

# Trust, ethics, data privacy and cybersecurity – challenges for Defence R&D and innovation

Dr Sanjay Mazumdar  
Executive Director

A COLLABORATIVE PARTNERSHIP BETWEEN



Supported by



Australian Government  
Department of Education



## Australia can do a better job of commercialising research – here's how

Published: May 3, 2018 1:58pm AEST

A tax incentive coupled with a new fund to support research translation could go a long way toward closing that gap in funding imbalances between medical and non

Email

Twitter

Facebook

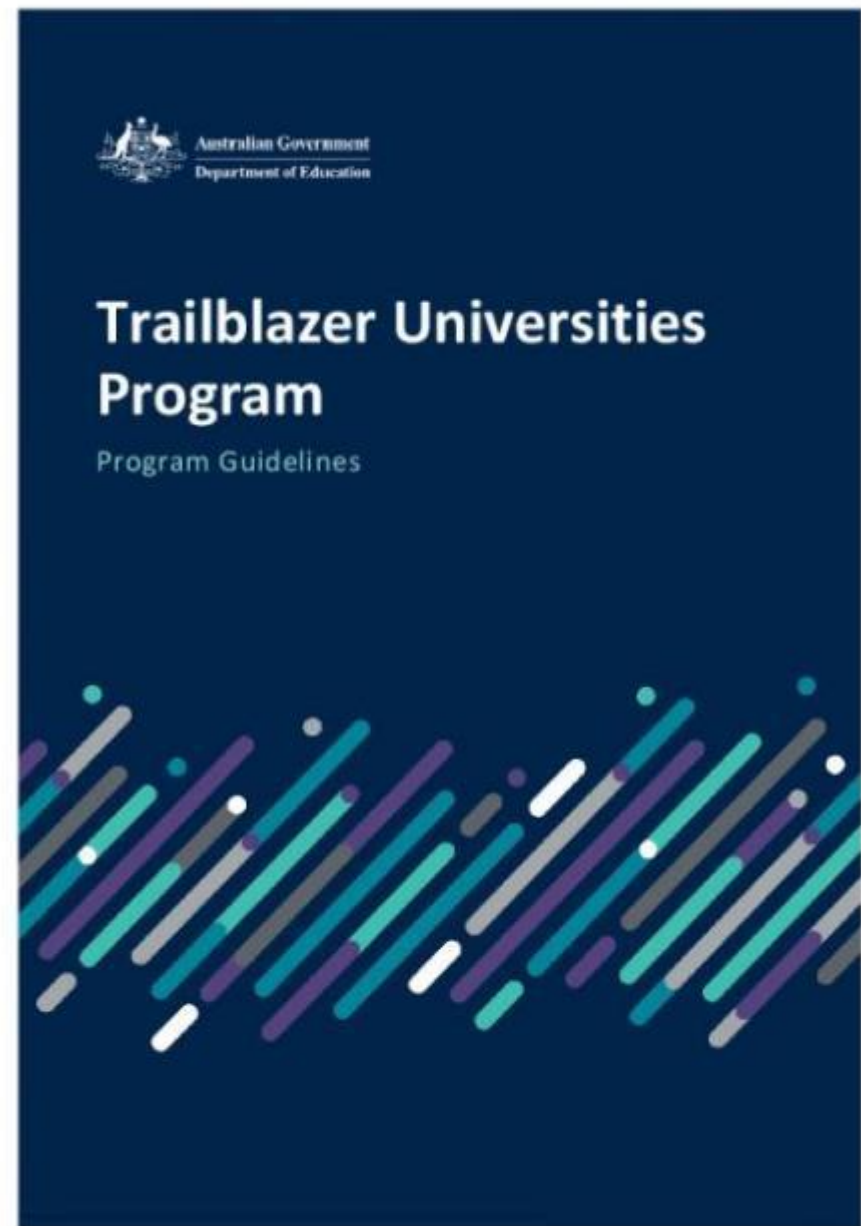
LinkedIn

Print

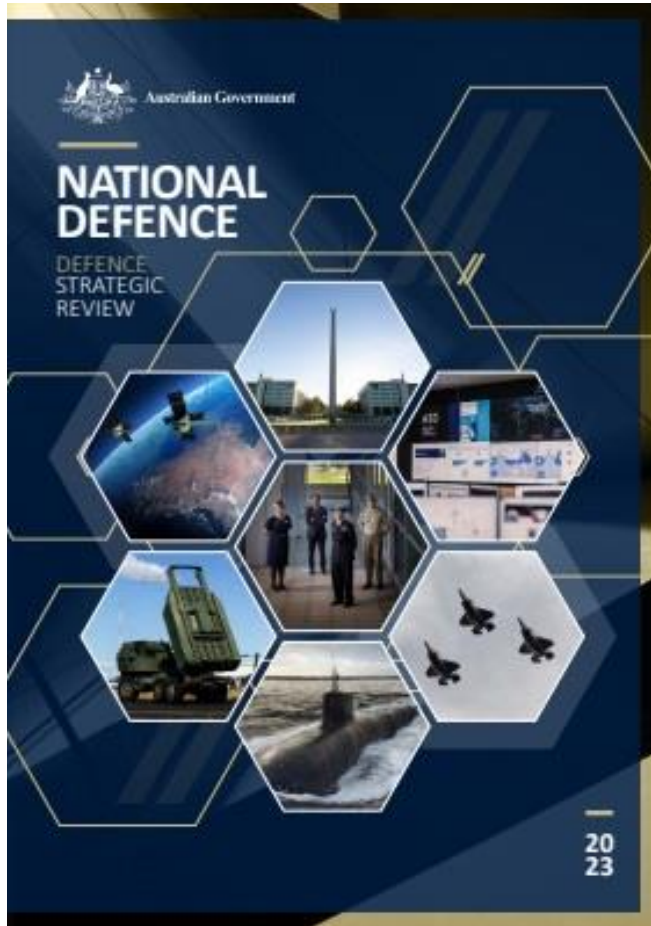
14

55

Australia can benefit much more than it does currently from the world-leading research in our universities. It ranks near the top of the OECD for research excellence but is less effective at collaboration between industry and researchers to drive the economic benefits of research. I suggest two important measures that could go a long way to achieving more translation of research to achieve



# A changing defence landscape



*The strategic demand for Defence's capability innovation systems has never been higher. Defence must have a national science and technology system that enables the development of disruptive military capabilities, including harnessing advanced and emerging technologies to provide asymmetric advantage for the ADF. (DSR report)*

*"The Defence Strategic Review makes clear that Australia **must invest in the transition to new and innovative technologies** for our Defence Force"*

Deputy Prime Minister Marles, Defence Minister

# Transforming Defence Innovation



## VISION

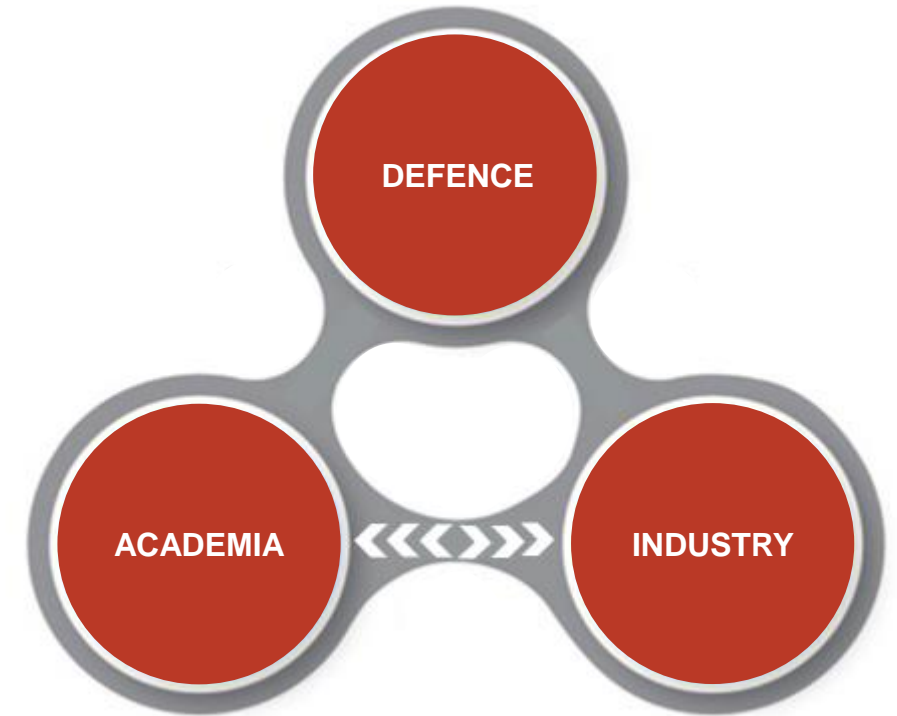
An exemplar for defence-industry-university partnerships accelerating the delivery of sovereign capabilities to the ADF.



## MISSION

Through an enhanced defence, industry and university partnership, we will:

- Trailblaze an entrepreneurial and innovative ecosystem maximising the value of IP and research translation;
- Skill the workforce of today and shape the workforce of tomorrow; and
- Accelerate the delivery of sovereign capabilities for the nation's security and prosperity....at-speed and at-scale.



# 41

## INDUSTRY PARTNERS



**31** SMEs

**10** primes

## FUNDING SOURCES

(cash and in-kind)



Industry



Grant



UoA + UNSW

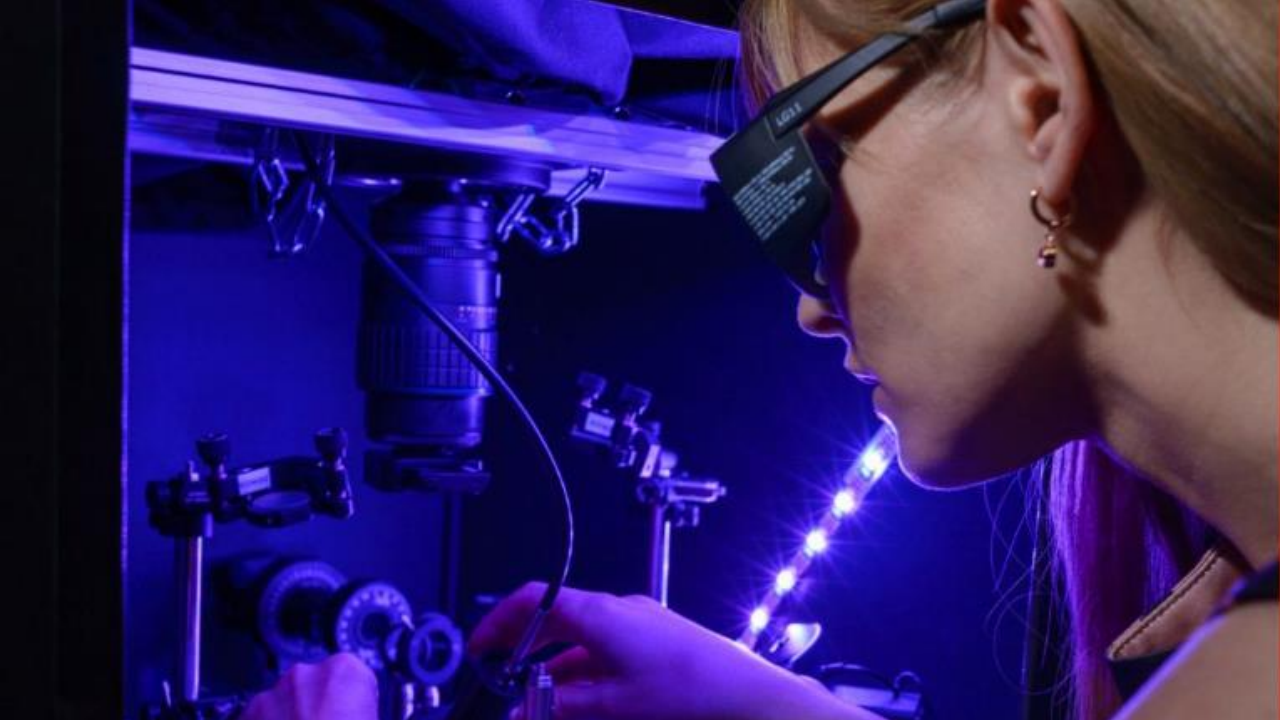






## Workforce, Innovation & Culture

Skilling the workforce of today and shaping the workforce of tomorrow, supporting the acceleration of ideas into commercial application, and promoting a culture of collaboration between industry and academia.



## Technology Development & Acceleration

Accelerating the translation and commercialisation of leading-edge defence technologies and solutions across the following key priority areas:

- Quantum Materials, Technologies & Computing
- Information Warfare & Advanced Cyber Technologies
- Defence Space Technologies
- Defensive Hypersonics & Countermeasures
- Robotics, Autonomous Systems & AI



# Sample of potential DTB projects

- Development of space-based optical links for distributed quantum networks
- Laser-based systems for defeating hypersonic threats
- AI and machine learning-enabled approaches for robust and adaptive control of hypersonics weapons
- Combatting vulnerabilities caused by the use, misuse and 'weaponisation' of information
- Multi-domain sensing and situational awareness for C2 for autonomous agents
- Space based ISR and Space Domain Awareness

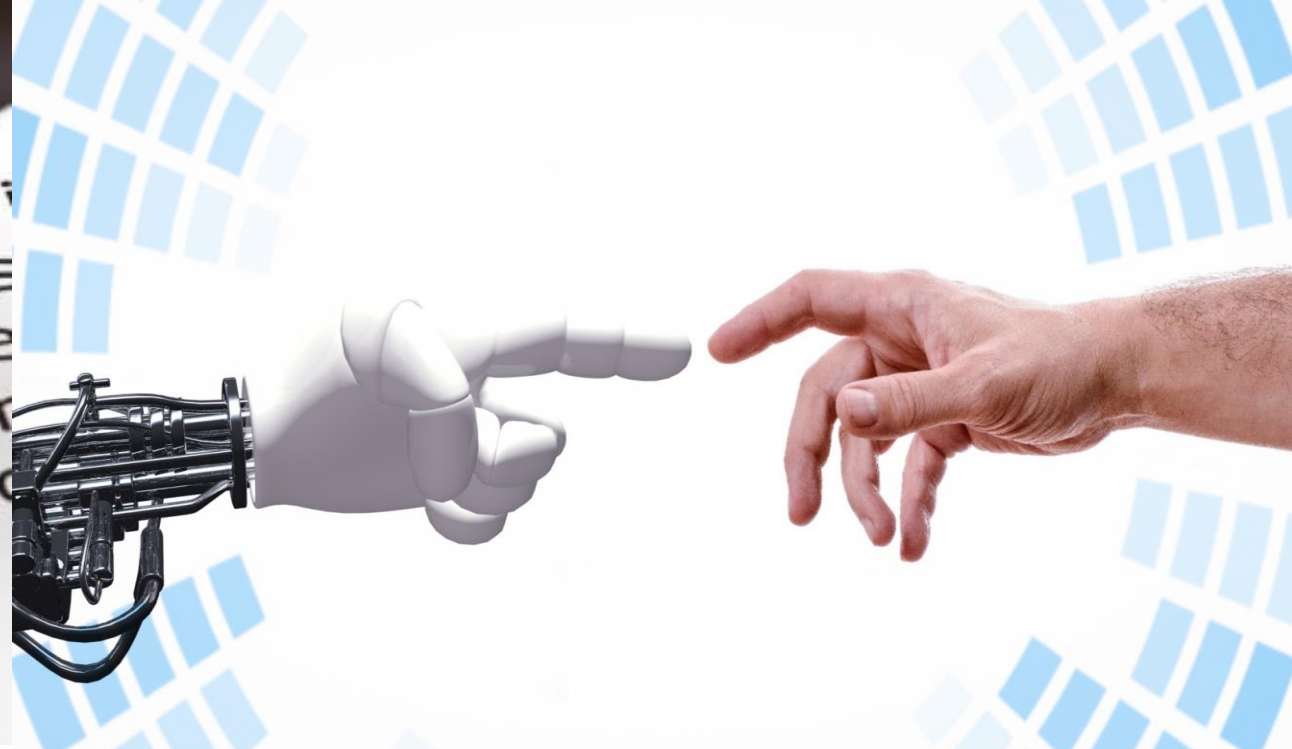


Credit: ASPI





Senex Energy



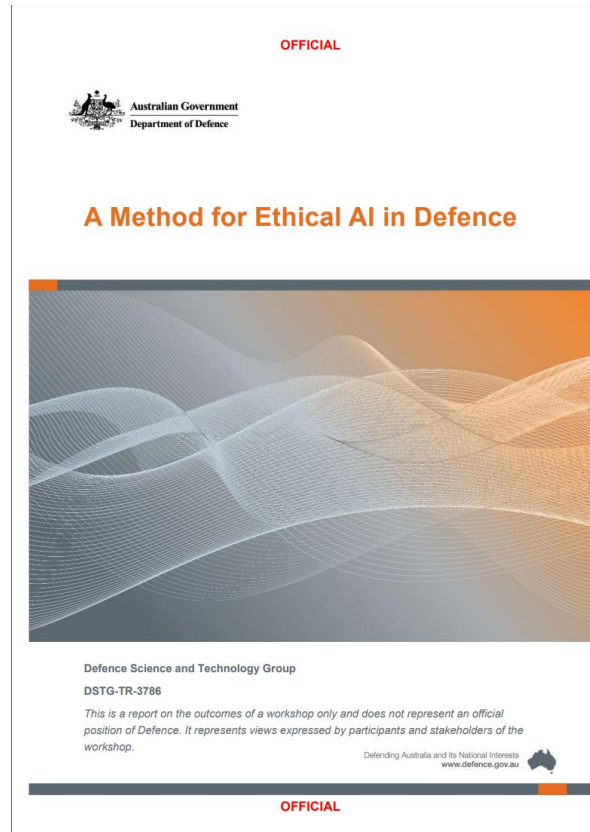
<https://www.keepsolid.com/blog/life-hacks-on-how-to-browse-the-web-privately/>

# Trusted and ethical use of AI

- Method for Ethical AI in Defence (ADF)
  - Responsibility – who is responsible for AI?
  - Governance – how is AI controlled?
  - Trust – how can AI be trusted?
  - Law – how can AI be used lawfully?
  - Traceability – How are the actions of AI recorded?

AI is becoming a “weapon of statecraft.... this tech future may accelerate truth decay” - General Angus Campbell, CDF

"AI is going to change many things about military operations, but nothing is going to change America's commitment to the laws of war and the principles of our democracy," SecDef Lloyd Austin





# ISO/IEC FDIS 42001

Information technology — Artificial intelligence — Management system

## General information

Status : Under development

Edition : 1

Number of pages : 51

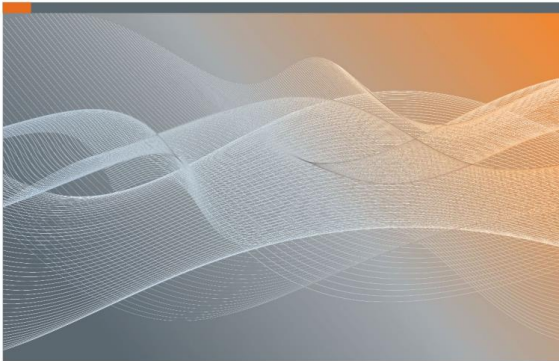
Technical Committee : ISO/IEC JTC 1/SC 42 Artificial intelligence

ICS : 35.020 Information technology (IT) in general | 03.100.70 Management

OFFICIAL



## A Method for Ethical AI in Defence



Defence Science and Technology Group  
DSTG-TR-3786

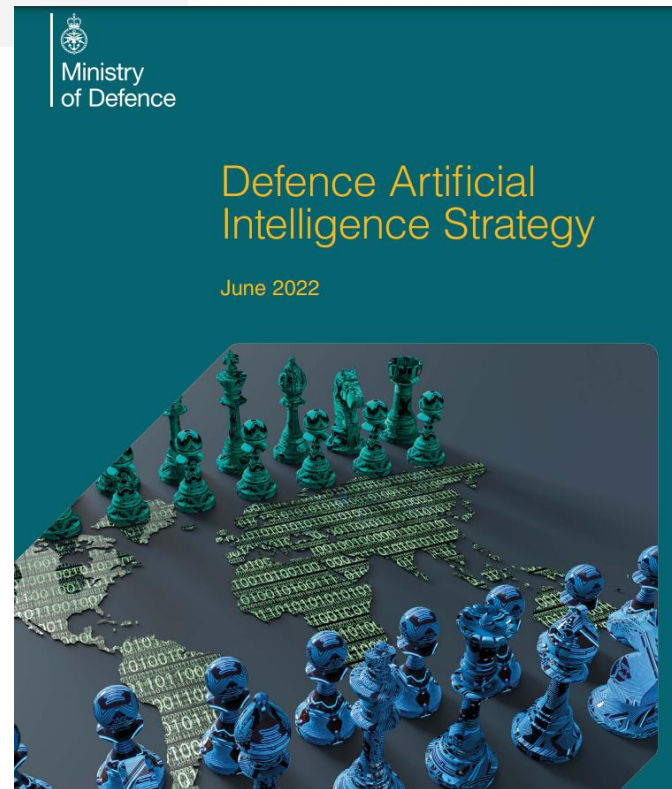
This is a report on the outcomes of a workshop only and does not represent an official position of Defence. It represents views expressed by participants and stakeholders of the workshop.

Defending Australia and its National Interests  
[www.defence.gov.au](http://www.defence.gov.au)

OFFICIAL

ISO/IEC FDIS 42001 is a process for evaluating whether AI use and development is being done by an organisation responsibly.

Standards Australia's AI Standards chair Aurelie Jacquet calls it the "crown jewel" of AI standards. – Innovation Aus

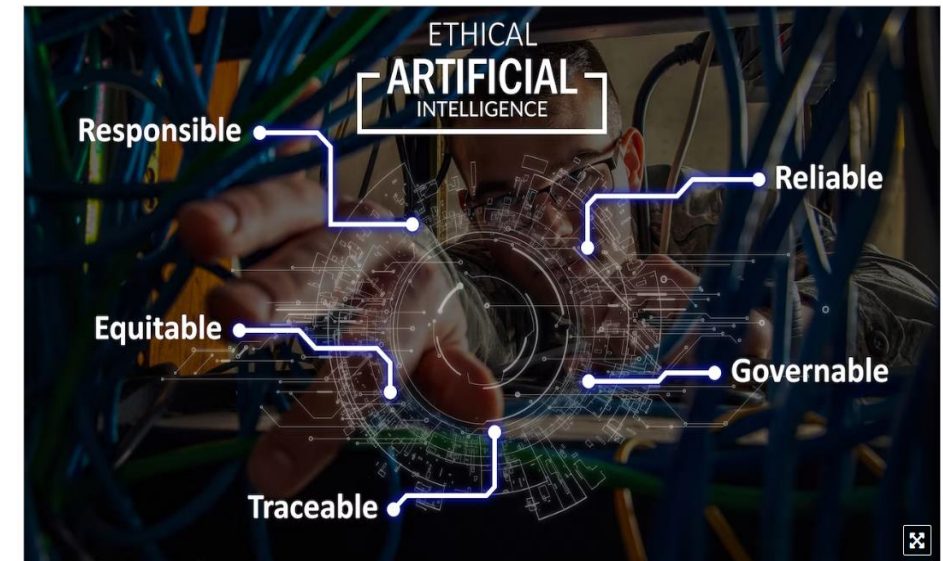


## DOD Adopts 5 Principles of Artificial Intelligence Ethics

Feb. 25, 2020 | By C. Todd Lopez, DOD News | f t p

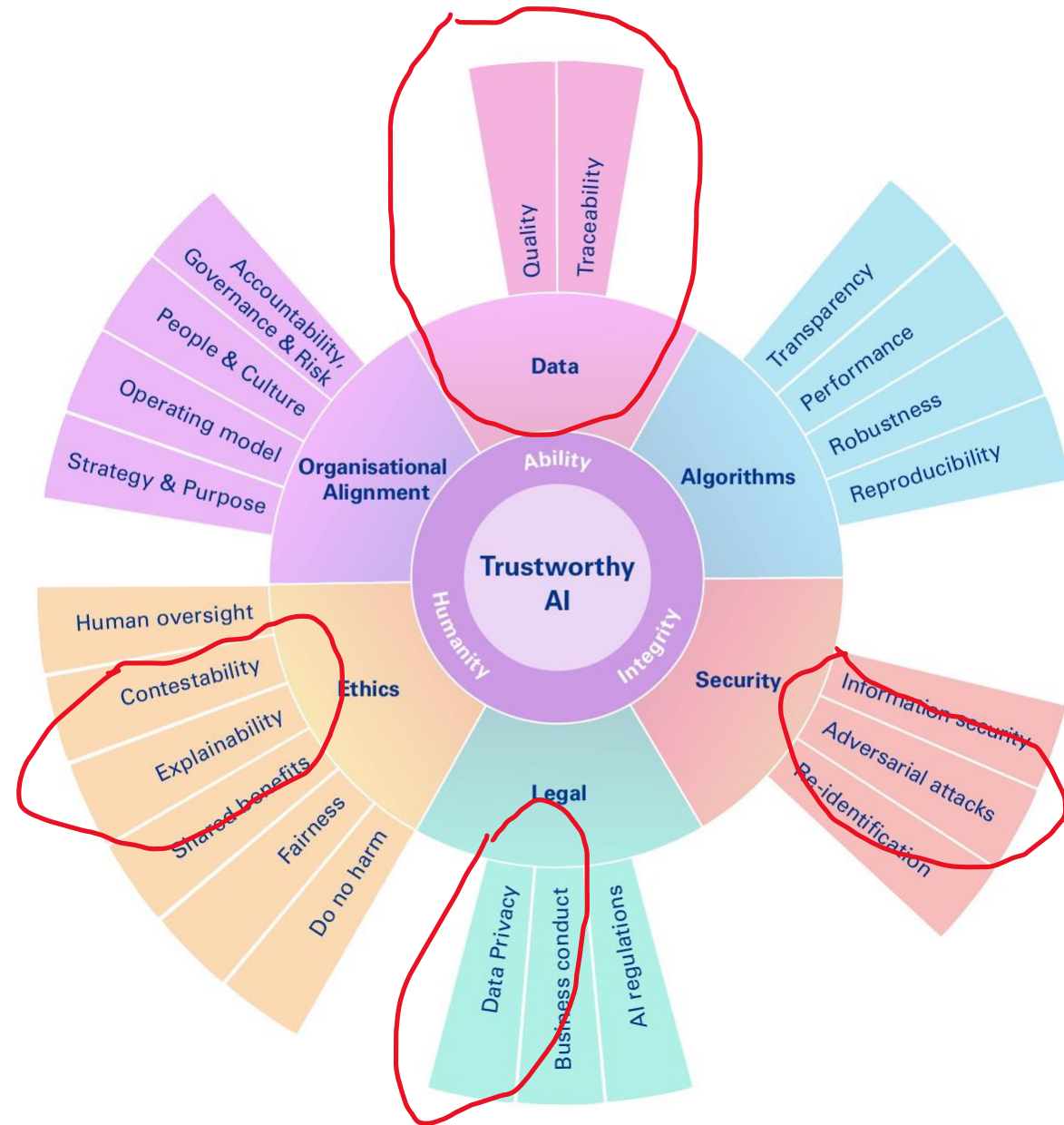
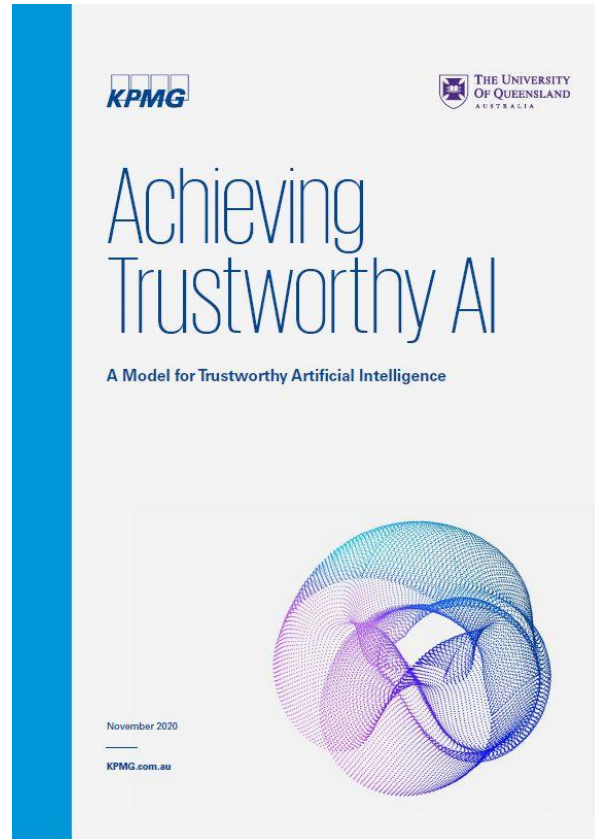
You have accessed part of a historical collection on defense.gov. Some of the information contained within may be outdated and links may not function. Please contact the [DOD Webmaster](#) with any questions.

The Defense Department has formally adopted five principles for the ethical development of artificial intelligence capabilities.





# Data fuels AI



# Data is an asset...it has value....it is therefore a target for cybercriminals

“...adversaries and cyber criminals are probing Defence’s networks for vulnerabilities to exploit. They are seeking insights into Defence capabilities, platforms, and personnel. They are seeking to steal data, slow Defence’s work, impact operations and identify gaps to exploit in the future. **Malicious cyber activity now represents one of Defence’s most critical risks.**”

*The Hon Matt Thistlethwaite MP, Assistant Minister for Defence*



# Some questions to leave you with.....

- Who is responsible for the AI? Does the use of AI in military operations change a commander's responsibility?
- Who would be liable if an AI decision resulted in injury or loss of life?
- How should the development or use of AI be governed? Should there be an AI regulator?
- How do we ensure the AI is "fit for purpose" for military applications?
- Should the human always be in the loop? Is AI actually "Augmented Intelligence"



*“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.*

*Upfront engagement on AI technologies, and consideration of ethical aspects needs to occur in parallel with technology development.”*

Professor Tanya Monro, Chief Defence Scientist

# Contact us

## **Executive Director**

Dr Sanjay Mazumdar | [smazumdar@dtb.solutions](mailto:smazumdar@dtb.solutions)

## **General Manager, Workforce, Innovation & Culture**

Heather Nicoll | [hnicoll@dtb.solutions](mailto:hnicoll@dtb.solutions)

## **General Manager, Technology Development & Commercialisation**

Dr Margaret Law | [mlaw@dtb.solutions](mailto:mlaw@dtb.solutions)

## **Senior Partnerships Manager**

Ilsa Stuart | [istuart@dtb.solutions](mailto:istuart@dtb.solutions)

This project is supported by the Australian Government Department of Education through the Trailblazer Universities Program.

**E:** [info@dtb.solutions](mailto:info@dtb.solutions)

**W:** [dtb.solutions](http://dtb.solutions)

A COLLABORATIVE PARTNERSHIP BETWEEN



Supported by



**Australian Government**  
**Department of Education**