White paper

Empowering cyber defence talent in an age of automation

verizon business

Introduction

Automation, powered by artificial intelligence (AI), is becoming increasingly intertwined with forging national resilience for Australia. While the past 100 years have shown how technology has gradually automated repetitive tasks and processes, AI is exponentially more disruptive, automating non-routine tasks and impacting more complex roles in both the private and public sectors, particularly defence.[1]

The defence industry plays a key role in nullifying cyber and terrorist threats and developing an agile, future-proof workforce to navigate geopolitical instability.

The ability to do this stands at a crossroads where government and academia must work closely together to innovate fragile supply chains and accelerate automated decision-making, while shielding workers from job loss and technological disruption.

The path forward lies in transitioning cyber talent to roles that harness automation while amplifying their problem-solving skills, critical thinking and creativity.

Australia's long-term ambition is to become a world leader in artificial intelligence and automation.

While immense, opportunities to do this are laced with risk if they are not framed within a long-term strategy that acknowledges that today's skills may be obsolete in the future, while newly acquired skills may have a limited shelf life.

Concerned thought leaders note that incomes often bend in favour of capital over employees in an industry that contributes over $10.6 billion to the Australian economy.[2]

There are numerous examples of private companies benefiting from automation to drive profits while cutting jobs or lowering wages. There's also a growing consensus locally and abroad that organisations preparing employees for future cyber roles with the right balance of automated support and technological skills will emerge as champions.[3]

Defence-focused organisations are key examples of nurturing and enhancing cyber talent with the latest breakthroughs in data science, machine learning and automation technologies. These organisations are driving innovation and scaling the next generation of mission-critical infrastructure, including new Industry 4.0 manufacturing facilities and processes.

While the Australian government may sometimes not match its political commitment to technological innovation with public action, the pledge to boost the Australian Defence Force's total permanent workforce by more than 18,500 or 30% by 2040 reveals the critical importance of people in keeping Australia safe in the uncertain and threat-laden global arena.[4]

Indeed, Australia's national prosperity and security depend on the government supporting the defence sector to unleash new automation technologies that provide high-paying jobs across AI, robotics, manufacturing and quantum computing. Research indicates that AI-driven automation could contribute $19.9 trillion to the global economy by 2030, driving 3.5% of global GDP, with China showcasing significant adoption. Australia's capacity to shape the Asia-Pacific (APAC) region and counter potential cyber threats relies on enhanced human decision-making, bolstered by automation.[5]

However, a 2024 report from the Technology Council of Australia (TCA) warns that by 2030, Australia may need up to 200,000 specialist AI workers to build and supervise new automation technologies. The report predicts that without significant reforms, job creation in the public and private sectors will not keep pace with this demand, requiring a 500% workforce expansion that current initiatives are unlikely to achieve.[6]

In this white paper, we argue that people, not machines, provide the ultimate digital edge. Data shows that organisations that equip their cyber talent with the right skills, complemented by automation, see stronger revenue growth over a three-year period. These organisations also report improved staff morale, which in turn fuels innovation and speeds up digital transformation.[6]

> "… the pledge to boost the Australian Defence Force's total permanent workforce by more than 18,500 or 30% by 2040 reveals the critical importance of people in keeping Australia safe…"[4]

Public and private governance

Ultimately, a framework for cyber talent empowerment falls under the remit of broader ethical governance in government and industry. In this ongoing process, leaders carefully consider the ethical implications of new skills and technologies and plan for their impact before being introduced into the defence sector.[7]

This strategic approach towards emerging automation and its supervising workforce has two influencing components: productivity and imported technologies. Both influence the future of work in Australia across manufacturing, especially in defence.

Productivity

The Australian government, through its 2025 policy initiatives, prioritises leveraging technological advancements, such as artificial intelligence, to foster competitive advantages in high-productivity, high-skill roles and future-focused industries, aligning with the strategic objectives of the Future Made in Australia framework.

Taking a long-term view, driving down costs, including worker wages, should not be the goal of automation. Instead, some technology-driven profits must flow back into cyber talent's pockets to improve their earnings and stimulate further innovation.

The government's vision, as outlined in 2025 policies, underscores the importance of collaboration with the private sector to enhance economic growth, boost productivity, and ensure long-term prosperity. By integrating the national research and innovation system with the Future Made in Australia framework, the government aims to address the nation's productivity challenges and seize strategic opportunities.[8]

The Brookings Institution, a US public policy nonprofit, affirms the stance that countries planning and structuring arrangements to address distributional concerns have the edge over those that do not.[9]

Imported technologies

In the past, the Australian government has leaned on using foreign expertise to launch and scale new manufacturing infrastructure—including space initiatives, quantum computing and defence. While generally favourable to economic growth, these foreign initiatives do not grow local cyber talent at the pace needed to compete with the US, Europe and China on a future AI-centric chessboard.

While foreign expertise will always have a place in a world where Australia has enduring and strong partnerships with its global allies, Australia also needs to invest in establishing sovereign primes that will boost economic growth, shrink economic complexity, and strengthen the defence sector's local talent and AI resources.

"If we stimulate interest in AI but do not deliver the skilled workforce and technological advantage, all we will create is frustration," said The Kingston AI Group, comprised of professors from eight Australian universities.[11]

Made in Australia (MIA) AI

Forging national research and education strategies to realise Made in Australia (MIA) AI technologies driven by a well-paid, expert cyber workforce is the holy grail. Pursuing productivity under this model encompasses four tactical approaches succinctly put forward by the ADF:

- Engage: Transparent, easy access to defence career opportunities with a particular focus on supporting science, technology, engineering and mathematics (STEM)-based roles
- Attract: Encourage local federal contractors and businesses to grow and attract a national cyber talent pool
- (Re)Train: Invest in the local defence industry to train and sustain a national AI-cyber workforce
- Collaborate: Connect critical stakeholders, thought leaders and industry players to build the workforce of the future that responds with quicker agility to local, national and global threats.[12]

Aligning public and private governance goals ultimately increases commercialisation opportunities. It encourages business in new defence sectors and markets while aggregating their capacities and expertise at higher wage levels.[13]

Human decision-making at scale

Outsourcing battlefield decisions to artificial intelligence is on the radar of all superpowers, including the US and China.[14] The rise of the self-optimising plant driven by automation under Industry 4.0 is underway globally, including in Australia.[15]

In both cases, the defence sector is wrestling with how to remove human bias without completely removing humans from the equation.

This tension between humans and machines prompts the creation of frameworks such as the AI Bill of Rights in the US for the responsible use of emerging technologies and sparks new debates around how to elevate human decision-making in the automation age.[16] It's also spawning innovative transdisciplinary research initiatives that blend social sciences with national defence strategies.[17]

In this golden age of automation, the ADF has created the Human and Decision Sciences Division to support human situational awareness, decision-making, control and protection.[18] Operating in a grey zone "where clear distinctions between peacetime and declared warfare are rapidly evaporating," the division specialises in helping humans cope with growing cyber attacks and disinformation campaigns. Grey zones are not limited to land. They span major defence domains including space, cyber, maritime and air. The division calls upon a range of human body and mind specialists to combat threats. These disciplines include biomechanics, cognitive enhancement and physical augmentation.[19] Moonshot applications of this program intend to scale human decision-making in ways unimaginable a decade ago. It includes, for instance, recent reports that the ADF may be testing an AI-brain interface that allows human operators to control robotic dogs telepathically on future battlefields.[20]

Using biosensors on the brain to decode brain waves, amplify them and transmit them to an AI decoder on a robot dog is an extreme examples of how humans are being removed from the battlefield and placed in creative, supervisory roles. Reaching this level of innovation requires a cross-sector collaboration of defence organisations and government innovation hubs.

More complex problems exist on the horizon for the Human and Decision Sciences Division. These include domains where trusted decision-makers disagree and no correct answer exists. These may be life-and-death decisions compounded by context: uncertainty, pressure, resource limitations and differing value systems. Counterpart divisions in the US, including the Defence Advanced Research Projects Agency (DARPA), are exploring how trusted algorithms can support decision-making during these critical moments.[21]

> "… the defence sector is wrestling with how to remove human bias without completely removing humans from the equation."

Global standards in the age of the Fifth Domain

Global defence spending reached a record high of $2.46 trillion in 2024, marking a 7.4% real-terms uplift, outpacing increases of 6.5% in 2023 and 3.5% in 2022.[22] This surge reflects heightened geopolitical tensions, the increasing frequency of state-sponsored cyber threats and the devastating impact of sophisticated attacks on public and private networks. Governments are jockeying for pole position in cybersecurity innovation as cyber investment has become a crucial pillar in modern defence strategy.[22]

Civilian and military networks share many similarities in approach, investment and threats. However, government systems require extra hardening layers to ensure national security on an industrial scale.

While automating security and networking is a priority to free up human decision-making and creativity, standards frameworks are the bedrock for future-proofing the defence industry from vulnerabilities and emerging security gaps.

These standards equip cyber talent to navigate complex technical landscapes and address the evolving nature of cyber warfare—often referred to as the Fifth Domain, alongside air, sea, land and space. Notably, the adoption and enforcement of global standards has positioned Australia as a rising leader in cybersecurity technology, supported by both global defence primes and emerging local players.

Australia strategically collaborates with allied nations, sharing best practices to sharpen the skills of its cyber defence experts. As a member of the Five Eyes intelligence alliance—together with Canada, New Zealand, the United Kingdom and the United States—Australia recently teamed up with the US Pentagon to explore adopting a zero trust security model.

In this framework, zero trust networks (ZTN) assume no party is trustworthy at any point, requiring ongoing verification before access is permitted.

"It is not a product or program but a paradigm shift for the US in response to vulnerabilities exposed by high-level breaches. It is also essential to delivering secure, data-centric Joint All-Domain Command and Control (JADC2) capabilities," according to the US Department of Defense (DoD).[23]

Several Australian government departments and agencies are working to ensure maximum security through zero trust automated interoperability between government and private networks.

The Australian Cyber Security Centre (ACSC) Essential Eight Maturity Model provides small, medium and large organisations a consistent baseline from which to approach the philosophy of ZTN in their operations. The eight mitigation strategies cover a range of security protocols, including user application hardening and multifactor authentication.[24]

While the ACSC Essential Eight currently has mixed adoption, it's crucial in helping free cyber talent from legacy software restrictions and enhancing automation while limiting privacy concerns.

By moving toward a ZTN, companies can protect themselves against various cyber threats and vulnerabilities.

Additionally, the emerging ZTN model supports manycritical standards that govern public and private infrastructural networking operations, including but not limited to:

- IS027001:2 is a standard that meets information security management system (ISMS) requirements, a framework for managing and protecting sensitive information.
- Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards developed by the payment card industry to ensure that merchants who accept credit card payments maintain a secure environment.
- The Cybersecurity Framework (CSF) is a National Institute of Standards and Technology (NIST) framework to help organisations manage cybersecurity risks and protect against cyber threats.
- NIST SO800-53 is a set of security controls and guidelines developed by NIST to help federal agencies and organisations protect their information and systems.
- CSA Cloud Control Matrix is a framework for evaluating and managing security risks associated with cloud computing.
- C2M2 (Cybersecurity Capability Maturity Model) is a framework for assessing an organisation's cybersecurity capabilities and maturity.
- COBIT (Control Objectives for Information and Related Technologies) provides an IT governance and management framework that helps organisations align their IT strategies with business goals and objectives.

While the plethora of standards and frameworks often challenge the technical capabilities of federal contractors and smaller businesses in the defence supply chain, they help ensure that future innovation in automation has solid foundations for success.

"These standards equip cyber talent to navigate complex technical landscapes and address the evolving nature of cyber warfare—often referred to as the Fifth Domain, alongside air, sea, land and space."

Gilmour Space

Australian space startups are closing the gap with their counterparts in the United States. Sovereign prime Gilmour Space is no exception, working toward launching Australia's first commercial rocket, Eris, into orbit.

Aerospace achievements like these unlock new opportunities for cyber talent while building cutting-edge automation technologies to support breakthroughs in building and launching rockets into orbit.

Gilmour is pioneering the Autonomous Flight Termination System (AFTS). The intelligent electronics unit features an independent decision-making capacity responsible for aborting a flight if severe issues arise. The collaborative effort with SENER Aeroespacial uses software processing algorithms that collect and analyse the Eris flight parameters, identifying deviations from the nominal trajectory with the power to terminate the mission if necessary.

According to both parties, improving the versatility of launch vehicle operations enables "more launches from places other than traditional launch centres; and their efficiency, by lowering the cost of operations."[25]

The Eris launch will mark a watershed moment in the Australian defence sector, a byproduct of strategic thinking under the Queensland Aerospace 10-Year Roadmap and Action Plan.[26]

Nurturing affordable access to space for small and medium-sized payloads has propelled defence technology spinoffs into hypersonics, ultra-high temperature composites, astrophysics, airborne Earth re-entry observations and robotic vision in uncontrolled environments. Automation stacks steered by AI algorithms, while supervised and improved by human decision-making, strengthen Australian national resilience and supply chains. Gilmour sources material and expertise from local suppliers, and it hires and upskills local talent while ensuring intellectual property is not foreign-owned.

> "Aerospace achievements like these unlock new opportunities for cyber talent"

Ghost Shark

One success story from Australia's Next Generation Technologies Fund is Ghost Shark, an autonomous robotic undersea warfare vehicle designed and manufactured in Australia for the Royal Australian Navy by Anduril Australia.

The co-funded project cost around $100 million. Its technology stack utilises edge computing, sensor fusion, propulsion and robotics. Built to carry heavy loads over long periods and long distances, it's another example of AI-driven automation freeing up human labour while reducing the risk to life.

While these innovations are examples of uncrewed or unmanned military applications controlled tactically by AI, the supervisory aspects still require human supervision to ensure successful outcomes.

Plans are underway to hire skilled workers in maritime engineering, software development, robotics, propulsion design and mission operations.[27]

Verizon

Attack surfaces increase as digital transformation grows. The deep domain expertise needed to deliver military-grade security gateways on new 5G platforms offers an opportunity to grow sovereign primes for mission-critical infrastructure. Partnering with global managed security and networking solution providers like Verizon enables local cyber talent to build new skills and develop the expertise needed to manage complex technology frameworks. These frameworks extend into ZTN, mobile edge computing, identity management and virtual simulation software like digital twins.

One possible future collaboration area lies in using 5G drones to capture real-time intelligence, surveillance and reconnaissance (ISR) data from in-flight aircraft to geolocate military targets. The technology, recently demonstrated to the US DoD, showcases advanced signal processing algorithms executed at the tactical edge of 5G infrastructure. Using open, secure standards, it illustrates 5G.MIL delivering accurate information to support human decision-making, often called "integrated deterrence."[28]

Conclusion

Automating scalable, secure decision-making doesn't compete with human talent; it unleashes creativity, problem-solving and critical thinking. The symbiotic partnership between artificial intelligence and human cyber talent opens a real opportunity for Australia to become a global leader in technology by 2040.

By integrating governance insights with advancements in zero trust networks and established global security standards, cyber talent is empowered to drive technological innovation. Further, it promises to reset the balance sheet and finally links productivity to wage growth, arguably missing from historical technological change in Australia.

"Made in Australia" AI is possible and should be pursued strategically.

Sovereign primes like Gilmour Space show us the spectacular rewards of local space innovation, up and down the national supply chain.

Meanwhile, connectivity and managed solutions linked to 5G reveal the power of harnessing data at scale, opening new doors to safer and faster decision-making through global operators like Verizon. Recent ADF advancements in uncrewed submarines like Ghost Shark via Anduril Australia show us a brave new world where humans are freed from high-risk environments to explore more exciting, data-centric supervisory roles.

The path forward to national resilience is clear. Still, bold decision-making is needed to empower our defence workforce with the tools and skills to tap artificial intelligence's supportive powers in the automation age. Putting people first, not machines, is the key to building the future workforce in the military-industrial defence landscape.

"Automating scalable, secure decision-making doesn't compete with human talent; it unleashes creativity, problem-solving and critical thinking."

Learn more

To learn more about future-ready public security sector automation, contact your Verizon Business Account Representative.

Email apaccontactus@verizon.com.
Visit verizon.com/business/en-au/contact-us/

References

1. United Nations Development Programme. “Future of Work: Augmentation.” https://www.undp.org/eurasia/our-focus/inclusive-growth/futuAugmentation

2. Australian Bureau of Statistics. “Australian Defence Industry Account, experimental estimates.” https://www.abs.gov.au/statistics/economy/national-accounts/australian-defence-industry-account-experimental-estimates

3. Accenture. “Digital Future of the Supply Chain Workforce.” https://www.accenture.com/us-en/insights/supply-chain-operations/digital-future-supply-chain-workforce

4. Australian Department of Defence. “STEM Support.” https://www.defence.gov.au/business-industry/skilling-defence-industry/stem-support

5. International Data Corporation. “IDC: Artificial Intelligence Will Contribute $19.9 Trillion to the Global Economy through 2030 and Drive 3.5% of Global GDP in 2030.” https://www.idc.com/getdoc.jsp?containerId=US51057924

6. Tech Council of Australia. “AI to create 200,000 jobs in Australia by 2030.” https://techcouncil.com.au/newsroom/ai-to-create-200000-jobs-in-australia-by-2030/

7. Australian Unions. “Ed Husic on Automation and the World of Work.” https://www.australianunions.org.au/podcast/ed-husic-on-automation-and-the-world-of-work/

8. InnovationAus.com. “Ayres arrives: New minister vows to link up policy, ditch ‘dogma’.” https://www.innovationaus.com/ayres-arrives-new-minister-vows-to-link-up-policy-ditch-dogma/

9. Brookings Institution. “Whoever leads in artificial intelligence in 2030 will rule the world until 2100.” https://www. brookings.edu/blog/future-development/2020/01/17/ whoever-leads-in-artificial-intelligence-in-2030-will-rule-the-world-until-2100/

10. InnovationAus. “Vic govt’s surprising $29m bet on foreign quantum.” https://www.innovationaus.com/vic-govts-surprising-29m-bet-on-foreign-quantum/

11. InnovationAus. “Australia risks ceding sovereign control to foreign interests on AI.” https://www.innovationaus.com/australia-risks-ceding-sovereign-control-to-foreign-interests-on-ai/

12. Australian Department of Defence. “STEM Support.” https://www.defence.gov.au/business-industry/skilling-defence-industry/stem-support

13. Global Australia. “Defence.” https://www.globalaustralia.gov.au/industries/defence

14. Defense Advanced Research Projects Agency (DARPA). “DARPA announces $2.1 billion in new investments.” https://www.darpa.mil/news-events/2022-03-03

15. Chemical Safety. “Chemical EMS Software Takes Center Stage in Industry 4.0.” https://chemicalsafety.com/chemical-ems-software-takes-center-stage-in-industry-4/

16. The White House. “ICYMI: Wired Opinion: Americans Need a Bill of Rights for an AI-Powered World.” https://www.whitehouse.gov/ostp/news-updates/2021/10/22/icymi-wired-opinion-americans-need-a-bill-of-rights-for-an-ai-powered-world/

17. Australian Department of Defence Science and Technology. “Dr. Katerina Agostino.” https://www.dst.defence.gov.au/staff/dr-katerina-agostino

18. Australian Department of Defence Science and Technology. “Human Decision Sciences.” https://www.dst.defence.gov.au/division/human-decision-sciences

19. Australian Department of Defence Science and Technology. “Defence Human Sciences Symposium 2022.” https://www.dst.defence.gov.au/event/defence-human-sciences-symposium-2022

20. Australian Department of Defence. “Brain Waves Control Robot Dogs’ Moves.” https://www.defence.gov.au/news-events/news/2022-06-07/brain-waves-control-robot-dogs-moves

21. Defense Advanced Research Projects Agency (DARPA). “DARPA announces $2.1 billion in new investments.” https://www.darpa.mil/news-events/2022-03-03

22. The International Institute for Strategic Studies. “Global defence spending soars to new high.” https://www.iiss.org/online-analysis/military-balance/2025/02/global-defence-spending-soars-to-new-high

23. United States Department of Defense. “Advancing JADC2: Second Site Summit Includes FVEY Partners.” https://www.defense.gov/News/Releases/Release/Article/3259862/advancing-jadc2-second-site-summit-includes-fvey-partners/

24. Australian Cyber Security Centre. “Essential Eight Maturity Model.” https://www.cyber.gov.au/acsc/view-all-content/ publications/essential-eight-maturity-model

25. Gilmour Space Technologies. “Gilmour Space, SENER Aeroespacial to Develop Autonomous Flight Termination System for ERIS.” https://www.gspacetech.com/post/gilmour-space-sener-aeroespacial-to-develop-autonomous-flight-termination-system-for-eris

26. Queensland Government. “Queensland Aerospace 10- Year Roadmap and Action Plan 2018-2028.” https://www.statedevelopment.qld.gov.au/ data/assets/pdf_file/0014/17231/aerospace-roadmap.pdf

27. Australian Department of Defence. “Ghost Shark: Stealthy Game Changer.” https://www.defence.gov.au/news-events/ news/2022-12-14/ghost-shark-stealthy-game-changer

28. Lockheed Martin. “Lockheed Martin, Verizon Demonstrate 5G-Powered ISR Capabilities for Department of Defense.” https://news.lockheedmartin.com/2022-09-28- Lockheed-Martin-Verizon-demonstrate-5G-powered-ISR- Capabilities-for-Department-of-Defense