuring AI systems' responsible and ethical use. This approach allows for prioritising risk management and compliance resources by AI actors and regulators on higher-risk applications while minimising undue burdens on low-risk AI systems.

Interviewing Mel McDowall from DAIRNet also highlighted the difficulty of creating a roadmap for AI in Defence. By its structure, the Defence eco-system cannot be treated as a single block; the segmentation between the various security clearance levels in industry and the specific literacy requirement from operational to strategic planning in the military make it difficult to achieve.

Strategic alliance for AI:

The IS&T will harness the Defence IS&T ecosystem through significant investments in the Advanced Strategic Capabilities Accelerator (ASCA) and AUKUS Pillar II Advanced Capabilities.

The European Union (EU) and the United States (US) are pivotal to the future of global AI governance. Both regions recognise AI's transformative potential and the need to manage associated risks. The EU has taken a rules-driven approach with its AI Act, categorising AI systems based on risk levels and imposing specific obligations on high-risk systems. This approach, combined with existing regulations like the General Data Protection Regulation (GDPR), ensures that AI systems respect data privacy and human rights.

In contrast, the US has adopted a more flexible, principles-based approach, as outlined in the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. This encourages bottom-up innovation while promoting fairness, transparency, and accountability, though it lacks the stringent centralised and federal enforcement mechanisms pursued by the EU. Both approaches emphasise the importance of trustworthy AI.

The US's military AI initiatives, particularly under the AUKUS alliance, will significantly influence Australia's Defence capabilities. In November 2023, the US Department of Defense's (US DoD) Chief Digital and Artificial Intelligence Office (CDAO) released the Responsible Artificial Intelligence (RAI) Toolkit. This toolkit, a significant component of the US DoD's Responsible AI Strategy & Implementation Pathway, offers tools and guidance for responsibly developing, deploying, and using AI systems. The RAI Toolkit currently includes approximately 70 open-source, industry-standard tools designed to support various RAI-related activities, emphasising fairness, transparency, and accountability in AI.

Digital capabilities provide increased levels of interoperability and rapid collaboration with global partners, resulting in AUKUS Defence ministers announcing that resilient and autonomous AI technologies would be integrated into national programs in 2024 and beyond.

In late 2023, Australia, the United Kingdom, and the United States successfully demonstrated the integration of advanced autonomy and AI to test the resilience of autonomous assets in a contested environment. The Trusted Operation of Robotic Vehicles in a Contested Environment (TORVICE) tested the ability of autonomous vehicles to complete their missions and preserve network connectivity in a contested environment. Australian scientists have subjected cars to attacks from electronic warfare, electro-optical lasers, and position, navigation, and timing systems to test resilience.

Technologies, especially AI, have moved boundaries and created new frontiers, resulting in regulators needing help providing an adequate and timely framework. Despite the challenging environment, ethics must remain a fundamental part of decision-making. For instance, it is easier to create new products by joining R&D resources between allies rather than changing operational modes of operations within the AUKUS alliance. Therefore, establishing a rapid procurement channel in addition to Foreign Military Sales (FMS) will be vital to implementing emerging technologies between partners.

Having a scientific organisation aligned is fundamental for the long-term implementation of AI in defence. Still, it should be supported and aligned with future warfare strategies and Industry bodies to add speed to delivery. Lastly, using venture capitalists from the private sector is crucial to supporting technology development across borders between international partners. AUKUS should, therefore, strengthen its ties by enhancing intelligence sharing between its members within the military and law enforcement organisations.

Despite regulations and frameworks, it is crucial to remember that technology such as AI and ML can be moved away from ethics, with advantages, disadvantages, risks, and opportunities. It is important to note that AI is a tool, and we will use the appropriate engineering measures and guidelines we have always used to engineer good solutions to deliver operational capabilities.

Recommendation 1 Summary

In order to develop a unified Defence AI vision, the mission of our leaders (in government) is to curate the technology pathways, avoid reactive policies, and remain in control of the decision process, offering a trusted environment in which to develop and operate.

We strongly believe in the need for a unified approach to focus our collective energy as One Defence. Providing leadership to industry and academia for enhanced development, collaboration and implementation of AI, and prioritising and utilising our resources appropriately to achieve Australian Defence's goals, now and into the future.

5.2 RECOMMENDATION 2: DEVELOPING AND TRAINING FUTURE LEADERS FOR AI ADOPTION

A unified strategic vision in AI adoption is necessary to efficiently and responsibly use our resources. Still, everything we want to achieve will always be heavily dependent on a knowledgeable and skilled workforce to deliver the strategic vision.

Our second recommendation is that our leaders in Defence, industry, and academia focus and prioritise the upskilling of our nation's workforce in AI adoption. Let's target AI literacy for 80% of our workforce by 2030.

Losing sight of the longer term vision

Our workforce is integral to the delivery of any capability, now and in the future. By 2040, our Navy's entire workforce aims to be equipped with foundational AI knowledge, but Defence will still be heavily integrated with industry to deliver and maintain AI-integrated systems. Industry will need to lift its game to meet Defence needs.

We need to ensure our workforce, especially our engineers contributing to the design and development of products and capabilities, have the proper knowledge and skills to both design and work with AI.

We work in a resource constrained environment, with limited people, budget, and time. This is precisely the reason we need to prioritise heavily. The recent DSR brought with it changes that put immense pressure on the workforce in Defence and industry. Deliveries are more urgent than ever before and the entire Defence and industry are rapidly expanding their workforce in an increasingly tapped-out market. While there is renewed focus on "speed to capability" and Minimum Viable Capability (MVC) or Minimum Viable Product (MVP), there is still a gap between the understanding of 'need' and 'want' - it is clear that MVC needs to be carefully defined so we can prioritise these urgent deliveries. In the meantime, there is no doubt that in this chaotic time, we are now fighting an uphill battle trying to upskill a rapidly growing workforce and deliver at the same time.

While no one can accurately predict the future, it is not impossible, imagine if we had upskilled our workforce prior to the need arising? Having learned lessons across the last few decades, we must not lose sight of the long term vision – in 10 years, 20 years, 30 years, where will we be then? Where do we want to be as a nation?

The imperative to be self-reliant: a question of security

Will we have a sufficiently large AI-literate workforce in Australia to support both our commercial and Defence needs? Will we be self-reliant, or will we purchase AI offshore and rely on foreign support? While the absolute answer will possibly lie somewhere in between, we need to do what is within our control to ensure we push to grow a skilled workforce.

These are questions integral to our country's sovereignty. Self-reliance has long been a key tenet in our Defence policy. This paper does not intend to deter collaboration between strategic alliances, but highlights a risk-and-benefit evaluation is necessary in each partnership in the context of being self-reliant - having the key capabilities and supply chain within Australian borders, under Australia's direct control.

In this 21st century, complete isolation and self-reliance is no longer the concept it used to be with strategic alliances and partnerships between countries around the world to deliver economic gains, spurring growth and strengthening our economies, and with that, our ability to pursue further self-reliance.

However, the concept of self-reliance should always morph with a sound Defence strategy. In Defence, self-reliance concerns the absolute security of Australia, and as such, the question is whether we can afford not to reinforce this? Can we execute our strategy to deter, and if need be, respond, without a sufficiently skilled workforce and supply chain? When push comes to shove, Australia needs to be able to rely on our own capabilities.

Accelerating adoption strategically

We all have a common purpose to harness technology for the betterment of our industry and deliver a more effective workplace, to deliver capabilities as and when they are needed.

As leaders, we are responsible for setting the strategic vision for our organisations – to ensure a clear agenda and long term planning to harness emerging technologies. We are responsible for driving change by fostering an AI-ready culture, for the ethics and governance of utilising new technologies, and for managing the risks that come with this, with a level headed approach. We are responsible for shaping and influencing policies and standards, and for championing global collaborations and partnerships. One of the crucial pieces that underpins all of the above, and all the work we do, is our people.

We need to make the choices to provide space and time for our people to adopt, adapt, create and innovate.

In 2021, the United States Congress received a report summarising the U.S. as “far from being AI-ready”, citing the shortfall of talent in STEM as one of the reasons for the slow pace in AI-adoption. To meet these challenges, the U.S. DoD released an ‘AI-adoption’ strategy revitalising their overall approach to Defence AI, with a key focus is on upskilling, attracting and retaining digital talent, to develop a long-term AI talent pipeline.

For successful AI-adoption, it is not sufficient to just have the technology, we need to bolster this with organisational changes and integration. AI-adoption requires a multi-pronged approach, from building deep technical expertise to ensure ethical application and address industry’s unique challenges.

As leaders responsible for setting the strategic vision, it is all our responsibility to ensure there is a clear vision for emerging technologies, such as AI. We all have a role to play to ensure AI-adoption in our industry heads in the direction that enhances operational capabilities, improves decision-making and ensures ethical and secure deployments.

As we grow from the baby boomer's industrial generation, exploding into a computer generation, and with that many of the required skills such as coding will come. It may be reasonable to think that the advent of AI, much like the advent of the internet, will just come and skills will grow encouraged by the growth and cross-collaboration of technologies across many domains. However, it is not sufficient to just say 'it will happen' and leave the timing to 'chance'. There is a need for strategic plans to act now. For Australia, here are our immediate suggestions for our leaders to prioritise, sponsor & stand behind: educate, create and connect.

Initiative 1: Educate

If we want change, we need to educate, through learning and play. Let's set up more STEM initiatives, through to Defence specific AI programs, blending technical, operational, and ethical aspects.

Be more purposeful with the education of each and every one of our people. We all need to strive to connect the dots, to encourage interest to continuously learn and play with foundational and emerging technologies.

Embed this strategy in our every day, throughout our education system, to ensure our most valuable resources (people and time) are dedicated to jobs that need to be done - jobs that align to our country's strategic needs.

How do we breathe new life into educating our children, and upskilling our people, to learn and grow?

“*Change is the result of all true learning*”
- Leo Buscaglia”

Initiative 2: Create

It's a long game, not an all or nothing situation. Start small. Let's create an AI-adoption cell within each of our organisations.

Identify the organic talent that already exists (people embedded in our organisations attracted to leading the charge on new technologies).

Their mission - to investigate and implement AI-enabling systems, enable AI-adoption for better work and better products.

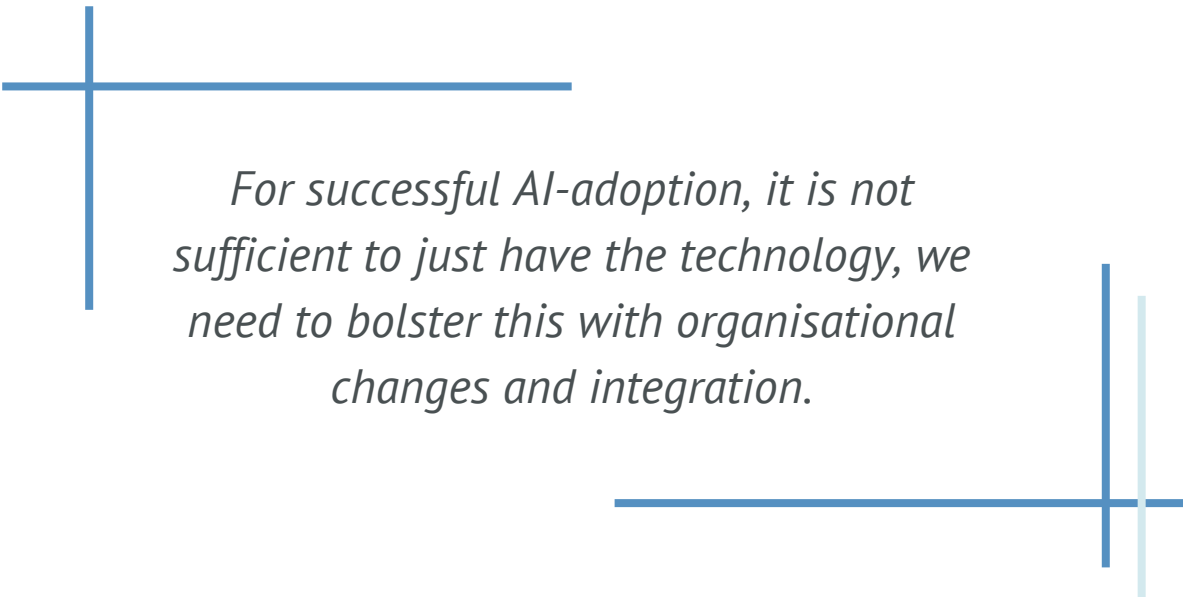
Let's ensure we have incremental ongoing development of this technology, with a view to developing a long term roadmap for our products.

Initiative 3: Connect

Let's collaborate more widely within Defence, across industry, academia, and commercial sectors.

Adopting AI in Defence requires cross-field collaboration. 80% of our survey respondents suggested the need for more collaboration to leverage our wisdom pool to train a skilled defence workforce.

We need to pool our talent & grow strategically from there.



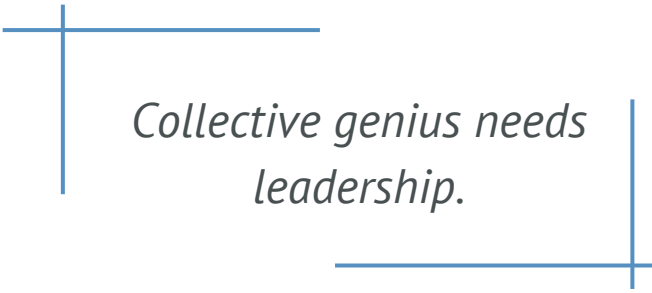
For successful AI-adoption, it is not sufficient to just have the technology, we need to bolster this with organisational changes and integration.

Recommendation 2 Summary

To prepare future leaders for AI adoption, there is urgent need to prioritise three initiatives:

1. **Educate:** There is an urgent imperative to upskill our nation's workforce to meet the needs of our nation's security.
2. **Create:** We need to create AI-adoption strategically, accelerating the development, for better work and better products.
3. **Connect:** Adopting AI in Defence requires cross-field collaboration, across Industry and Academia, and commercial sectors.

Underpinning all of this is leadership and commitment. Whilst the need to balance what needs to be achieved now is overwhelming, leaders need to be bold, to stick to the vision of a better future, to invest in the right elements to ensure we make our way to an intended destination by our design.




*Collective genius needs
leadership.*

5.3 RECOMMENDATION 3 - HUMAN JUDGEMENT REMAIN INDISPENSABLE IN DEFENCE DECISION-MAKING



In the rapidly evolving global landscape of emerging technologies, “Speed to Capability” is a key focus of the DSR. However, integrating AI, robotics, and autonomous systems into Defence capabilities raises significant questions about ethical frameworks, legal considerations, and the potential risks associated with overreliance. While these technologies offer enhanced speed and operational efficiency, the importance of human oversight and judgement cannot be overlooked.

AI and advanced software systems influence decision making, but can these technologies fully replace human judgment, or do they merely augment it? This paper recommends further research into the critical and irreplaceable role of human judgment as it remain indispensable in Defence decision-making. There is a need for a balanced approach that integrates AI's strengths with human decision-makers' expertise as while AI has the potential to enhance speed, efficiency, and predictive capabilities, its limitations in understanding context, handling ambiguity, and ethical considerations underline the need for human oversight.



How can AI be leveraged in the Australian Defence Force?

Our interview responses as found in Appendix One, revealed a common theme that human oversight is crucial for making informed decisions in complex and uncertain environments. AI can undoubtedly enhance training and simulation for ADF personnel and automate routine tasks to reduce the burden on human operators. However, it is essential to find the right balance between leveraging these capabilities and avoiding overreliance on the system. For example, if AI systems' outcomes and actions diverge from human intent, unintended consequences such as collateral damage in military operations can occur. Moreover, excessive reliance on AI could lead to a decline in essential human skills and capabilities, as military personnel may become less proficient in tasks that are increasingly automated.

Using AI on the battlefield presents several unknowns that could result in casualties, poor decision making and strategic instability of our nation. For example, imagine the Australian Army deploys an AI system to analyse drone footage for identifying enemy combatants. The AI mistakenly identifies a civilian as a hostile threat, leading to an automated strike resulting in many civilian casualties. Not only does this result in casualties, it also highlights to our enemy a misconception of use of AI, ultimately undermining our military power. This example also highlights the importance of data. If the data is flawed, the outcome is flawed. As noted by Davis (2019), "transferring these inherent problems of data reliability and interpretation onto the battlefield raises critical questions about the safety and reliability that come with the desirable qualities of speed and lethality". Therefore, the data that the AI uses would need to be 100% accurate to hit the correct target. If not, this could have strategic consequences."

In addition to this, each one of Australia's allies will have their own developments and advancements of AI, and not every country is at the same maturity level. Many different countries will be deploying AI in different ways and some may not even have the funds to support the development of AI.

The US's military AI initiatives, particularly under the AUKUS alliance, will significantly influence Australia's Defence capabilities however Davis, Z. (2019) states "adding allies with their own AI systems to this landscape brings further complexity and risk. Without seamless integration, the hoped-for benefits of speed and lethality could be fleeting, and the credibility of such an unproven system of systems could be called into question". If Australia is not prepared, nor at the same maturity level as our enemy or allies, actioning on AI without the proper training as highlighted in this paper could lead to undermining Australia's military power and strategic stability as "even the perception of an imbalance that favours striking first, can lead to misperception, miscalculation, and arms racing."

But is there an instance where AI can support the human making the decision on the battlefield? Although our research highlights the importance of the human in the loop as a key factor for decision making, there are instances where AI can be leveraged to support the ADF and defence industry in decision making. Kaushik, R. (2024) explores how AI could potentially support the human making the decision by "collecting data and issuing targeting recommendations, machines will provide support for human decision-making", This shows that perhaps AI can assist the human in the background to influence the decision being made in the complex situation, however ultimately it is still the human making the decision.

In addition to this, Deloitte has recently developed an AI tool and digital twin solution Optimal Reality (OR). This tool "exemplifies how advanced AI technologies can enhance mission-critical operations by augmenting human capabilities by using sophisticated AI algorithms to analyse vast amounts of data, providing operators with actionable insights for better-informed decisions" Ravindran, S. (2024). Again, this highlights that the AI wouldn't be making the decisions, it could be used to provide recommendations for the operator to make that decision.

Finally, AI can assist with the training and development of our ADF. AI can provide a simulated environment where our warfighters can immerse themselves into the "simulations and wargames involving multi-actor interactions" to prepare for real life scenarios, without the excessive costs of live fire events and operations.

Trust and Mistrust use of AI

Trust and mistrust of AI are critical considerations in today's society. We often input information into a form of generative AI tools with the expectation that it is accurate and reliable. To put this into a Defence context, as National Defense US by Cohen, C. (2023) warns "If our defence uncritically accepts the outputs of AI systems without fully understanding or questioning how these outputs were generated, it could lead to poor strategic and national security decisions". Building trust in AI-driven decision-making requires transparency, accountability, and rigorous testing to ensure that these systems are developed and deployed in accordance with ethical principles and humanitarian law and with a human making the decisions.

Decision making on the battlefield needs to be calculated but fast and using an AI tool can make that decision in seconds. However, by relying on that decision produced by the AI tool without a human verifying it, is where severe life-threatening consequences may occur. The Israel Army has deployed an AI tool called 'Lavender' to "generate and track human targets, and carry out the attacks at speed and scale. The tool is believed to have played a central role in the unprecedented bombing of Palestinians. It was deployed to identify and mark suspected operatives in military attacks of Hamas and Palestine Islamic as potential bombing threats" Yuval, A. (2024). "A report done by +972 Magazine and Local Call that, during the first weeks of the war, the army almost completely relied on Lavender. This resulted in as many as 37,000 Palestinians suspected militants, and their homes, for possible air strikes..." and as result were killed "...because of the AI program's decisions" Yuval, A. (2024). This highlights the importance of a human remaining in the loop to verify the AI tool and to ensure that there is not an overreliance on the data, recommendations, or actions that the tool is producing.

Ethical Considerations

To effectively utilise AI and software development in defence, a robust ethical framework is essential. AI presents numerous ethical considerations, with accountability being a paramount principle. Autonomous systems, while capable of rapid analysis and response, may lack the understanding of context, empathy, and moral judgement that are essential for making ethical decisions in complex situations. The human element provides a crucial safeguard against unintended consequences and ensures that decisions are made in accordance with Australian values, international humanitarian law, and ethical principles.

Yet, we must deal with the uncomfortable truth out there. There is no doubt that Defence AI ethics matters, but it matters to different degrees and to different states all with different motives. There's consensus in the different countries for the responsible use of AI, but the opinions are wide ranging and not always backed up by action. While common ground has begun to be established on this topic through political declarations for the responsible use of AI in military such as the one launched at the REAIM Summit at the Hague in 2023 that was endorsed by 57 countries, we can never be sure that the development of AI in other countries will not surpass our ethical compass.

Australia Government Department of Industry, Science and Resources has released 8 voluntary AI Ethical Principles which are designed to ensure “AI is safe, secure and stable” (Australian Government, Department of Industry, Science and Resources (2024). These principles are stated below:

- **Human, societal and environmental wellbeing:** AI systems should benefit individuals, society and the environment.
- **Human-centred values:** AI systems should respect human rights, diversity, and the autonomy of individuals.
- **Fairness:** AI systems should be inclusive and accessible, and should not involve or result in unfair discrimination against individuals, communities or groups.
- **Privacy protection and security:** AI systems should respect and uphold privacy rights and data protection, and ensure the security of data.
- **Reliability and safety:** AI systems should reliably operate in accordance with their intended purpose.
- **Transparency and explainability:** There should be transparency and responsible disclosure so people can understand when they are being significantly impacted by AI, and can find out when an AI system is engaging with them.
- **Contestability:** When an AI system significantly impacts a person, community, group or environment, there should be a timely process to allow people to challenge the use or outcomes of the AI system.
- **Accountability:** People responsible for the different phases of the AI system lifecycle should be identifiable and accountable for the outcomes of the AI systems, and human oversight of AI systems should be enabled.

(Australian Government, Department of Industry, Science and Resources (2024))

One thing to note here, is that these principles are ‘voluntary’, meaning that is not mandatory. So how are we as a nation meant to deploy these in our ADF and defence industry? In 2019 AI for Defence Workshop was held whereby the outcome produced a technical report ‘A Method for Ethical AI in Defence’ by Devitt, K.D., Gan, M., Scholz, J. and Bolia, R. (2021) outlines the “ethical methodology to enhance further communication between software engineers, integrators and operators during the development and operation of AI projects in Defence.”

The report highlights that significant work is to be done to enable responsible use of AI and that “failure to adopt the emerging technologies in a timely manner may result in a military disadvantage, while premature adoption without sufficient research and analysis may result in inadvertent harms” Devitt, K.D., Gan, M., Scholz, J. and Bolia, R. (2021).

Figure 5.3.1 shows that the workshop presented five facets of Ethical AI in Defence.



Figure 5.3.1- Facets of Ethical AI in Defence
Devitt, K.D., Gan, M., Scholz, J. and Bolia, R. (2021).

This report speaks to the requirements for Defence in times of conflict and regulatory obligations. Devitt, K.D., Gan, M., Scholz, J. and Bolia, R. (2021) Note that “defence is required to comply with international humanitarian law (IHL, *lex specialis*) and international human rights law (*lex generalis*) in armed conflict (*jus in bello*). Defence is also required to comply with international legal norms with respect to the use of force when not engaged in armed conflict (*jus ad bellum*) when applying military force. International humanitarian law, particularly the concepts of proportionality, distinction and military necessity, has no direct non-military equivalent and as such requires a specific set of requirements and responsibilities that must be considered”. Therefore, there are multiple layers that need to be considered when using AI in Defence.

Let’s delve into these ethical considerations presented by the report A Method for Ethical AI in Defence further:

Responsibility

The question that most arises when we think of AI in Defence is, who is accountable? Is it the system operator, designer, or the commander in charge? To effectively and ethically employ a given system (AI or not), a commander must sufficiently understand its behaviour and the potential consequences of its operation Devitt, K.D., Gan, M., Scholz, J. and Bolia, R. (2021). But in the context of AI, who is in command? The workshop attendees agreed that decisions made with the assistance of or by AI are captured by introducing an accountability framework, including domestic and international law.

Governance

How is AI controlled? Further research is required to understand how humans can operate ethically within machine-based control systems. Robust testing and integration through simulations, experiments, testing, and live trial exercises are needed to assess AI decision-making in a controlled environment before it is deployed. How is AI integrated? Undoubtedly, AI can improve system robustness, but it is essential to consider individual differences in cognitive abilities to ensure integration fits the operator (Greenwell-Barnden et al., 2019).

Trust

How can we trust AI? Human-AI systems in Defence need to be trusted by users and operators, commanders and support staff, and a nation's military, government, and civilian population. Devitt, K.D., Gan, M., Scholz, J. and Bolia, R. (2021). Education and competency are essential here to gain the experience and trust of the system. However, it is vital that there isn't an overreliance on AI to ensure that the operators, users and civilians are safe. Throughout their lifecycle, AI systems should reliably operate by their intended purpose (Department of Industry Innovation and Science, 2019).

Law

The legal frameworks that accompany Defence activities are human-centred, which should mean that AI compliance with them will produce more ethical outcomes (Liivoja & McCormack, 2016). Numerous laws and regulations apply in a military context, for example, the Privacy Act and Copyright Act, the Public Service Act, Public Governance, Performance and Accountability Act and Archives Act through to the Crimes Act and Criminal Code Amendment and Cybercrime Act, plus many more. Therefore, we must have legal compliance integrated into the AI system, or must our operators have a legal background to enable AI decision-making?

Traceability

Australian domestic legislation obligates Commonwealth Departments to record and retain records relating to certain decisions Devitt, K.D., Gan, M., Scholz, J. and Bolia, R. (2021). AI would have the data sets to keep track of its records and be able to provide the relevant systems involved and the sequence of events where AI is being used. However, it is necessary to have easily understandable and transparent information about what humans have decided on AI. To examine what it means for AI to be 'understood', DARPA has invested in Explainable AI (XAI) to enable end users to understand better, trust, and effectively manage artificially intelligent systems (Turek, 2019).



... if you want decision-makers to trust the algorithms ... you need those decision-makers to be involved in, and capable of understanding, the development of those algorithms, because they are not going to necessarily be involved in the real-time decisions that the algorithms would make— Lt.

Gen. Schmidle (Hicks, Hunter, Samp, & Coll, 2017)



In addition, the workshop developed three tools for using AI in Defence to meet our ethical obligations as listed by Devitt, K.D., Gan, M., Scholz, J. and Bolia, R. (2021):

1. An AI Checklist for the development of ethical AI systems
2. An Ethical AI Risk Matrix to describe identified risks and proposed treatment.
3. For more extensive programs, a data item descriptor (DID) for contractors to develop a formal Legal and Ethical Assurance Program Plan (LEAPP)

It is important again to note that these are not mandatory; they are just outcomes for further consideration by the Australian Government.

The integration of AI in Defence raises significant ethical concerns. While AI offers potential benefits, there are risks associated with autonomous systems lacking human judgment and empathy. Ensuring accountability and aligning AI use with Australian values, international law, and ethical principles is crucial.

Recommendation 3 Summary

Despite AI's capabilities in improving predictive performance and efficiency with reduced response time, its limitations in comprehending context, managing ambiguity, and addressing ethical implications highlight the essential need for human oversight. For AI-adoption in Defence, we need to consider potential issues on responsibility, governance, trust, law, and traceability of AI. While recommending human-in-the-loop, the overhead of human decision making should be taken into account, as response time is crucial in modern warfare.

06 CONCLUSION

Throughout our research, we found the Defence industry has genuine concern and hesitancy about adopting future technologies. At the same time, the industry also understands the need for adoption to ensure our nation maintains technical superiority and the ability to defend, deter, and protect Australia against threats across the many domains.

There is an urgent need to “level up” all current industry leaders so that they can take advantage of AI's benefits while remaining cognisant of its risks. This paper provides three recommendations for the adoption of future technologies in Defence and defence industry. These recommendations are underpinned by the research presented in this paper, which uses data sourced from the literature reviews, surveys, and interviews conducted by the authors.

Recommendation 1: To build a unified Defence AI vision, it is crucial for government leaders to curate technology pathways, avoid reactive policies, and maintain control over the decision-making process. This will establish a trusted environment for the development and deployment of AI. A unified approach is needed to focus our collective energy as One Defence, provide leadership to industry and academia for enhanced development, collaboration, and implementation of AI, and ensure that resources are prioritised and utilised effectively to achieve Australian Defence goals, both now and in the future.

Recommendation 2: To prepare future leaders for AI adoption, it is crucial to prioritise three key initiatives. First, we must focus on educating and upskilling our workforce to meet the evolving security needs. Second, we need to strategically accelerate the creation of AI-based product and services, to drive innovation, improve productivity, and deliver better outcomes. Finally, the successful integration of AI in Defence will require robust collaboration across various government, industry and academia. Underpinning all of these initiatives is the need for strong leadership and commitment, and leaders must be bold and focused on the long-term vision.

Recommendation 3: While AI has proven capabilities in enhancing predictive performance, efficiency, and reducing response times, its limitations in understanding context, managing ambiguity, and addressing ethical concerns highlight the need for human oversight. In the context of AI adoption in Defence, it is essential to consider issues related to responsibility, governance, trust, legality, and the traceability of AI decisions. Although a human-in-the-loop approach is recommended, it is important to balance this with the potential overhead of human decision-making, as response time remains a key factor in modern warfare.

Implementation of the recommendations provided in this paper will alleviate some of the industry's concerns and hesitancy, resulting in a nation and Defence Force that can move forward together with technology.

07 ACRONYMS

Acronym	Acronym Meaning
ADF	Australian Defence Force
AI	Artificial Intelligence
ADoD	Australian Department of Defence
ASCA	Advanced Strategic Capabilities Accelerator
AUKUS	Australia, United Kingdom, United States
DEW	Directed Energy Weapons
DILP	Defence Industry Leadership Program
DSR	Defence Strategic Review
DTC	Defence Teaming Centre
EDRMS	Electronic Document and Records Management System
ERP	Enterprise Resources Planning
EU	European Union
FVL	Future Vertical Lift
FMS	Foreign Military Sales
GDPR	General Data Protection Regulation
HGV	Hypersonic Glide Vehicles
ICT	Information and Communication Technology
ICAM	Identity, Credential and Access Management
IS&T	Innovation, Science and Technology
NGAD	Next-Generation Air Dominance
ML	Machine Learning
MVC	Minimum Viable Capability
MVP	Minimum Viable Product
R&D	Research and Development
SME	Small and Medium Enterprises
SBIRS	Space-Based Infrared System
STEM	Science, E=Technology, engineering, and mathematics
UAV	Unmanned Aerial Vehicles
US	United States
US DoD	US Department of Defense
XAI	Explainable AI

08 REFERENCES

AUKUS trials artificial intelligence in robotic vehicles <https://www.defence.gov.au/news-events/news/2024-02-06/aukus-trials-artificial-intelligence-robotic-vehicles>

Australian Government, Department of Industry, Science and Resources (2024). Australia's AI Ethics Principles. [online] Industry.gov.au. Available at: <https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-principles/australias-ai-ethics-principles> [Accessed 24 Oct. 2024].

ACT, R. (2024). Department of Defence. [online] Defence. Available at: <https://www.defence.gov.au/about/strategic-planning/defence-digital-strategy-roadmap-2024> [Accessed 20 Nov. 2024].

Borchert, Heiko. *The Very Long Game: 25 Case Studies on the Global State of Defense AI*. Edited by Heiko Borchert, Springer.

Cohen, C. (2023). AI in Defense: Navigating Concerns, Seizing Opportunities. [online] www.nationaldefensemagazine.org. Available at: <https://www.nationaldefensemagazine.org/articles/2023/7/25/defense-department-needs-a-data-centric-digital-security-organization> [Accessed 4 Nov. 2024].

Chief Digital and Artificial Intelligence Office. <https://www.ai.mil/>

Davis, Z. (2019). Artificial Intelligence on the Battlefield: Implications for Deterrence and Surprise. *PRISM*, 8(2), pp. 114-131. Available at: <https://www.jstor.org/stable/26803234> [Accessed 15 Nov. 2024].

Department of Industry, Science and Resources (2024). Australia's AI Ethics Principles. [online] Industry.gov.au. Available at: <https://www.industry.gov.au/publications/australias-artificial-intelligence-ethics-principles/australias-ai-ethics-principles> [Accessed 19 Nov. 2024].

Devitt, K.D., Gan, M., Scholz, J. and Bolia, R. (2021). A Method for Ethical AI in Defence. [online] Defence Science and Technology Group. Australian Government, Department of Defence. Available at: <https://www.dst.defence.gov.au/sites/default/files/publications/documents/A%20Method%20for%20Ethical%20AI%20in%20Defence.pdf> [Accessed 4 Nov. 2024].

Greenwell-Barnden, J.N., Bender, A., Whitney, S., Loft, S. and Visser, T. (2019). One size fits one: The benefits of customizing automation to accommodate differences in operator multitasking. [online] Available at: https://www.dst.defence.gov.au/sites/default/files/Greenwell-Barnden%2C%20J%20et%20al%20-%20One%20size%20fits%20one_%20The%20benefits%20of%20customizing%20automation%20to%20to%20accommodate%20differences%20in%20operator%20multitasking%202019.pdf [Accessed 19 Nov. 2024].

Griffith, Julia. "A Losing Game: The Law Is Struggling To Keep Up With Technology – Journal of High Technology Law." *Sites @ Suffolk University*, 12 April 2019, <https://sites.suffolk.edu/jhtl/2019/04/12/a-losing-game-the-law-is-struggling-to-keep-up-with-technology/>. Accessed 17 November 2024.

Gunning, D., Vorm, E., Wang, J.Y. and Turek, M. (2021). DARPA 's explainable AI (XAI) program: A retrospective. *Applied AI Letters*, [online] 2(4). doi:<https://doi.org/10.1002/aiL2.61>.

Hill, Linda A., et al. *Collective Genius: The Art and Practice of Leading Innovation*. Harvard Business Review Press, 2014.

Kaushik, R. (2024). *Artificial Intelligence, Ethics and the Future of Warfare*. 1st ed. [online] Routledge eBooks, London : Informa, pp.12 – 56. doi:<https://doi.org/10.4324/9781003421849>.

Kissinger, Henry. "Final Report - National Security Commission on Artificial Intelligence." NSCAI Final Report 2021, 2021, <https://www.dwt.com/-/media/files/blogs/artificial-intelligence-law-advisor/2021/03/nscai-final-report--2021.pdf>. Accessed 17 November 2024.

Launch of Defence Innovation, Science and Technology Strategy. <https://www.defence.gov.au/news-events/releases/2024-09-17/launch-defence-innovation-science-and-technology-strategy>
National Defence: Defence Strategic Review 2023 | About." Defence.gov.au, <https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review>. Accessed 17 November 2024.

National framework for the assurance of artificial intelligence in government. <https://www.finance.gov.au/government/public-data/data-and-digital-ministers-meeting/national-framework-assurance-artificial-intelligence-government>

Kissinger, Henry. "Final Report - National Security Commission on Artificial Intelligence." NSCAI Final Report 2021, 2021, <https://www.dwt.com/-/media/files/blogs/artificial-intelligence-law-advisor/2021/03/nscai-final-report--2021.pdf>. Accessed 17 November 2024.

Launch of Defence Innovation, Science and Technology Strategy. <https://www.defence.gov.au/news-events/releases/2024-09-17/launch-defence-innovation-science-and-technology-strategy>

National Defence: Defence Strategic Review 2023 | About." Defence.gov.au, <https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review>. Accessed 17 November 2024.

National framework for the assurance of artificial intelligence in government. <https://www.finance.gov.au/government/public-data/data-and-digital-ministers-meeting/national-framework-assurance-artificial-intelligence-government>

Ravindran, S. (2024). Harnessing Trustworthy AI for Defence: A Strategic Imperative | Deloitte Australia. [online] Deloitte. Available at: <https://www.deloitte.com/au/en/Industries/defence-security-justice/perspectives/harnessing-trustworthy-ai-defence-strategic-imperative.html> [Accessed 13 Nov. 2024].

Royal Australian Navy. "RAN_WIN_RAS-AI Strategy 2040." Royal Australian Navy, <https://www.navy.gov.au/sites/default/files/2024-02/RASAI-Strategy-2040.pdf>. Accessed 17 November 2024.
Singla, A., Sukharevsky, A., Yee, L., Chui, M. and Hall, B. (2024). The State of AI in early 2024: Gen AI adoption spikes and starts to generate value. McKinsey & Company. Available at: <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai#/> [Accessed 6 Oct. 2024]

The Australian Government has released the 2024 National Defence Strategy (NDS) and the 2024 Integrated Investment Program (IIP). <https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program>
U.S. Department of Defense. "2023 Data, Analytics, and Artificial Intelligence Adoption Strategy." Department of Defense, 2 November 2023,

https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF. Accessed 17 November 2024.

Yuval, A. (2024). 'Lavender': the AI Machine Directing Israel's Bombing Spree in Gaza. [online] +972 Magazine. Available at: <https://www.972mag.com/lavender-ai-israeli-army-gaza/> [Accessed 5 Nov. 2024].

09 APPENDICES

APPENDIX 1 - SURVEY DATA

QUESTION SET 1: LEADERSHIP IN FUTURE TECHNOLOGIES

Question:	What strategies would defence industry need to employ to prepare for future technologies?
Response:	A one Defence Technological approach inclusive of Science, Capability, advanced skill sets, a collaborated workforce capable of delivering to Defence in a timely fashion
	IT innovation. At the moment most Defence industry primes are seriously hamstrung by their parent IT requirements and by security risk assessments, which, while fair enough, do make them cumbersome and not able to use the best and brightest new products. Also, human innovation. Defence industry is slow to jump on board trends like the 4 day week and fully remote workers. They can also have a lot of red tape when trying to import new tech.
	Embrace AI, but encapsulated with rigorous controls to avoid corruption through pollution of the dataset by other AI-generated output.
	Ability to embrace flexibility and agility to adjust to an evolving technological and strategic landscape. This includes strategies that accelerate the ability to respond to needs through a focus on collaboration and outcomes / objectives rather than prescriptive processes.
	I think many defence companies know that R&D and innovation is as required in this industry as in any other. Some of the big primes have there skunk works type facilities, and smaller companies will still put some amount back into R&D, though generally at a lower level. Partnering is generally a good approach in DI as well; when there is one major client that doesn't like to 'pick winners' the scale can sometimes only be produced in industry.
	Defence industry is bound by legislative constraints that ensure goods are export controlled and secure. Industry would need to ensure it has a strategy to ensure legislation and the surrounding frameworks keep up with changes to technology to ensure there are no negative consequences. A failure to do so could lead to accidental breaches of legislation, and/or less secure use and exchange of technologies which can cause domestic, regional and international harm and/or frameworks that stifle research and development due to overly cumbersome controls.
	Increasing collaboration and standardisation of protocols for sharing data for safe operations – this is especially important in the space domain, which is very hard to work in. Space operators act mostly independently and at the rate of current growth of orbital objects this becomes vital for safety. A centralised and maybe even legally enforceable approach to data management and sharing.Embracing autonomy with varying levels of AI across C4I and operations across the different sub-domains in defence, viz. air, surface or space. Modern warfare is fast and is poised to become even faster as saturation attacks increase and autonomous drones are employed for attack.Fast adaptation to emerging technologies that have the potential to bring about radical changes in the defence space and may consequently make an organisation more competitive.Enhanced integration between sub-domains in defence, viz. Surface, air and space. This is already happening but will need to become more integrated as sensor technology advances.Re-looking at defence doctrine. As an example consider that most attacks in these times have been saturation attacks by a mix of projectile weapons. Rather than use expensive interceptors at the front line, using cheaper cruise missiles and other forms of missile defences act like pickets that let only the most serious threats in. Expensive interceptors can then be used deeper inside protected territory to destroy those left over missiles.
	A more flexible and agile pathway for the introduction of new-emerging capabilities.
	The pace of development of new technologies is rapid and to best prepare defence industry needs to be very agile in adaptation. There also needs to be the right level of risk appetite in relation to trialling and adoption of technologies.
	Highly mobile, able to pivot to support ADF in gaining equipment to front lines or even cutting edge equipment.
Defence need to bring Defence Industry closer, to understand the challenges being faced and the possible solutions required.We, Defence and Defence Industry, need to be actively part of the same team in the development of new technologies.Defence and Defence Industry also have to be better at understanding which technologies can get into the warfighters' hands in a timely manner, depending on the technology horizon and Defence risk appetite.Defence Industry has to improve collaboration pathways to improve commercialisation gains.	
1. Work with universities/government laboratories to appreciate the relevant technologies and to understand their maturity (i.e., TRL). This is critical to avoid optimistic views of when future technologies will mature.2. Use university student internship programs to spread the work among young graduates that your company is at the forefront of their field and so an attractive place to work. Use this as a stepping-stone to recruiting from this cohort, to ensure that the company has "young blood" as well as experienced technologists.	

Question:	What types of leaders would be required for advanced AI and software development in defence industry?
Response:	Innovated, motivational with a strategic understanding of Defence, its enemies and outcomes
	Lateral thinkers. People who aren't afraid to break things. People who follow the "if we've never tried it how do we know it doesn't work" path.
	Leaders don't necessarily need to know how the tools work, just be able to recognise the talents of their employees and empower them to succeed in their roles.
	Once that understand the warfighter need and are open to experimentation with new techniques. They have to learn to break things and be happy with small incremental failures. These are cultural attributes.
	Leaders who are flexible, have integrity (to ensure ethical considerations are addressed) and can develop / articulate a future state, draw a strategic line of sight to that outcome in order to plan and implement near term change for outcome achievement.
	From my experience the best leaders for this situation are those who are realistic about the capabilities of new tech. Promising that with a small amount of effort you can have an AI do some specific business process based on poor data is not helpful to the perception of the new tech or the industry. But being open about what is required and what the current ability of technology is (not everything is LLMs!) allows progress across the industry.
	Progressive, strategic and forward thinking. Also bold, and comprehensive leaders who can communicate effectively and inspire.
	AI is complex and a better understanding of its concepts, the latest advancements and of course the limitations of software in delivering the benefits coveted by AI technologies will make a leader better. Such leaders will be better positioned to take decisions about the development of technologies that can benefit defence.
	Leaders that better understand the environment within which defence operates.
	With rapid changes in any area it is important that leaders have sufficient knowledge and background to be able to make informed decisions. This doesn't mean being an expert in AI or software development, but it does require sufficient knowledge to understand both the opportunities and challenges. In my mind this requires leaders who have the time and capacity to undertake basic training in these areas.
	Leaders who can think outside the square. Leaders who are rock the industry who can develop solution which is totally left field.
	Leadership is a quality required regardless of the technology. A key attribute of a good leader of teams is the ability to develop the next leader. Leaders with qualities of: communication; integrity; adaptability; vision and creativity; and active listening are key attributes (probably many more, but a solid start).
	A leader with an engineering background, who has considerable experience in software and dealing with software engineers. This is critical, as there are three challenges: 1) software engineers need to have the real world abstracted into a software problem that they can solve. Otherwise, they are not good at analysing practical problems and so the software will be incorrectly specified, to the wrong design, and not suited to its purpose. 2) an ability to talk to software people in "their" language, recognising that this is at a level of abstraction different to the physical domain that most engineers are experienced in. 3) understanding that software engineers' perspectives are quite different, and so, at a human level, need more careful management than most other engineering disciplines.
	Researchers, leaders to be well versed in AI. Leaders need to understand both the human and business implications

Question:	Does current organisational structures support advancement in AI and software development?
Response:	The current organisational structure needs more forward thinking teams
	No. We are restricted by our security and global trade concerns, which are very valid. It's not an environment that will be easy to implement the new developments in.
	No. Although there are some shining lights in the organisation, it is too conservative to support the wholesale uptake of AI.
	Yes
	No, the traditional engineering, program, sustainment and governance organisational frameworks are not well suited to the more dynamic approaches needed for AI/SW work.
	I think the key to structuring teams will be to continue finding diverse talent that can work together to generate new ideas and approaches.
	Within the Government, No. Varies with industry.
	I believe more support is needed. The field of AI, though old has only started making advancements in recent years, in relative terms. Many aspects of the technologies have limitations or haven't been researched enough. More investment and funding is needed.
	Organisational structure cannot be rigid and must be willing to evolve within its sphere of operations and influence, what is good today may not meet the needs of tomorrow. This does not mean that whole scale change is necessary, that often causes unnecessary and disruptive upheaval, but rather that controlled, responsive and evolving change would provide the best outcomes. [Our organisation] will need to continuously evolve but has already shown a willingness to implement change.
	I don't have enough direct experience to be able to answer this well, but from what I do know, I would say no.
	Depends, if a tech company is advancing in AI, maybe. However, I believe some companies have structures in place but will need to constantly refine and update/develop to support the moving goal posts as this is a constant topic currently in Defence.

Question:	How does the role of leaders change with the introduction of emerging technologies?
Response:	When dealing with emerging technologies a leader needs interdisciplinary skills, innovation and a voice that's able to speak at various levels to influence partners of all levels to be open minded and forward thinking
	I think leaders need to encourage their people to bring solutions, ideas and new technology. Whether it can be done or not, leaders should always know about things that are out there. They don't change roles, necessarily, although I think new tech might be able to remove a lot of the admin from them. Imagine if AI could do expense reports and timesheets.
	Unless the workforce has been replaced by AI, it doesn't.
	Leaders must be flexible and consider both upstream strategic and downstream use. They should focus on client needs and measure the quality of new technology as it emerges. They should have a good understanding of integration and CI/CD pipelines which are the backbone of any good innovation program.
	Leaders are required to adapt to change in order to maximise and optimise the benefits of the new/emerging technologies
	Change management is a big part of leadership over the long term, so I would hope that good leaders would be able to take emerging technologies in their stride and continue to adapt processes and policies to keep pace.

Leaders need to ensure they remain agile, and keep in front of trends and technologies to ensure effective implementation and management. A focus on culture is increasingly important to ensure organisations adapt, but adapt in a manner that is compliant, secure and practical.

	Leaders will need to stay abreast of latest technological advancements to be able to chart the course of development forward in an informed manner. They will need to accept the challenges posed by new technologies and evolve accordingly and be capable of making data-driven or AI guided decisions. As complexities in AI and software increase, they will need to drive technological adoption and foster a culture of innovation with an increased focus on training and support for members of their organisation.
	The role of leaders does not necessarily need to change, leadership is about providing a pathway for others to willingly follow and contribute to a shared (organisational) vision.
	I don't think it does. All of these things are just tools. Leaders continue to have the same sort of role - they need to identify how these new tools relate to their area and support their teams in adapting to the use of the new tools
	Leaders need to have the foresight of this ground-breaking technology to help further develop such products to support overall outcome. Leaders need to go into such New Product Introduction activities with open minds and support others to continually push boundaries.
	Leaders may not be required to be experts in AI, but need to be aware of the science behind this technology in order to be brave and enable their teams to develop new technologies. Their role changes to encourage their team to learn and take risks to develop new technologies. Additionally, the ability to learn and innovate from other industries, to take these learning's and adapt them to Defence is a key attribute of leadership.
	The role is one of recognising how the emerging technologies, e.g., AI, will affect the teams that they are managing. Some engineers will be positive, many cautious, and some sceptical. Leaders must be focusing on how to bring these three groups into a common way of thinking. If this can be done then new technologies can be introduced while minimising the technical and organisational risk.

Question:	What changes are required to develop future leaders?
Response:	The Defence pathway to change and cultural reform - transformation of toxic work environments through a need to be coercive and succeed
	I think we have to move our mindset of "time served". Someone who was a great people manager in an organization selling kids toys would be just as great a people manager in a defence prime. Same skills. And just because someone is good at their job, doesn't mean they'd be good at leading humans. Completely different skill set. So I think a more open mind about the experience of people we hire. Yes we need technical skills, but it isn't technical skills alone that inspire people to stay with a company or make them happy to come to work.
	Awareness of changes in technology. Tools and support to embrace these emerging technologies, but also well-developed risk analysis to ensure high ROI decisions are made in the knowledge that identified risks are mitigated.
	I don't think the attributes of leadership needs to change, merely a focus on leadership styles which are flexible to rapid technical changes
	Development of methods to encourage and develop flexibility, outcome focus and being comfortable with change
	Recognition that with new technology like AI providing so much power to workers, the realisation that everyone will need to be a leader in some capacity. It's never a bad time to develop people's leadership skills.
	More focus on culture and fostering innovation and the organisational structures and frameworks required to support.
	An understanding of how control and decision making can shift when varying levels of autonomy are involved in decision making processes. Risk management strategies may have to change to manage how outcomes dependent on the introduction of autonomy (with respect to AI) change. Future leaders also have to be aware of the level of trustworthiness required from a system that can be given partial or full control of AI/software.
	More comprehensive and continuous formal leadership training throughout an individual's career.
	The opportunities I see them currently is the new generation coming through from schools and universities who would prefer to discuss/talk via texting people through teams and Skype instead of approaching people face to face. That is the difficult part in my current role is to get people actually communicating effectively is difficult. For future leaders it's a must have tool in your toolbox is high communication to gain high value outcomes.
Huge question. For organisations to look beyond qualifications - just because someone has an MBA does not equal leader. Ditto with PhD. Being able to transcend beyond this, to see through examples of on the job leadership to find, support and provide professional development opportunities for leaders is a great start.	

QUESTION SET 2: EMERGING TECHNOLOGIES IMPACT

Question:	How do you think AI will reshape Australia's defence industry?
Response:	Without a Human Systems Integration study AI may increase workload on Deployed Defence members however it can also provide a reduction in cognitive work loads - huge potential for the future
	Current AI lends itself to repetitive and structured tasks. Capabilities related to ISREW and cyber security, as well as tactical battlefield analysis will be (are being) revolutionised by these technologies. In these areas, defence industries is likely to become saturated by SMEs both inside and outside of defence. With very little current standardisation, many of these small organisations will likely boom or bust on the adoption of specific products.
	It will enable higher precision munitions, rapid decision making under uncertainty. For ADF it is a new tool they can leverage if they choose to be competitive
	In bursts, there are already proof of concept summarisation and RAG tools running in Defence, and it's reasonable to expect this will work its way into the existing technology infrastructure of Defence. But I doubt that it will vastly reshape what is ultimately a human organisation, not a technological one.
	Increased speed of complex decision making (tender evaluations, trade studies) Better integration of business systems eg ERP tools/applications Increased production automation
	I am not sure that anyone can predict how wide changing AI will be for all industry, defence is no exception. We are already seeing it used for simple tasks such as auto generated tech pubs, bid writing, but also for complexity such as automation in algorithm generation for EW, target recognition in BMS and sensor sorting, and self healing networks. I have no doubt it will permeate all parts of the industry.
	I think AI has the potential to assist in a more rapid and agile framework within which capability is developed and fielded within the ADF. This would require further enhancement of the collaboration between defence and defence industry.
	AI will bring about transformative changes in the defence industry by changing quality processes, assistance in certification, changing roles of humans vis-a-vis handling of technology, new requirements for data management and acquisition, improved collaboration between defence industry partners, especially in the space domain.
	AI is the one technology that can be a game-changer across the land, sea, air, space and cyber domains. Quantum technologies could too, but years of development are still required for quantum. Parallel to this, computational power will also scale to support AI capabilities. On board, cloud and distributed AI driven computational capabilities will drive autonomy across a range of Defence platforms. In the medical support area as well, AI will help support our warfighters with the next generation of sensors and wearables.
	Australia has a tiny, but expert and well equipped armed force. The only way to present a credible defence to a country such as China is to demonstrate massive improvements in productivity, to offset the scale imbalance. AI and autonomous systems are the means for achieving the required productivity, and thus capability.
AI's ability to drive innovation and efficiency can significantly impact Defence's long term long-term goals and competitive edge, leaders need to take the reins and ensure AI initiatives align with strategic vision and to maximise value. AI can help identify an area for development, which may have been overlooked with traditional means.	

Question:	Is Australia's defence industry prepared for changes in software development?
Response:	In years gone by Defence Industry has been lacking the vision to stay ahead of software development due to costs unless they change the approach then no
	Yes and no. Much of defence industry have already adopted agile development practices and understand the importance of these new technologies. However, many existing defence contracts are slow moving and monolithic, hampering industries ability to transition to new paradigms.
	Not yet. They are 5-10 years behind automation and agile development practices
	I think I said this before, but technology and software are all about change constantly. Different defence industry businesses and projects will have different levels of inertia to keep up with changes, which ultimately can be a benefit as different risk profiles can be applied to different projects. So, I think yes, defence industry is prepared, overall.
	I think the increased adoption of agile methodologies has helped to prepare industry for incremental changes
	Yes and no. We are never prepared enough, but due to resource constraints we will have to embrace at risk. Auto code generation is already prevalent, refining this and building smarts in the key inputs to auto generated code will be the differentiator.

	I think industry is maturing its understanding of how AI may be able to contribute to software development, my concern is defence's understanding of any potential second and third order effects in the outcome.
	Yes and no. Testing compliance standards exist and may prove to be adequate. Quality standards for software haven't evolved well over time. Australian defence contracts often have quality metrics and requirements that are derived from software standards that may not completely align with how newer technologies are shaping up. This is especially important in the case of AI models where the quality of training data, and design of models may not necessarily have enough metrics for compliance checks and quality certification.
	Yes and no. I think Defence Industry is a step ahead of the end user, Defence as it is risk averse by nature, and it takes time to adopt new technologies. That said, Defence Industry may not be at the bleeding edge of these technologies. While Defence Industry may have some time to develop a workforce as Defence slowly takes on new capabilities. I hope it takes this time to innovate, develop their staff, engage with universities to help them do this. Can Defence Industry democratise innovation, that is, enable all staff to contribute to innovation. You don't need to be in the R&D section of the business to innovate. Create a culture of curiosity and development. We need to push our (foreign owned) Defence Industry businesses to invest in R&D in Australia. CASG need to find a pathway to create innovation within their programs and contracts. Noting that there were "19 models of the Spitfire and 52 sub-variants being produced throughout the Second World War, and beyond". Is CASG ready for this 75 year old paradigm? If no, review and replace.
	I have limited knowledge, but unless defence industry is different from everyone else - no.
	Among small defence industry companies: generally yes. Among the primes: generally no.
	No, changes are happening rapidly need to be more reactionary

Question:	What changes do you feel would be required to adopt emerging technologies?
Response:	Planning and a vision, build software into the obsolescence package
	On top of broad changes to the current contracting model of Australian defence, a greater understanding of the commercial and licencing implications of AI technology is key. The introduction of tools such as ChatGPT have changed the architecture of the internet overnight, with significant content being locked behind pay walls to inhibit its use. This is an early indication of one of the key problems AI technology faces.
	DevSecOps platform, rapid acquisition programs, innovation-acquisition scouting
	Ultimately adoption is about having the technology's usefulness realised within Defence, which requires a joint understanding of the technology and of the problem domain, as well as the reality of deploying to the target environment. Defence is attempting to narrow the gap on the deployment front, some progress was made within CIOG FastPath for instance, though I'm not sure what has replaced that since the switch to JCG. The ASCA approach of DARPA-style missions should present the problem domains to industry in an accessible way, and allow industry's understanding of the technology, gained through internal R&D or higher-risk-appetite projects, to be applied in an integrated way with Defence.
	Security and cyber regulators would need to keep up with emerging technology assessments and approvals
	Risk appetite of industry and the government. We also need to be in a place we AI and emerging tech can be accredited for use by the defence sector to ensure cyber and security risks are addressed.
	A more forward leaning and collaborative relationship with defence as a customer. Industry also needs to better understand defence's operating environment from the strategic to the tactical in order to best employ emerging technologies when shaping solutions to meet defence's unique capability needs. To quote a former Chief of Navy, "Navy is in the business of executing the lawful will of government, up to and including the use of lethal force".
	Improvement of newer quality standards regarding AI models, quality and sufficiency of training data, test outcomes with data inadequacy. May also require establishment of newer standards for safety. Making sure different levels of an organisation up skill to keep up with newer technologies. This is a change higher management may have to drive.
	Culture change in Defence (it's happening, but slowly), including CASG. Pathways to collaboration, sponsored by Defence - the Services, ASD. Perhaps it is all via ASCA, then scale ASCA.
	Predominantly it is in relation to appropriate training for people at all levels - from a broad/high level understanding of the challenges and opportunities presented by AI and other emerging technologies, through to technical and operational training for on-ground personnel.
The ability to understand emerging technologies and to manage the technical, programmatic and financial risks that come with doing things for the first time.	

Question:	How can Australia's defence industry leverage AI to enhance our nation's Defence capabilities?
Response:	By understanding the concepts of Human - AI, Decision making, motion and creation against OEMs, Contractors, COTs and of course the end users in the Military
	Initial it will be to identify and demonstrate novel ways to use AI to solve capability problems that were largely impossible 5 years ago. Defence itself is grappling to understand how AI will impact them, industry needs to bring its expertise to bear to give defence the knowledge it needs to navigate the new technology.
	Too many ideas to answer, but all framed within autonomy, analysis of "fog of war", some EW applications, and automated decision making.
	Currently, AI is great at ingesting large amounts of data and summarising or highlighting individual pieces of information, this is likely the next thing to make waves through Defence. Already appearing in various tools is the MS Clippy-style AI that guides a human through some repetitive process that the model can learn patterns from. In future who knows? Studies show that athletes perform slightly better when more motivated, could LLMs be used to coach COs on motivation of troops, perhaps tailored to individuals by monitoring performance and behaviour? The range of possibilities is large.
	Design systems that are open to AI access, monitoring and control. Invest in AI centric simulation/prototype/ R&D labs to rapidly develop and evaluate conceptual designs.
	As stated above, start by taking out the non value add tasking that is very inefficiently done every time by humans then build on that model over time. Some run rules set by government would help, certified AI engines would also help early adoption.
	By developing and fielding capability in a more responsive and agile manner. And delivering capability that provides the warfighter with the knowledge edge over their adversary. Today's operators are suffering from information overload, they have little ability to assess and process all 'data' available to them in a meaningful and timely manner without 'computational' support.
	As an example, consider the following examples that have been observed in battle spaces recently:- GPS/ADSB spoofing prevalent- Saturation missile attacks are a new norm, defending against well-equipped enemies is proving to be difficult- Extensive EW capabilities on all sides As battle spaces become very complex advanced AI software and systems for distinguishing friend from foe, spoofed from real will be needed to help the existing military workforce in being effective. An enhanced speed of response with due consideration of costs in involved in autonomously determining the use of inventory for response against threats. Battlespace aspect design with trials and formulations for training and preparation for future battles and missions being planned.
	Engage and connect more with universities. Take on university students for internships. Sponsor PhD students (could be your staff), and collaborate on research projects. Invest in their staff through professional development programs, training and project opportunities.
	There are many established ways in which AI could be incorporated into systems to assist with decision making. There are also a range of more novel and innovative ways in which AI might be utilised in defence industry applications, these present the greatest opportunities.
Predictive analytics and ML can help uncover patterns and insights that inform better decision making.	

Question:	What collaboration efforts should defence industry undertake to prepare for advances in AI and software development?
Response:	Investments to the decision and motion making layers providing an understanding to the developers on how AI will enhance Lethality through Autonomy, threat analysis and Rules of Engagement
	Likely what it is best at, a healthy competition of technologies to grow our sovereign capability. Standardisation will likely also be key, but this is unlikely to be driven by defence industry (or even defence in general)
	DevSecOps + Cloud + Agile development. "Agile" here must include the warfighter / end user in the loop
	Most innovation in AI/software engineering is happening outside of Defence, so having cross-pollination between defence and non-defence projects is a good way to bring innovation from less-constrained environments in. At the same time to bring considerations from within Defence out to broader industry projects to guide research and development with principles that mean it can be applied into a Defence context more simply.
	Keeping the military personnel, end user in the loop, identifying their needs and helping them to see how things could be better. Need to increase sovereign content and local workforce for software maintenance. Need to identify appropriate use cases for AI to develop trust in emerging AI technology.

	Organise, participate in and sponsor AI conference(s) with Defence Primes, SMEs and Commonwealth agencies.
	Work together to build the principles of use and mechanics to utilise, the companies that crack this early will become market leaders quickly.
	Better integration of defence industry into the defence capability lifecycle.
	Promotion of development of standard operational procedures in the space domain that may gradually bring them up at par with the standards of operations in aviation. Standardisation of data formats for data that describes orbital objects. Collaboration to integrate data from many observation sources - optical, visual, ground and space based radar for accurate modelling of orbital trajectories.
	Partner up with innovative SMEs and universities. There are so many different grants available for companies to engage with universities and leverage their available funding. As above, take on interns, invest in PhD students, and collaborate on research.
	Some collaborators will have greater expertise and levels of exposure to AI and software development than others. Defence Industry needs to ensure that this is one of the strategic factors taken into account when identifying potential partners
	Close links with universities to understand the AI innovation and their advantages and risks. Also, close links with Defence customers to explain these, so that their expectations can be managed.

Question:	What changes in defence industry are required to support emerging technologies?
Response:	A better understanding of the motion layer through realistic simulation and investing in training
	Defence industry is driven by the demand signals from defence, so most real change will come from an overhaul to defence procurement. For industry itself, a greater emphasis on collaborative endeavours, especially in these emerging areas, will get the capabilities into war fighter hands faster.
	They need to fix their acquisition practices, which are old/slow/prone to anticompetitive practice
	Each organisation is going to have their own take on R&D and risk in that space. The more 'emerging' and further from 'stable' a technology is the greater the required investment and the risk along with that. Some organisations will put more of an emphasis on being the leader in certain technologies than others, and hopefully across the whole defence industry there can be enough bets that come off to keep the whole industry moving forward.
	Appropriate regulatory approvals (security, cyber) to allow implementation. Contracting mechanisms that allow for inclusion of low TRL subsystems into Mission Systems.
	A more collaborative and forward leaning relationship with defence is required to ensure the CoA remains an informed and responsible customer.
	Greater Investments towards Space Situational Awareness (SSA) technologies that aim to utilise available data and AI models and thus aid human operators, e.g. civil and military personnel tasked with monitoring jobs. Likewise for the air-domain situational awareness, especially when integrated with other domains. Investments towards new technologies that enhance trustworthiness in autonomous systems and software, e.g. XAI (Explainable AI), hybrid AI models.
	For foreign owned Defence Industry companies, the ability to self govern and lead in R&D efforts in Australia. And/or for these businesses to help connect across the US and UK (for example). Support from CASG and Defence to help you innovate.
	I don't know
	Increased emphasis on software innovation and software engineering (to manage this innovation). Employing new graduates who have already been exposed to the innovations and can communicate this to their managers.
We are a high labour cost nation. For us to be cost effective we need to be disruptive, not compete against replication or price but innovation.	

Question:	How can Australia's defence industry leverage AI to enhance our nation's Defence capabilities?
Response:	By understanding the concepts of Human - AI, Decision making, motion and creation against OEMs, Contractors, COTs and of course the end users in the Military
	Initial it will be to identify and demonstrate novel ways to use AI to solve capability problems that were largely impossible 5 years ago. Defence itself is grappling to understand how AI will impact them, industry needs to bring its expertise to bear to give defence the knowledge it needs to navigate the new technology.
	Too many ideas to answer, but all framed within autonomy, analysis of "fog of war", some EW applications, and automated decision making.
	Currently, AI is great at ingesting large amounts of data and summarising or highlighting individual pieces of information, this is likely the next thing to make waves through Defence. Already appearing in various tools is the MS Clippy-style AI that guides a human through some repetitive process that the model can learn patterns from. In future who knows? Studies show that athletes perform slightly better when more motivated, could LLMs be used to coach COs on motivation of troops, perhaps tailored to individuals by monitoring performance and behaviour? The range of possibilities is large.
	Design systems that are open to AI access, monitoring and control. Invest in AI centric simulation/prototype/ R&D labs to rapidly develop and evaluate conceptual designs.
	As stated above, start by taking out the non value add tasking that is very inefficiently done every time by humans then build on that model over time. Some run rules set by government would help, certified AI engines would also help early adoption.
	By developing and fielding capability in a more responsive and agile manner. And delivering capability that provides the warfighter with the knowledge edge over their adversary. Today's operators are suffering from information overload, they have little ability to assess and process all 'data' available to them in a meaningful and timely manner without 'computational' support.
	As an example, consider the following examples that have been observed in battle spaces recently:- GPS/ADSB spoofing prevalent- Saturation missile attacks are a new norm, defending against well-equipped enemies is proving to be difficult- Extensive EW capabilities on all sides As battle spaces become very complex advanced AI software and systems for distinguishing friend from foe, spoofed from real will be needed to help the existing military workforce in being effective. An enhanced speed of response with due consideration of costs is involved in autonomously determining the use of inventory for response against threats. Battlespace aspect design with trials and formulations for training and preparation for future battles and missions being planned.
	Engage and connect more with universities. Take on university students for internships. Sponsor PhD students (could be your staff), and collaborate on research projects. Invest in their staff through professional development programs, training and project opportunities.
There are many established ways in which AI could be incorporated into systems to assist with decision making. There are also a range of more novel and innovative ways in which AI might be utilised in defence industry applications, these present the greatest opportunities.	
Yes. See my answer to Q1	
Predictive analytics and ML can help uncover patterns and insights that inform better decision making.	

Question:	What collaboration efforts should defence industry undertake to prepare for advances in AI and software development?
Response:	Investments to the decision and motion making layers providing an understanding to the developers on how AI will enhance Lethality through Autonomy, threat analysis and Rules of Engagement
	Likely what it is best at, a healthy competition of technologies to grow our sovereign capability. Standardisation will likely also be key, but this is unlikely to be driven by defence industry (or even defence in general)
	DevSecOps + Cloud + Agile development. "Agile" here must include the warfighter / end user in the loop
	Most innovation in AI/software engineering is happening outside of Defence, so having cross-pollination between defence and non-defence projects is a good way to bring innovation from less-constrained environments in. At the same time to bring considerations from within Defence out to broader industry projects to guide research and development with principles that mean it can be applied into a Defence context more simply.
	Organise, participate in and sponsor AI conference(s) with Defence Primes, SMEs and Commonwealth agencies.

Response:	Work together to build the principles of use and mechanics to utilise, the companies that crack this early will be market leaders quickly.
	Better integration of defence industry into the defence capability lifecycle.
	Promotion of development of standard operational procedures in the space domain that may gradually bring them up at par with the standards of operations in aviation. Standardisation of data formats for data that describes orbital objects. Collaboration to integrate data from many observations sources - optical, visual, ground and space based radar for accurate modelling of orbital trajectories.
	Partner up with innovative SMEs and universities. There are so many different grants available for companies to engage with universities and leverage their available funding. As above, take on interns, invest in PhD students, and collaborate on research.
	Some collaborators will have greater expertise and levels of exposure to AI and software development than others. Defence Industry needs to ensure that this is one of the strategic factors taken into account when identifying potential partners
	Close links with universities to understand the AI innovation and their advantages and risks. Also, close links with Defence customers to explain these, so that their expectations can be managed.
	Keeping the military personnel, end user in the loop, identifying their needs and helping them to see how things could be better. Need to increase sovereign content and local workforce for software maintenance. Need to identify appropriate use cases for AI to develop trust in emerging AI technology.

Question:	What changes in defence industry are required to support emerging technologies?
Response:	A better understanding of the motion layer through realistic simulation and investing in training
	Defence industry is driven by the demand signals from defence, so most real change will come from an overhaul to defence procurement. For industry itself, a greater emphasis on collaborative endeavours, especially in these emerging areas, will get the capabilities into war fighter hands faster.
	They need to fix their acquisition practices, which are old/slow/prone to anticompetitive practice
	Each organisation is going to have their own take on R&D and risk in that space. The more 'emerging' and further from 'stable' a technology is the greater the required investment and the risk along with that. Some organisations will put more of an emphasis on being the leader in certain technologies than others, and hopefully across the whole defence industry there can be enough bets that come off to keep the whole industry moving forward.
	Appropriate regulatory approvals (security, cyber) to allow implementation. Contracting mechanisms that allow for inclusion of low TRL subsystems into Mission Systems.
	As stated above
	A more collaborative and forward leaning relationship with defence is required to ensure the CoA remains an informed and responsible customer.
	Greater Investments towards Space Situational Awareness (SSA) technologies that aim to utilise available data and AI models and thus aid human operators, e.g. civil and military personnel tasked with monitoring jobs. Likewise for the air-domain situational awareness, especially when integrated with other domains. Investments towards new technologies that enhance trustworthiness in autonomous systems and software, e.g. XAI (Explainable AI), hybrid AI models.
	For foreign owned Defence Industry companies, the ability to self govern and lead in R&D efforts in Australia. And/or for these businesses to help connect across the US and UK (for example). Support from CASG and Defence to help you innovate.
	I don't know
	Increased emphasis on software innovation and software engineering (to manage this innovation). Employing new graduates who have already been exposed to the innovations and can communicate this to their managers.
	We are a high labour cost nation. For us to be cost effective we need to be disruptive, not compete against replication or price but innovation.

Question:	What are the implications of AI into Defence?
Response:	AI in many cases will challenge the warfighters ethics, taking away the ability of being the 'final' decision maker and trusting the equipment and software
	Likely similar to the broader world. Less reliance on labour for tasks AI excels at, a hunger for more data. The battle is already fought at machine speeds, AI will make this more so. As AI is brought into decisions loops, the ethical concerns of the technology will become more prevalent, and this is likely to make or break the strategic advantage.
	AI and Space both. Space is a new domain, AI is a series of techniques. Implication is the pace of innovation is far outpacing the pace of their acquisitions systems
	Need-to-hold, need-to-know, imperfect responses, lack of operator understanding.
	The ability to ingest and process vast quantities of data very quickly, for things like target identification in camouflaged/cluttered environments (eg undersea mine identification). Implication of potential loss of human control in decision making.
	With use of AI comes trust, the model is only as good as the data it injects, this works well for data sources that are in the public domain. But for defence we have classified data with various caveats along with commercial in confidence. How do you aggregate this to not share commercial and country security details, how do you work cross domain, is the AI engine at the highest classification. Very complex data problem. Also if an AI makes a decision who is legally responsible for the outcome, the AI, the company that used it, the country that used it or the human with the "tool"
	The potential to remove the human from the decision-making loop when employing warfighting capability could have a significant impact on defence's legal responsibility to only employ warfighting capability domestically (e.g within established ROE) and internationally (e.g. within the recognised LOAC framework).
	Enhanced productivity and innovation, especially in the field of decision making and mission planning. Increased shift towards autonomy where there can be an incremental loss of authority of the user. Stringent data security requirements as its use becomes more vital in decision making. Change in roles of human operators from, say monitoring and designing, to, prompting AI models to achieve a desired military goal. Increasing emphasis on explaining and inspecting of decisions made by AI systems that can have far reaching impact.
	AI has the potential to be all invasive and supportive across Defence. Keeping our AI cyber safe is key.
AI implications into Defence are quite profound, as they are across a range of sectors. In defence they are perhaps even more important - in particular autonomous systems and decision making because of the nature of defence related work.	
Improving performance, removing humans from high-threat environments, reducing capability costs and achieving asymmetric advantage. Take high cognitive load off of human operators.	

Question:	What are the environmental responsibilities with the adoption of AI in the defence industry?
Response:	One of the key emerging AI technological advances has been to reduce the carbon footprint during climate crisis
	Difficult to say just yet. One could argue AI will breed efficiency, and therefore reduce wastage and improve environmental impacts. Possibly too early to tell.
	All Australian businesses need to work together to reach the Government's goal of carbon neutrality by 2050. It's no secret that AI uses a lot of compute hardware, which requires a lot of resources to create, and also a lot of energy to run. Estimates from the IAE project the global AI energy consumption could reach 1000 TWh in 2026, roughly the electricity consumption of Japan. Australia currently produces 250 TWh per year
	AI decision-making should factor in priorities such as environmental impact, which may not be quantifiable in convention or monetary terms.
	I would suggest this maybe an advantage, as less human power is required. However the increase in data centre and high levels of computing power would clearly have an environmental impact.
	No different to the responsibilities defence or defence industry has with any other capability. Both must operate with the legal framework provided by domestic legislation and by international law and treaties. I think there is a moral obligation on industry to be a responsible citizen too, but that is a more nuanced conversation that is difficult to answer here.
With increasing levels of autonomy in defence there will be an incremental loss of authority so the repercussions of autonomous decisions can be dire and expensive. A responsible use of AI is possible with implementation of safe guards and checks in the form of explainable and inspectable AI that also allows humans-on-the-loop to help override decisions as appropriate.	

	AI chipsets will generate higher levels of heat. There are waste heat recovery technologies available to take this heat and reuse it, store, or to generate energy. Being aware of these technologies is critical for environmental purposes.
	The main environmental consideration with AI is the power usage for things like LLM. At the moment these are very energy intensive how and where Defence uses AI will impact this.
	In the case of LLMs in particular, managing the energy required to run the large computational facilities required.
	Need for high computing power, energy consumption.

Question:	Is there a concern of over-reliance of AI in Defence?
Response:	Ethics - the over reliance of AI in Defence without proportionate levels of oversight and human judgement can or could pose very real risks such as ethical dilemmas or a loss of control in the battlefield causing untold Political back lash
	Yes and no. Defence will likely be slow to adopt AI technology (at least initially), but because the technology isn't well understood, it is often seen as the silver bullet. Even in areas where it excels, this is certainly overselling at least current day AI technology.
	Concern? Not yet, it's too early in practice, ask again in 5-years when AI becomes a bit more in-use in practice by warfighters
	Not from me, I think Defence is appropriately but painfully cautious about new technologies, and people will require convincing and training before any operationalisation of these technologies.
	Yes, a framework for human interaction and control over AI should be developed so that autonomous systems do not go open loop.
	Yes, as with the increase in complexity we see today, the technical mastery of our ADF and industry personnel cannot keep up, the same with AI, we potentially run the risk of creating Dumb soldiers that cannot think with out the aide of the AI engine, resulting in panic in the battlefield when AI fails.
	I think there is a warranted concern in defence over the introduction and use of AI in operational and tactical applications, but I don't feel this is unreasonable. The risk of removing the human from the decision-making process when it comes to warfighting activities should always be at the forefront of mind, this will hopefully lead to a more responsible use of AI capabilities.
	It is a distinct possibility. However, this concern or risk can be mitigated through the safe development of technologies and supported through research, and vigorous T&E processes prior to adoption.
	A degree of concerns on over-reliance is always healthy, but there will be a need for significant use of AI systems to assist with decision making and data fusion.
No, rather appropriate use, and far greater knowledge of AI, so that informed decisions are made.	
Yes as it could lead to a decrease in essential human skills and capabilities, however it needs to be understood that it can't fully ever replace human interaction.	

QUESTION SET 3: INTEGRATION AND RISK MANAGEMENT

Question:	What are some of the risks you can think of in the introduction of autonomous systems and weapons in Defence?
Response:	In a contested Battle Zone consisting of more than two allied forces then interoperability between systems if disparate and non interoperable could result in fratricide given the inherent brittleness of algorithms
	friendly fire due to identification errors, civilian casualties, target spoofing
	Removing the human element of decision making in the application of warfare that is by its nature designed to harm other humans.
	How faithful (trustful) machine's decisions, and verifying and validating that aspects in real world conditions.
	Lack or inadequacy of explainability of (safety-critical) decisions made by autonomous systems and weapons, thereby reducing the trustworthiness of such systems. Inadequate processes and standards around the testing, deployment and certification of such systems. Delays in introduction due to the time it may take to earn the trust of such systems by human experts. Managing the sometimes huge data requirements autonomous systems need for proper development and deployment. Getting access to datasets is another challenge. Mitigating side-effects and short-cuts taken by AI employed in autonomous systems.

	Reliance on AI/machine-based decision making, loss of human control and accountability, introduction of machine-made errors and insufficiently tested edge cases, potential for reduced accuracy due to insufficient prediction algorithms, lack of sufficiently diverse data sets for inference and machine-based identification purposes, risks posed by incorrect/malfunctioning system performance, potential for AI/machine learning to train on false positives without detection until an error is made.
	False positives and True negatives are always possible with any autonomous system, but in the Defence systems and weapons context these can be particularly impactful. Decisions need to be made before hand what level of each of the above is acceptable in an operational environment and ensure that realistic training situations can be created to establish and test that compliance.
	I think the greatest risk is NOT introducing them. Our potential adversaries are implementing these technologies and to help protect our personnel, this technology will be required. By being an autonomous system, we should be able to reduce the number of personnel from front-line activities in the future. Additionally, while the ADF regulate the implementation of robotics and autonomous systems (RAS), I would like to see that the level of autonomy could be increased or decreased depending on what the opposition is doing at that time. Put another way, if the opposition is using RAS in a non-legal way, then we should be able to switch on RAS to help get our crew get out of harm's way.
	1. Sovereign risk; if the software is developed outside Australia and cannot be modified here. 2. Explainability: why is the autonomous system doing what it's doing? 3. Safety and safety assurance: how do we assure AI and autonomous systems?
	Unpredictability in actions, human distrust in the systems

Question:	What risk management strategies should we undertake to manage the introduction of autonomous systems and weapons?
Response:	risk management needs to fall under the following sub headings - Moral Responsibility, Semantic Gap, Resolving uncertainty and understanding behaviour all of which affect the front end users in the Military
	layered abstractions, human in the loop for strategic decisions, cyber protections, limiting use cases based on risk vs reward vs "demonstrated technical capacity"
	The risk strategies are already in place, its about applying them in a responsible and considered manner.
	Verification and validation of the autonomous aspects, Building operators' trust towards the AI systems
	Careful implementation of XAI (Explainable AI) that can be use to engender trust in autonomous systems, where a system may keep a human on the loop, rather than in the loop, where a system could be queried and audited about how it arrived at a decision, what assumptions were made, analysis results, inspection of data utilised or excluded. Extensive testing and simulation before and during deployment with updated standards that have been reviewed and re-crafted keeping in mind the nature of autonomy involved in the conceptual requirements of a system. Through evaluation of goals imparted to systems, implementation of human oversight and intervention in design right from the start. Avoiding discrepancies between datasets used during development/testing and deployment.
	Appropriate policy and legislation needs to be developed at the same time as the development of AWS to help ensure appropriate consideration is afforded to assurance and accountability of such systems, personnel should be trained in the operation and understanding of said systems, and human-in-the-loop overrides should ALWAYS be available and appropriately secured. Rigorous system maintenance, updates, and testing should occur to ensure systems remain highly functional, accurate, and without conditions that could cause erroneous operation.
	Well established training protocols and systems, along with as much independent oversight as can be allowed.
	Surveillance and intelligence gathering of our potential adversaries of the RAS and AI technologies under development and in use. Teaching and deployment in the safe use of RAS in military contexts. Worth reading: https://researchcentre.army.gov.au/library/occasional-papers/understanding-how-scale-and-accelerate-adoption-ras Site visits to Australian mining sites such as Fortescue Metals Group (FMG) in the Pilbara to see, first-hand complete work-sites devoted to autonomy (100+ autonomous mining vehicles), with the addition of off-site operations management (at Perth).
	1. First, an informed customer, who knows what they are asking for, and the risks. 2. A well-managed agile development strategy, that ensures the software is appropriate for the requirements, and the risks fully understood. 3. A safety assurance approach that is flexible and appropriate to the risks. An inflexible safety assurance and regulatory environment will cripple the development of autonomous systems.
use of autonomous systems will not change the current doctrine. The risk strategies which apply to manned systems apply to autonomous systems.	

Question:	What changes is the defence industry required to undertake to support the greater integration in autonomous systems and weapons?
Response:	Prioritise research, development and experimentation utilising SME's in all areas
	experience operationally, proper DevSecOps in software pipelines
	A better understanding of the nature of defence business at all levels; strategic, operational and tactical.
	Integrated closely knitted researcher, engineer and operator collaborative environment.
	Establishment of proper channels between government bodies and industry participants for easy and quick access to datasets that are required in the integration and deployment of such systems. Processes to share and collaborate the use of datasets originating from defence industry participants. Harmonising data formats from different sources involved in integration systems.
	More training in the field of AWS and the policies and legislative concerns surrounding the field, open channels between Five Eyes and other allied nations for purposes of data collection, information sharing, identification, and other use cases to ensure more accurate, reliable, and effective systems.
	With Defence, the development of RAS autonomy test sites. Note Fortescue example above about the technologies required to undertake this. Invest more R&D of RAS and AI technologies. Development of coding standards for RAS and AI technologies to support interoperability (at scale). Onboard, cloud and fixed AI computational capabilities across Defence to support RAS and AI at scale and across land, sea, air and space platforms.
Much stronger emphasis on software and working with universities to fully understand the risks associated with software and managing these.	
trust, how much are we willing to trust in the system? We are a small defence force we need Autonomous systems to increase the combative masses. Autonomous systems are most commonly deployed in situations, which are dull, dirty and dangerous, situations where human lives would be in danger.	
Question:	What are the concerns related to potential ethical dilemmas with the integration of autonomous systems and weapons into Defence?
Response:	AI bias and technical autonomy can weaken the moral bias of operators
	as above, robotic vision recognition systems are pretty good for low risk scenarios. Not sure I trust an automated weapon systems for cases where friend or foe are unknown. They dynamics of warfare and competitive pressure will use this as a point of leverage in warfare.
	See answer to Q1. The removal of humans from the decision making loop.
	Whom to take the responsibility in decisions actioned by an autonomous system
	Due consideration of possible collateral damage and how, if at all, it was evaluated in relation to other options before a decision was arrived at by an autonomous system. Whether the datasets used in design incorporated human factors associated with outcomes of such systems.
	How much, why, and how comfortable we are with reducing/removing human decision making in the context of war and peace-time decisions, the ability/inability for AWS to appropriately apply sensitive decision making strategies such as reducing human harm and adopting non-lethal approaches/conservative identification where appropriate.
	The primary one would be an AI system which in an unanticipated and untested scenario arrives at a decision which most human operators would not
Not having RAS integrated poses the ethical and real risk of sending our personnel into combat with asymmetrical disadvantage. It would be an asset to have the ability to switch up and down the levels of autonomy on platforms depending on the situation to allow for ethical implementation and personnel safety. Vigorous T&E of our RAS and AI systems is required to support integration.	
In simple terms: avoiding Blue-on-Blue and Blue-on-White, and ensuring that the autonomous behaviours respect the current Rules of Engagement.	
Human aspect is taken out of the loop	

Question:	What actions does the defence industry need to take to address ethical dilemmas?
Response:	Research
	Testing, training, CONOPs development to better understand and quantify these risks
	Ensure defence is an informed customer. This could be achieved through more integrated introduction into service and sustainment processes between the parties, i.e. the OEM has a through life responsibility and stake in capability it provides to defence.
	Incorporate a globally accepted ethical framework for verifying the compliance to human ethics.
	Explainable AI, human-on-the-loop type of involvement right from the start - conceptualisation and design through to integration and deployment. Testing and verification methodology involving extensive simulations that assess collateral damage and other human factors.
	Consult user groups, Defence, the public to appropriately gather information related to sentiment around AWS, educate, inform, and train people in the use-of, and use-cases for AWS and openly discuss the pros and cons of the approach, as well as the limitations, safeguards, and open questions about emerging technologies, collaborate with allies to share best-practice approaches to common solutions to ensure high-quality systems are developed.
	Establish guidelines as to what level of "mistake" for systems are acceptable and ensure testing and systems to achieve that.
	Training in ethics to understand the challenges of implementing or not implementing RAS and AI technologies. Leadership at the highest levels to understand and support the ethical implementation of RAS and AI technologies.
The Ukraine has shown these to be less of a concern than might have been expected, due to their widespread use of aerial and maritime drones.	
As with any technology need appropriate boundaries to make sure unwanted behaviour is avoided.	

Question:	Is there anything else you'd like to comment, in relation to the above questions?
Response:	When it comes to conflicting scenarios, how can we ensure the adversary will be ethical?
	I think this is a very well thought out topic, and extremely pertinent to the current Defence landscape. These are the questions we should be considering, and while some of them may remain unanswered in their entirety for some time, it is important that the discussion remains open and alive in the meantime so that we can be best informed as we progress AWS technologies.