Journal of Strategic Trade Control
Vol. 2, February 2024

Australia's defense export control regime and critical technologies

Lauren Sanders *

Abstract

In 2023, Australia entered its second statutory review of export control legislation, an ongoing process since the unimplemented findings of the 2018 review, which declared the legislative framework no longer fit for purpose. A key finding of the 2018 review underscored the inadequacy of the existing legislative regime in addressing critical technologies, such as artificial intelligence. This paper proposes a strategic approach for Australia to enhance its defense export controls by drawing insights from other export control systems that have tackled similar issues. Through adept adaption of existing legislation and exploration of alternative strategies for regulating critical military technologies, this study aims to bring about concise and meaningful updates. The primary focus of the analysis centers on the challenges posed by emerging and disruptive technologies (EDT). Specifically, it seeks to highlight the novel characteristics of EDT and their potential military applications, necessitating specific consideration in the design of an export control regime. Furthermore, the paper aims to explore feasible enhancements to Australia's domestic regulation, addressing existing gaps. These proposed reforms could assist in harmonizing Australia's controls with those of the European Union (EU) and the United States (US), fostering global consistency in export control models. By identifying methods to enhance export control regimes of countries that play middling roles in the global defense export markets, such as Australia, this paper outlines a pathway for Australia's legislative evolution while contributing valuable insights to reflect upon the efficacy and influence of EU and US models in achieving global non-proliferation objectives.

Keywords

Australia; export control; emerging and disruptive technology; EDT; artificial intelligence; military technologies; critical technologies; defense export.

* Dr Lauren Sanders is a Senior Research Fellow at the Law and Future of War research group. Her research focuses on emerging and disruptive technologies in the context of international humanitarian law, arms control regimes and export controls; with recent publications on the legal review of autonomous weapons systems, and a commentary on the AUKUS technology agreement. She has recently published in the Journal of Conflict and Security Law on the utility of weapons review in regulating autonomous weapons systems, and co-authored a number of reports on the findings of the Group of Governmental Experts on legal reviews. She would like to thank the peer reviewers of this paper for their valuable insights and recommendations to improve this paper; and for the assistance of the JoSTC editors (and Veronica Vella in particular) in refining this paper. All errors are the responsibility of the author.

Article info

Submission date: April 27, 2023. Acceptance date: September 21, 2023. Publication date: February 21, 2024.

How to cite

Lauren Sanders, "Australia's defense export control regime and critical technologies", *Journal of Strategic Trade Control,* Vol. 2, (February 2024). DOI: 10.25518/2952-7597.93

Publisher

European Studies Unit (ESU), University of Liège.

Peer review

This article has been peer-reviewed through the journal's standard double-anonymous peer review, where both the reviewers and authors are anonymized during review.

Open access

The Journal of Strategic Trade Control is a peer- reviewed open-access journal. Accessible at www.jost.org

Introduction

Critical technologies—including artificial intelligence (AI)[1]—underpin Australia's national security.[2] Through its AI Action Plan, the Australian government intends to leverage critical technology to strengthen Australia's economy and counter national security threats.[3] In the military context, the Australian, United Kingdom, and United States (AUKUS) trilateral security partnership also enables enhanced cooperation with Australia's closest allies on critical technologies and advanced capabilities, which includes AI and autonomy.[4] Separately, AI capabilities are being applied to fields ranging from transport (with autonomous vehicles), the medical industry, and gaming, to office administration (such as through the use of virtual assistants).[5] The dual-use nature of most AI applications means that technologies developed for civilian purposes may be capable of military application and therefore subject to export control;[6] and in some cases, technology not originally envisaged for defense use may be readily adapted for use in a military context. Further, many of these technologies are being used outside of traditional military frameworks, to achieve economic strategic advantage over competing states. Grouped together, these novel capabilities are often referred to as emerging and disruptive technologies (or 'EDT'), given their ability to change the course of military operations, in unforeseen and significant

---

[1] AI is a broad term used to describe a collection of technologies able to solve problems and perform tasks without explicit human guidance. AI may be used to perform tasks and solve problems that, if done by humans, would require thinking.

[2] Commonwealth of Australia, Department of Prime Minister and Cabinet, *Blueprint for Critical Technologies: The Australia Government's framework for capitalising on critical technologies to drive a technologically-advanced, future-ready nation,* (Australia: Department of Prime Minister and Cabinet, November, 2021), p. 2.

[3] Australian Government, "Australia's AI Action Plan", June18, 2021, https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-action-plan.

[4] United States Government, The White House, "Fact Sheet: Implementation of the Australia – United Kingdom – United States Partnership (AUKUS)", April 5, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/05/fact-sheet-implementation-of-the-australia-united-kingdom-united-states-partnership-aukus/; United States Government, The White House, "Joint Leaders Statement on AUKUS", March 13, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/13/joint-leaders-statement-on-aukus-2/.

[5] Glennn Moy, et al., *Technical Report: Recent Advances in Artificial Intelligence and their Impact on Defence,* (Canberra: Joint and Operations Analysis Division, Defence Science and Technology Group, 2020), p. 1.

[6] Maaike Verbruggen, "The Role of Civilian Innovation in the Development of Lethal Autonomous Weapon Systems", *Global Policy,* Volume 10, Issue 3, (September 2019), p. 338.

ways.[7]

Having regard to Australia's current system of export controls, this paper explores the opportunities presented by the ongoing statutory review of Australia's export controls.[8] It proposes specific areas of focus to ensure the maintenance of an appropriate balance between innovation and national security. The analysis will particularly concentrate on the challenges posed by EDT. Specifically, it will highlight the novel characteristics of EDT, and the capacity for their military use, requiring specific consideration in the design of an export control regime. Additionally, the paper will explore feasible enhancements to Australia's domestic regulation to close the existing gaps.

This paper is primarily intended to contribute to the discussion about the details of the legislative gaps in the current Australian regime, noting the recommendations of the still-to-be-implemented 2018 report (the 'Thom Review'), that identified Australia's export controls are not fit for purpose in regulating dual-use technologies.[9] Secondly, this paper is intended to contribute to a broader debate in export control discourse about the preferred approach to export controls for novel technology: by offering an analysis of Australia's divergent regime, and its effectiveness on overall non-proliferation efforts, separate from the dominant discourse relating to the European Union (EU) or the United States (US) regimes.

Notable also is whether there may be any additional considerations as to how Australia might approach its legislation updates in the shadow of US announcements in July 2023 about the relaxation of its export control rules to Australia (specifically the proposal to deem Australia, like Canada, a 'domestic' supplier to US markets, for the purposes of exempting Australian companies from the US International Trade of Arms Regulations ('ITAR')). The enhanced defense trade flagged by the recent AUKUS announcement,[10] as well as the recently announced Five Eyes

---

[7] "Emerging and Disruptive Technologies", NATO, last updated June 22, 2023, https://www.nato.int/cps/en/natohq/topics_184303.htm.

[8] Richard Marles, Deputy Prime Minister/Defence Minister of Australia, "Review of Defence Trade Controls Act 2012", August 29, 2023, https://www.minister.defence.gov.au/media-releases/2023-08-29/review-defence-trade-controls-act-2012.

[9] Vivian Thom AM, *Independent Review of the Defence Trade Controls Act 2012*, (Australia: Defence Publishing Services, Department of Defence, 2018), https://www.defence.gov.au/sites/default/files/2020-10/DTC_Act_Review_Final_Report.pdf.

[10] "Agreement between the Government of Australia, the Government of the United Kingdom of Great Britain and Northern Ireland, and the Government of the United States of America for the exchange of naval nuclear propulsion information", conclusion date:

export control enforcement cooperation agreement, demonstrates the need for smaller export control regimes.[11] Consequently, there have been minor adjustments to the export control legislation accounting for streamlined processes and enhanced protections vis-à-vis US technologies.[12] In light of these developments, the need for Australia's controls to be capable of interoperability with the larger regimes of the EU and the US, while also addressing issues of security governance and national interest thus requires deeper consideration.[13]

Further, as the race for AI supremacy has been likened to the nuclear arms race of several decades ago, it is timely to contemplate how smaller defense industrial bases, such as Australia, are seeking to impact upon this broader issue of non-proliferation.[14] Current literature in the field focuses on US export controls on emerging technologies, and EU controls relative to cyber surveillance items, but there is little analysis of competing regimes and how they interact with or contribute to, broader non-proliferation and security initiatives.[15] For this reason, this assessment focuses on how Australia's export controls might be updated, borrowing from the experiences of US and EU systems to

---

February 8, 2022, *Treaties and International Agreements Registered or Filed and Recorded with the United Nations Secretariat*, no 57347 (2022), https://treaties.un.org/Pages/showDetails.aspx?objid=08000002805edc16; Australian Government, "AUKUS Factsheet", March 2023, https%3A%2F%2Fwww.defence.gov.au%2Fabout%2Ftaskforces%2Faukus&usg=AOvVaw1Obbg90tXgUvrvpAdlx33Y.

[11] Bureau of Industry and Security, US Department of Comments, "Press Release: Five Eyes Partners Agree to Formalize Cooperation on Export Control Enforcement", June 28, 2023, https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3294-2023-06-28-bis-press-release-five-eyes-export-enforcement-coordination/file.

[12] Parliament of Australia, Defence Trade Controls Amendment Bill 2023 [Provisions], accessed December 2023, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Foreign_Affairs_Defence_and_Trade/DTCAmendment47.

[13] Jessica Lewis, US Department of State, "House Committee on Foreign Affairs Hearing: Modernizing U.S. Arms Exports and a Stronger AUKUS", May 24, 2023, https://www.state.gov/house-committee-on-foreign-affairs-hearing-modernizing-u-s-arms-exports-and-a-stronger-aukus-a-s-jessica-lewis/.

[14] Paul Scharre, "AI's Gatekeepers Aren't Prepared for What's Coming", *Foreign Policy*, June 19, 2023, https://foreignpolicy.com/2023/06/19/ai-regulation-development-us-china-competition-technology/.

[15] See for example: Diederik Cops, Nils Duquet, Gregory Gourdin, *Towards Europeanized arms export controls? Comparing control systems in EU Member States*, (Brussels: Flemish Peace Institute, 2017), https://vlaamsvredesinstituut.eu/wp-content/uploads/2019/03/Towards-Europeanized.pdf; Laurence Lustgarten, *Law and the Arms Trade: Weapons, Blood and Rules,* (Oxford: Hart Publishing, 2020); "Dual-use and arms trade controls", Chap. 12, SIPRI Yearbook 2023;

address the challenges of critical technologies.

In undertaking this analysis, this paper will demonstrate that there are some helpful analogies that can be made in export control approaches between countries and regions. However, as is the case in Australia, each state's individual legislative framework impacts the options and methodologies by which the challenges of technology controls can be achieved. In the Australian case, there are a number of relatively minor adjustments that can be implemented to the existing list-based export control regime to account for some of these challenges. Additionally, certain structural changes could be considered to overcome the deficiencies inherent in a list-based regulatory approach.

However, the issue of balancing trade partners (such as China) with Australia's key military allies (specifically the US and the UK) demonstrates how export control approaches can be impacted by more than their primary national security aims. In this way, the paper demonstrates that in adopting updates to export control regimes, there are trade-offs that necessitate a balance between free market innovation and national security interests and controls.

The paper will first identify what characteristics of critical technologies (and AI in particular) may challenge existing export control frameworks. This includes AI technology that may augment more 'traditional' military capabilities. It will then outline how Australia's export control system operates and who it applies to. It will also explain the outcomes of the recent review of that system following the 2019 Independent Review of the Defence Controls Act 2012 conducted by Dr Vivienne Thom AM (hereinafter the Thom Review), and its recommendations for amendments to the Defence Trade Controls Act 2012, associated regulations and other implementing legislation.[16] In assessing whether or not these recommended changes adequately address the challenges presented by AI, the paper will demonstrate that the existing regime can adequately cope with emerging and disruptive technology with minor amendments. Finally, the paper will conclude with suggestions as to how these gaps and areas of uncertainty may be rectified during the implementation of the Thom Review's recommendations, as accepted—but still to be implemented–by the Australian government.

[16] Thom AM, Independent Review of the Defence Trade Controls Act 2012.

Characteristics of critical technologies that challenge export control regimes

Critical technologies possess a range of characteristics that challenge conventional export control regimes. These include the dual-use nature of the technology, the open-source availability of enabling software, the technologies' susceptibility to foreign appropriation, and the emerging and disrupting nature of its development outpacing national regulatory measures.[17] While this paper does not propose to engage in a literature review of EU and US export control laws, recent reforms to these regimes have also sought to address the challenges posed by critical technologies, and specifically narrow their focus on control of items considered dual-use critical technologies.[18] The recent amendments to international export control regimes can be used as a broad measure for the accepted focus of the larger export control systems, like the EU and the US:[19] developments to the Wassenaar Arrangement in the 2010s have included a focus on cyber-surveillance technology–similarly one of the focus points of the EU;[20] with the EU also updating its dual-use regulation to incorporate better human rights protections.[21] Separately, the focus on

---

[17] See for example: Scott A. Jones, "Trading Emerging Technologies: Export Controls Meet Reality", *Security and Human Rights*, 31, (2021).

[18] In Europe, the focus on EDT has been on the development of regulatory frameworks that address how to regulate dual-use technologies in particular, with a focus on particular 'critical technologies' that are deemed to have security implications. See, for example: Samuel Stolton, Jorge Valero, Alberto Nadelli, "EU to Focus on Export Controls, Critical Tech in Security Plan", *Bloomberg*, June 19, 2023, https://www.bloomberg.com/news/articles/2023-06-19/eu-to-focus-on-export-controls-critical-tech-in-security-plan;In the US, the focus has been on adjusting export controls for specific dual-use critical technologies by focusing upon end-users who are likely to misuse that technology, such as the recent focus upon the supply and design of semi-conductors that might find their way to China, and then be re-exported to Russia. See, for example: Hannah Kelly, "Dual-Use Technology and U.S. Export Controls: Findings from the CNAS Lab", *Centre for a New American Society*, June 15, 2023, https://www.cnas.org/publications/reports/dual-use-technology-and-u-s-export-controls.

[19] Tobia Gehrke, Julian Ringhof, "The Power of Control: How the EU Can Shape the New Era of Strategic Export Restrictions", European Council on Foreign Relations, May 2023; Maria Shagina, "The Role of Export Controls in Managing Emerging Technology", in *The Implications of Emerging Technologies in the Euro-Atlantic Space,* ed. J. Berghofer et al, p. 58.

[20] Heejin Kim, "Global Export Controls of Cyber Surveillance Technology and the Disrupted Triangle Dialogue", *International and Comparative Law Quarterly*, Vol 70, Issue 2, April 2021, pp 379-415; Mark Bromley, *Export Controls, Human Security and Cyber-Surveillance Technology: Examining the Proposed Changes to the EU Dual-Use Regulation*, (SIPRI, December 2017).

[21] Shagina, "The Role of Export Controls in Managing Emerging Technology", p. 60.

country-specific sanctions reflects the US' focus on control of specific emerging technologies based upon strategic risk rather than general proliferation concerns.[22]

Many critical technologies are dual-use in nature. It is probably fair to suggest that most critical technologies could have secondary uses capable of militarization and are therefore likely to be worthy of export control consideration. However, the list-based approach to export control regimes does not account for the secondary or potential military uses of many critical technologies. The breadth of the Wassenaar Arrangement Dual-Use List demonstrates the extent to which items and technologies that are considered primarily for civilian purposes can also be considered to have a military purpose.[23] Dual-use technologies under the Arrangement encompass those technologies that augment military capabilities. For those critical technologies that have inherent characteristics useful for military as well as commercial purposes, then the item will be one on the controlled item list and thus be regulated. This approach does not account for the nature of critical technologies and AI. Specifically, many civilian technologies can be utilized either in direct support of military systems or to directly augment them.

Equally, the use of specific lists to control novel technology is not overly effective. Control lists can become quickly outdated. As a basic example, an AI designed to identify patisserie has been adapted to read x-ray imagery to detect cancer cells within twelve months of its development.[24] This dual-use technology translation reflects the key challenge raised by AI technologies that have applications both in the military and civilian domains. While there can be design limitations placed upon the AI capability to address control of the system, in spite of such controls the use of the AI systems to conform with existing international humanitarian law obligations cannot be guaranteed. Once exported, a system designed

---

[22] Kelly, "Dual-Use Technology and U.S. Export Controls"; Ian Stewart, "Export Control and Emerging Technology in an environment of Strategic Competition", CNS NonPro Notes, James Martin Center for Nonproliferation Studies, March 2022; Gehrke, Ringhof, "The Power of Control".

[23] Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, Public Documents Volume I, Founding Documents, as amended in December 2019, https://www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-I-Founding-Documents.pdf; see generally, Wassenaar Arrangement, Public Documents Volume II, List of Dual-Use Goods and Technologies and Munitions List, compiled by the Wassenaar Secretariat, as amended in December 2022, https://www.wassenaar.org/app/uploads/2022/12/List-of-Dual-Use-Goods-and-Technologies-Munitions-List-Dec-2022.pdf.

[24] James Somers, "The Pastry A.I. That Learned to Fight Cancer", *The New Yorker*, March 18, 2021, https://www.newyorker.com/tech/annals-of-technology/the-pastry-ai-that-learned-to-fight-cancer.

for one purpose can be readily transformed into another.

In 2020, the International Panel on the Regulation of Autonomous Weapons (iPRAW) released a working paper outlining considerations for the export control of weapon systems with autonomy in their targeting functions.[25] While focused on challenges to the regulation of lethal autonomous weapon systems (LAWS), rather than artificial intelligence more generally, the report identified a number of broad challenges relevant to the consideration in the export and proliferation of systems capable of supporting LAWS which can be underpinned by artificial intelligence technology. The working paper concluded that there is a need for "new or adapted export control mechanisms" in conjunction with multilateral regulation; but that:

> "a complementary approach to list-based export controls is required due to the unique characteristics of LAWS and their essential components; and existing multilateral export control regimes should be expanded to account for the challenges presented by open-source software and data, that is not otherwise adequately controlled under existing regimes".[26]

Similarly, Scharre and Lamberth's 2022 report identifies the general challenges with all arms control regimes but notes these challenges are exacerbated in the case of new technology by the inability to predict how technologies will evolve.[27] As a result of the inability to predict how the technology may perform, or evolve, its regulation thus becomes difficult.

Several specific challenges relating to the proliferation of LAWS are identified in these reports, which warrant further consideration in assessing the suitability of export control regimes applying to AI technology more generally:

1. Enabling software applications can be readily adapted for other purposes with differing data inputs. This dual-use software might be capable of use for other important civil functions.[28]

---

[25] "LAWS and Export Control Regimes: Fit for Purpose?" (working paper, International Panel on the Regulation of Autonomous Weapons (iPRAW), April 2020), https://www.ssoar.info/ssoar/bitstream/handle/document/77412/ssoar-2020-LAWS_and_Export_Control_Regimes.pdf?sequence=1&lnkname=ssoar-2020-LAWS_and_Export_Control_Regimes.pdf.

[26] "LAWS and Export Control Regimes", (working paper, iPRAW).

[27] Paul Scharre and Megan Lamberth, *Artificial Intelligence and Arms Control* (Washington, DC: Centre for a New American Society, October 2022), https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/AI-and-Arms-Control_FINAL.pdf.

[28] "LAWS and Export Control Regimes", (working paper, iPRAW).

2. They are readily adapted based on existing software, which is often open-source and thus not readily controlled.[29]
3. The data used to train the machine is not regulated in any way so data sets from any source can be input into the AI system.[30] While national regulations relating to medical information and the privacy of personal information may apply, the same cannot be said for data used to train an algorithm on military uses.[31]
4. The hardware (that is the sensors and computer componentry) that enables the AI is also highly translatable. AI hardware componentry is therefore highly likely to be dual-use, and readily capable of being implemented into military systems.[32]

The ubiquitous and intangible nature of AI-enabling software makes it difficult to target for export controls.[33] Instead, in some cases targeting specific and bespoke componentry, such as semi-conductors, can effectively curtail the proliferation of these types of technology.[34] It is

---

[29] "LAWS and Export Control Regimes", (working paper, iPRAW); Scharre and Megan Lamberth, *Artificial Intelligence and Arms Control*; Carrick Flynn, "Recommendation on Export Control for Artificial Intelligence" (issues brief, Centre for Security and Emerging Technology, February 2020), https://cset.georgetown.edu/publication/recommendations-on-export-controls-for-artificial-intelligence/.

[30] "LAWS and Export Control Regimes", (working paper, iPRAW); David Plotinsky, "Could sensitive personal data become export controlled?", Morgan Lewis, July 19, 2022, https://www.morganlewis.com/pubs/2022/07/could-sensitive-personal-data-become-export-controlled.

[31] For Australia, see: Jordan Cox and Bryce Siu, "Australia" in AI, Machine Learning & Big Data Laws and Regulations 2023, Global Legal Insights, 2023. See generally, the exemption in the EU Data AI for national security, military and defence purposes: Council of the EU Presse Release, "Artificial Intelligence Act: Council calls for promoting safe AI that respects fundamental rights", December 6, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/12/06/artificial-intelligence-act-council-calls-for-promoting-safe-ai-that-respects-fundamental-rights/; Interinstitutional File 2021/0106 (COD) Proposal for a Regulation of the European Parliament and on the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative acts, draft article 12, https://data.consilium.europa.eu/doc/document/ST-8115-2021-INIT/en/pdf.

[32] "LAWS and Export Control Regimes", (working paper, iPRAW); Flynn, "Recommendation on Export Control for Artificial Intelligence".

[33] Andrew W. Reddie, "Accelerating the Evolution of AI Export Controls", Tech Policy Press, 2023, https://www.techpolicy.press/accelerating-the-evolution-of-ai-export-controls/.

[34] See for example the US restriction on advanced computing integrated circuits, through export control classification number (ECCN) 3A090: Federal Register, "Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification", October 13, 2022.

therefore important to consider the technology holistically, rather than in terms of just controlling the software components of it.[35] Accordingly, the update to the methodologies to control critical technology and AI requires multiple and overlapping adjustments to existing regimes to enable effective control, while not stifling innovation.

Finally, the emerging and disruptive nature of critical technologies is another characteristic with export control implications. Critical technology is developed quickly, and its applications and their impact can be difficult to foresee. This challenges the reactive nature of legislative instruments designed to incorporate new technologies. This delay in regulation is not novel: the law has long been observed to follow well behind the technology leading to ineffective or inefficient export control.[36]

These characteristics require national and multilateral export control regimes to adapt their hardware-based approaches to export control to deal with software-based export risks. Accordingly, before understanding how Australia's regime requires adaptation, it is relevant to outline Australia's existing approach to implementing export controls and identify the measures it is undertaking to address the challenges presented by these critical technologies.

Australia's export control regime applied to critical technology

Australia's export control regime was created to prevent the export of military goods and technology to those who may threaten Australia's security including military goods and technology that can be used in conventional, chemical, biological, and nuclear weapons.[37] It centers on the Defence Strategic Goods List (DSGL) which attempts to define controlled goods and technology. However, it is well accepted that emerging and disruptive technologies that are dual-use, non-physical, and electronically exportable challenge this old control paradigm.[38] These challenges are recognized by the Australian government which has

[35] Stewart, "Export Control and Emerging Technology Control in an Era of Strategic Competition".
[36] John H. Henshaw, "The Origins of COCOM: lessons for contemporary proliferation control regimes", Henry L. Stimson Center Report, (Washington, DC: 1993), https://www.stimson.org/wp-content/files/file-attachments/Report7_1.pdf.
[37] Thom AM, *Independent Review of the Defence Trade Controls Act 2012,* p. 11.
[38] "LAWS and Export Control Regimes", (working paper, iPRAW).

sought to address the gaps and uncertainty in its export control regime.[39]

Introduction to Australia's EDT industry and technologies of national security concern

In discussing the term critical technology, it is useful to understand the types of technology that Australia is concerned with. While Australian universities and sovereign industry undertake a breadth of research activities that trigger defense export controls, the recently announced AUKUS arrangement and the Australian Defence Strategic Review (the 'DSR')—which provided 'a once in a generation' review of Australia's defense priorities and has adjusted its acquisition approach to align to this refocusing of its new (or restated) defense priorities)—provide an indication of the high level of attention and effort being diverted by the Australian government to enhancing defense capability, industry, and trade.[40] Through the DSR, Australia has notably identified that it is no longer capable of retaining a technological edge over competitors as a pillar of its national defense strategy, and has returned its focus to strategic deterrence and strategic alliances. The DSR expressly stated that "[t]echnology has a significant impact on the character of warfare and deterrence, and will shape the changing balance of power"; and "the implications of strategic competition, mean it is no longer feasible to maintain a broad-based regional capability edge", requiring a "focus on asymmetric advantages and ensure […] parity or a qualitative advantage in critical military technology areas".[41] Accordingly, the Australian Department of Defence is working on acquiring capabilities focused upon their value to strategic deterrence, and enhancing integration across the Indo-Pacific region. Part of this strategy is to reinforce existing allegiances, but also to bolster Australia's sovereign defense industry and

[39] Australian Government, Department of Defence, Initial Government Response to the Review of the Defence Trade Controls Act 2012, n.d., https://www.defence.gov.au/sites/default/files/2020-10/Initial_Government_Response.pdf.

[40] Australian Government, "National Defence: Defence Strategic Review", public version, 2023, https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review; The Hon Anthony Albanese (Australian Prime Minister) and The Hon Richard Marles (Australian Defence Minister), "Joint Media Release: Release of the Defence Strategic Review", April 24, 2023, https://www.minister.defence.gov.au/media-releases/2023-04-24/release-defence-strategic-review. Jake Evans, "The Defence Strategic Review triggered on of the greatest changes in Australia's military since WWII. Here's what will change", *ABC News Online*, April 24, 2023, https://www.abc.net.au/news/2023-04-24/defence-strategic-review-key-takeaways/102260364.

[41] Australian Government, "National Defence: Defence Strategic Review", p. 75.

its capability to influence smaller states in the Indo-Pacific region.[42] From a technology perspective, this necessarily requires military capability that is interoperable with key partners, like the US and the UK, but capable of sustainment independently by Australian industry. Equally, as a partner of the AUKUS deal, Australia will no doubt seek to demonstrate its value not merely through its geographic advantages to the US and UK defense strategy, but also in reciprocating in the sharing of military innovation. Thus, the import, export, and re-export of military technology in Australia have renewed attention from the Australian, US, and UK governments.

From the perspective of the Australian government's priorities, the specific types of capabilities being considered can be discerned from several recent strategic reviews and announcements. For example, the recent AUKUS agreement identifies 'pillar two' technologies, in addition to the announcement regarding the acquisition of nuclear-powered submarines, including cyber capabilities, electronic warfare, quantum technology, hyper-sonics, AI, and autonomous military capabilities.[43] The recently announced Australian government technology priorities further identify the focus of critical technologies in Australia:

- "advanced manufacturing and materials technologies
- artificial intelligence (AI) technologies
- advanced information and communication technologies
- quantum technologies
- autonomous systems, robotics, positioning, timing and sensing
- biotechnologies
- clean energy generation and storage technologies".[44]

Exercises run between the defense industry and the Australian Defence Force also give insight into the types of technologies that are the focus of current activities: such as the Australian Army Robotic Expo, the Australian Army Quantum Technology Challenge, and the Australian

[42] Australian Government, "National Defence: Defence Strategic Review", pp. 8, 32, 45, 81 and 82.

[43] "Agreement between the Government of Australia, the Government of the United Kingdom of Great Britain and Northern Ireland, and the Government of the United States of America for the exchange of naval nuclear propulsion information", conclusion date: February 8, 2022, *Treaties and International Agreements Registered or Filed and Recorded with the United Nations Secretariat*, no 57347 (2022), https://treaties.un.org/Pages/showDetails.aspx?objid=08000002805edc16.

[44] Australian Government, Department of Industry, Science and Resources, "List of Critical Technologies in the National Interest", Critical Technologies Statement, May 19, 2023, https://www.industry.gov.au/publications/list-critical-technologies-national-interest.

Navy's Autonomous Warrior maritime exercise.[45]

The flip side of the export control focus is on technologies that, if not appropriately controlled, may have negative national security impacts. Australia's force posture (that is, its defensive security footing rather than its force structure) is anticipated to be reviewed imminently, "amid a deteriorating strategic situation".[46] Most recently, statements from Australian intelligence heads flagged that the foreign intelligence service threat and threats from espionage are at an "all-time high".[47] Australia's Parliamentary Committee on Intelligence and Security has focused some of its recent reform efforts on counter-foreign interference at universities, linked directly to the alleged heightened risk of technologies being used by adversaries for military ends.[48] The 2023 proposal to amend the Defence Trade Controls Act almost solely focused on enhancing protections on access to controlled technologies, rather than adjusting the broader system to align with recommendations of the Thom Review.[49] In 2019, the government went so far as to establish a University Foreign Interference Taskforce aimed at building "trust and resilience" but aimed at countering foreign interference in the Australian university sector.[50]

---

[45] "Australian Army Quantum Technology Challenge", Australian Army Research Centre, August 11, 2022, https://researchcentre.army.gov.au/event/army-quantum-technology-challenge-2022; "Australian Army Robotics Expo 2022", Australian Army Research Centre, August 29, 2023, https://researchcentre.army.gov.au/event/army-robotics-expo-2023; Department of Defence, "Press Release: Exercise Autonomous Warrior Testing New Technologies to Meet Emerging Security Challenges", May 16, 2022, https://www.defence.gov.au/news-events/releases/2022-05-16/exercise-autonomous-warrior-testing-new-technologies-meet-emerging-maritime-security-challenges

[46] Parliament of Australia, "The state of Australia's defence: a quick guide", Quick Guides, July 27, 2022, https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/pubs/rp/rp2223/Quick_Guides/StateofAustraliasDefence.

[47] "Foreign Interference at All Time High: ASIO Boss Says", *The Sydney Morning Herald,* February 22, 2023, https://www.smh.com.au/national/foreign-interference-at-all-time-high-asio-boss-says-20230222-p5cmfk.html

[48] Australian Parliamentary Joint Committee on Intelligence and Security, *Report: Inquiry into national security risks affecting the Australian higher education and research sector*, March 2022, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/NationalSecurityRisks/Report, pp. 3, 47-55.

[49] James Riley, "Defence export changes are a disaster for local deep tech companies", *InnovationAus News*, November 14, 2023, https://www.innovationaus.com/defence-export-changes-are-a-disaster-for-local-deep-tech-companies/.

[50] Australian Government, Department of Education, "Guidelines to Counter Foreign Interference in the Australian University Sector," (University Foreign Interference Taskforce, 2019), https://www.education.gov.au/guidelines-counter-foreign-interference-australian-university-sector/university-foreign-interference-taskforce#:~:text=The%20UFIT%20brings%20together%20the%20university%20sector

Accordingly, there are capabilities, the sharing of which could be damaging to Australia's national security interests—as well as that of its allies—require control.[51]

Introduction to Australia's export control regime

Australia's export control regime represents a balance between two competing strategic interests. The first relates to Australia's national security and the need to prevent the export of military goods and technology to those who may threaten Australia's security. This extends to preventing military goods and technology that can be used in conventional, chemical, biological, and nuclear weapons, from being transferred to individuals, states, or groups with interests prejudicial to Australia's interests.[52] The second interest is to ensure Australia's sovereign industry is able to support Australia's Defence Force by providing "essential skills, technology, intellectual property, financial resources and infrastructure within our defense industrial base".[53]

Australia's export control regime also furthers national interests by minimizing regional and international instability and conflict, ensuring the Australian Defence Force maintains a capability edge, while also complying with its international obligations to prevent illicit and irresponsible trade in conventional weapons and proliferation of weapons of mass destruction.[54] It also supports Australia's international obligations under multilateral export control regimes intended to reduce the proliferation of chemical, biological, and nuclear weapons through international best practices, consistency of practice, and coordination of export controls.[55] Further it is designed to regulate the export of

---

%20and,Australian%20universities%20can%20continue%20to%20produce%20world-class%20research.

[51] "Australia to Toughen Export Controls over Fears Technology Could Fall into Hands of Foreign Armies", *The Guardian*, January 2021, https://www.theguardian.com/australia-news/2021/jan/06/australia-to-toughen-export-controls-over-fears-technology-could-fall-into-hands-of-foreign-armies; Australian Government, "National Defence: Defence Strategic Review", p. 33.

[52] Thom AM, *Independent Review of the Defence Trade Controls Act 2012*, p.11.

[53] "Sovereign Industry Capability Requirements", Australian Government, Department of Defence, accessed 23 January 2023, https://www.defence.gov.au/business-industry/capability-plans/sovereign-industrial-capability-priorities.

[54] "Defence Export Controls*:* Exports explained"*,* Australian Government, Department of Defence, accessed 23 January 2023, https://www.defence.gov.au/business-industry/export/controls/export-controls/export.

[55] "Legislation, regimes and agreements", Australian Government, Department of Defence, Defence Export Controls, accessed 23 January 2023,

capabilities to "support international efforts to stem the proliferation of conventional, chemical, biological, and nuclear weapons and the systems that deliver them".[56] The control regime is centered on a statutory instrument describing controlled goods and technology. This list-based regulatory paradigm, based primarily on physical goods, is increasingly challenged by software-based EDT.[57]

As export control is a national system, it is enabled by federal legislation designed to regulate the export, transfer, and brokering of goods and technologies across Australia's borders. The focus of export control is "controlled goods and technology" which are those that have either a specific military purpose or are inherently lethal, or commercial goods that can be adapted for a military purpose or used in the development and production of chemical, biological, or nuclear weapons systems.[58] Controlled goods include tangible goods such as weaponry and blueprints and intangible goods including software and emails.[59]

The principle laws are the Customs Act 1901(the Customs Act) and the Defence Trade Control Act 2012 (the DTC Act).[60] The Customs Act regulates the 'export' of defense and strategic goods and technologies through Regulations 13E-EK of the Customs (Prohibited Exports) Regulations 1958 (the Regulations).[61] These regulations prohibit the export of certain goods listed on the DSGL without an export permit or certificate of clearance by the Minister for Defence or an authorized person.[62] In contrast, the DTC Act broadens the range of controlled activities to include the 'supply' and 'publication' of intangible technology and the 'brokering' of DSGL goods and technologies.[63] The DTC Act also

---

https://www.defence.gov.au/business-industry/export/controls/export-controls/legislation-regimes-agreements#International.

[56] "Approach to Compliance: Defence Export Controls and Compliance", Defence Export Controls, Australian Government, Defence, accessed 23 January 2023, https://www.defence.gov.au/business-industry/export/controls/compliance/approach

[57] "LAWS and Export Control Regimes", (working paper, iPRAW).

[58] Commonwealth of Australia, Defence Trade Controls Bill 2011, Explanatory Memorandum, General Outline, 2010 – 2011, http://www5.austlii.edu.au/au/legis/cth/bill_em/dtcb2011217/memo_0.html.

[59] Commonwealth of Australia, Defence Trade Controls Bill 2011.

[60] Commonwealth of Australia, Customs Act 1901, December 8, 2021, legislation.gov.au/Details/C2022C00017; Commonwealth of Australia, Defence Trade Control Act 2012, July 1, 2018, https://www.legislation.gov.au/Details/C2018C00318.

[61] Commonwealth of Australia, Customs (Prohibited Exports) Regulations 1958, December 21, 2021, https://www.legislation.gov.au/Details/F2022C00069.

[62] Minister for Defence, Defence and Strategic Goods List 2021, August 25, 2021, https://www.legislation.gov.au/Details/F2021L01198.

[63] Commonwealth of Australia, Defence Trade Controls Act 2012; for a general description of the Australian regime, see: Australian Government, "Module Two –

provides for offenses in the handling of items covered in the Defense Trade Cooperation Treaty between Australia and the US.[64]

The DSGL is a statutory instrument under the Defence Trade Control Act 2012.[65] It also regulates the export of uncontrolled goods or technology that have a military end-use and reflects Australia's obligations under multilateral, non-proliferation, and export control regimes of which Australia is a participating state.[66] These regimes are supported by several other international agreements and initiatives that Australia has incorporated into its domestic law.[67]

Unlike the US approach, the Australian system combines the controlled goods lists into one legislative instrument.[68] Both lists are managed by the Defence Export Control office, resident in the Department of Defence.[69] The DSGL was most recently updated in August 2021 and is described as the "centrepiece of Australia's export control system".[70] It is divided into two parts:

a. Part 1 covers military and related goods, including software and

---

Overview of Australia's Export Controls", Department of Defence, Defence Export Controls, accessed January 23, 2023, https://www.defence.gov.au/business-industry/export/controls/training-faqs/awareness-training/module-two.

[64] Commonwealth of Australia, Defence Trade Controls Act 2012.

[65] Minister for Defence, Defence and Strategic Goods List 2021.

[66] These laws implement Australia's obligations under four key international regimes: the Australia Group, the Missile Technology Control Regime, the Nuclear Suppliers Group, and the Wassenaar Agreement.

[67] The Arms Trade Treaty; Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction (Biological Weapons Convention); Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction (Chemical Weapons Convention); United Nations Conventional Arms Register; United Nations Security Council Resolution 1540 – Non-proliferation of weapons of mass destruction; United Nations Security Council Resolution 1673 – Non-proliferation of weapons of mass destruction.

[68] "Export Licensing (ITAR & EAR)", US Department of Commerce, accessed January 23, 2023, https://www.bis.doc.gov/index.php/documents/technology-evaluation/781-export-licensing/file

[69] Parliament of Australia, *Principles and practice – Australian defence industry and exports. Inquiry of the Defence Sub-Committee,* (Joint Standing Committee on Foreign Affairs, Defence and Trade, 2015), Chapter 6: Operations of the Defence, https://www.aph.gov.au/-/media/02_Parliamentary_Business/24_Committees/244_Joint_Committees/JFADT/Foreign_Affairs_Defence_and_Trade/Defence_Industry/Principles_and_Practice_-_Australian_Defence_Industry_and_Exports.pdf?la=en&hash=47B14B5C847BECE66F0D6186AEE324D4BA7C1232.

[70] Parliament of Australia, *Principles and practice.*

technologies designed or adapted for use by the armed forces or goods that are inherently lethal. This includes parts and accessories and non-military firearms, ammunition, and explosives.

b. Part 2 covers dual-use goods which include equipment, software, and technologies developed to meet commercial needs, but which may be used as military components or for the development or production of military systems or weapons of mass destruction.[71] Part 2 is further subdivided into ten categories.[72]

Critically, in relation to emerging and disruptive technologies, the system seeks to regulate software by articulating specific system design criteria, that trigger regulation. This is best illustrated by having regard to a specific example and comparing its regulation to that of the EU approach. Concerning communications surveillance systems, specific design criteria are listed in the DSGL, articulating hardware requirements, and the capability of the system, with a further articulation of the specific design intent of the capability.[73] This approach is very functionally specific and may not capture secondary mapping processes that result in a similar

---

[71] Defence and Strategic Goods List Explanatory Memorandum, 27 August 2021, available at: https://www.legislation.gov.au/F2021L01198/latest/text/explanatory-statement.

[72] 0 – Nuclear Materials; 1 – Materials, Chemicals, Micro-organisms and Toxins, 2 – Materials Processing, 3 – Electronics, 4 – computers, 5 – Telecommunications and 'information security', 6 – Sensors and lasers, 7 – Navigation and avionics, 8 – Marin, 9 – Aerospace and propulsion: Defence and Strategic Goods List 2021.

[73] Defence and Strategic Goods List 2021, Part 2 Dual-Use List, Category 5, Part 1 – Telecommunications, 5A1, 'Systems, Equipment and Components' defines controlled items as, inter alia:

j. IP network communications surveillance systems or equipment, and specially designed components therefor, having all of the following:
    1. Performing all of the following on a carrier class IP network (e.g., national grade IP backbone):
        a. Analysis at the application layer (e.g., Layer 7 of Open Systems Interconnection (OSI) model (ISO/IEC 7498-1));
        b. Extraction of selected metadata and application content (e.g., voice, video, messages, attachments); and
        c. Indexing of extracted data; and
    2. Being specially designed to carry out all of the following:
        a. Execution of searches on the basis of "hard selectors"; and
        b. Mapping of the relational network of an individual or of a group of people.

    Note: 5A001.j. does not apply to systems or equipment, specially designed for any of the following:
        a. Marketing purpose;
        b. Network Quality of Service (QoS); or
        c. Quality of Experience (QoE)

surveillance outcome, and associated concerns pertaining to data privacy.

Conversely, the EU control measures applied to communications surveillance technology are more purposive, insofar as they create controls of additional cyber-surveillance technologies, beyond the explicit technology listed within the Regulation, to be considered based upon their intended use and in particular, if their use might be "in connection with internal repression and/or the commission of serious violations of international human rights and international humanitarian law".[74] This broader approach is more suited to addressing the unpredictable and rapidly changing nature of critical technologies.

Finally, for goods not listed on the DSGL, but which are suspected could be used for a military or weapon of mass destruction 'end-use', their export may be prohibited by the Weapons of Mass Destruction (Prevention of Proliferation) Act 1995 (WMD Act)[75] or the Charter of the United Nations Act 1945 which implements UN sanctions including arms embargoes, bans on the import and export of certain goods. This is complemented by Australia's autonomous sanctions under the Autonomous Sanctions Act 2011 administered by DFAT. These export control laws apply to 'Australian persons' who are defined by the DTC Act to include Australian nationals and in some cases Australian citizens and residents overseas.[76]

The Thom Review considered, among other things, whether the Act aligned with international export control best practices and provided appropriate regulation and security for controlled technologies. Critically, it identified that the Act in its current form is "inadequate" in "control[ling] emerging and sensitive military and dual-use technology".[77] Rectification of this gap was recommended by legislative amendment, which was

---

[74] Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast), 2021, Official Journal (L 206), Article 5.

[75] Australia, Weapons of Mass Destruction (Prevention of Proliferation) Act 1995, No 38, November 6, 2018, https://www.legislation.gov.au/Details/C2018C00445.

[76] The Defence Trade Controls Act 2012, section 4, defines an Australian Person as:

a. the Commonwealth, a State or a Territory or an authority of the Commonwealth, a State or a Territory; or
b. an individual who is an Australian citizen; or
c. an individual who is, within the meaning of the Migration Act 1958, the holder of a permanent visa; or
d. a body corporate incorporated by or under a law of the Commonwealth or of a State or Territory.

[77] Thom AM, *Independent Review of the Defence Trace Controls Act 2012.*

accepted by the Australian Government. As of December 2023, this appears to still be under consideration by a multidisciplinary working group meeting to develop legislative proposals to ameliorate this risk, despite the second round of statutory legislative review commencing in November 2023.[78]

Australia's export control regime applied to EDT

Having outlined Australia's export control laws, it is possible to identify how the central challenges relating to critical technologies, including AI, are addressed by Australia's existing regime. There are a number of key features of Australia's export control regime that influence its ability to regulate critical technology. These features include:

a) The DSGL is a statutory list-based control regime designed to regulate the export of tangible goods.[79]
b) The national system adopts the Wassenaar Arrangement's catch-all clauses relating to the definition of dual-use technologies focused on 'major or key elements' that relate to the "indigenous development, production, use or enhancement of military capabilities".[80]
c) Statutory end-use agreements are limited only to technologies that are related to weapons of mass destruction or implementing UN sanctions (administered by a different Department), or deemed to prejudice the security, defense, or international relations of Australia.[81]
d) The legislation has limited extra-territorial application in that it only applies to Australian persons.[82]

---

[78] Australian Government, Initial Government Response to the Review of the Defence Trade Controls Act 2012. See also, Thom AM, *Independent Review of the Defence Trace Controls Act 2012*; Richard Marles, "Review of Defence Trade Controls Act 2012".

[79] Commonwealth of Australia, Defence Trade Controls Act 2012, section 4; Commonwealth of Australia, Customs Act 1901, section 1112(2A)(aa).

[80] Flynn, "Recommendation on Export Control for Artificial Intelligence"; Wassenaar Agreement, Criteria for the Selection of Dual-Use Items, adopted in 1994 and amended by the Plenary in 2004 and 2005, https://www.wassenaar.org/app/uploads/2019/consolidated/Criteria_for_selection_du_sl_vsl.pdf

[81] Commonwealth of Australia, Weapons of Mass Destruction (Prevention of Proliferation) Act 1995 sections 7, 9(2), 10(2), 11(2); Commonwealth of Australia , Autonomous Sanctions Act 2011 section 10; Commonwealth of Australia, Autonomous Sanctions Regulations 2011 Regulation 5D; and Commonwealth of Australia, Customs Act 1901, section 112BA.

[82] Commonwealth of Australia, Defence Trace Controls Act 2012, section 4.

e) While the DSGL can be updated by issuing a new statutory instrument and does not need to go before the Federal Parliament, it is not quickly responsive to specific technological advancements.[83]

Additionally, the Australian regime is highly dependent on the controls implemented by the US—through the ITAR—applying extra-territorially and controlling any Australian industry seeking to incorporate American technology into their own or engage in trade with the US. These regulations are highly process-driven and have been seen by industry and commentators to stifle innovation and export of Australian technology.[84]

Although there are moves afoot to mitigate the impact of ITAR upon Australian defense industry, through the 2023 US proposal to create specific exemptions for Australian industry from the Regulations, this change will take some time, is limited in scope, and there will remain significant overheads for Australian industry in applying the other administrative burdens associated with the use of US military technologies (such as security clearances, nationality-based employee discrimination, data security requirements and so on).[85] Thus, there are questions about the benefits of more closely aligning the Australian export control process to mimic the requirements of the US to alleviate some of these burdens, noting the stated intent of the Australian government to "greater advanced scientific, technological and industrial cooperation in the [Australia-US] Alliance."[86]

---

[83] Thom AM, *Independent Review of the Defence Trade Controls Act 2012,* p. 40.

[84] Brandon How, "Australia works to soften US defence export controls for AUKUS", *InnovationAus,* November 15, 2022, https://www.innovationaus.com/australia-works-to-soften-us-defence-export-controls-for-aukus/.

[85] Notably, the exemption passed in the 2023 US Fiscal Authorities Act requires that Australian markets can only be treated as 'domestic' US markets exempt from ITAR requirements if the US has exhausted its own domestic supply opportunities first: National Defense Authorization Act for Fiscal Year 2024 (H.R. 2670, NDAA 2024); White House, Press Release, "Australian United States Joint Leader's Statement: An Alliance for Our Times", May 23, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/05/20/australia-united-states-joint-leaders-statement-an-alliance-for-our-times/); Tim O'Callaghan, Travis Shueard, Laura Coppola, "AUKUS, ITAR, Export Control Reform and the Australian Defence Industry", PiperAlderman Insight, May 8, 2023, available at: https://piperalderman.com.au/insight/aukus-itar-export-control-reform-and-the-australian-defence-industry/); Brandon How, "ITAR exemptions for AUKIS should come via Biden executive order", *InnovationAus,* May 18, 2023, https://www.innovationaus.com/itar-exemptions-for-aukus-should-come-via-biden-executive-order/; Bryant Harris, "Congress lays groundwork for AUKUS export control reform", *DefenseNews*, March 23, 2023, https://www.defensenews.com/congress/2023/03/22/congress-lays-groundwork-for-aukus-export-control-reform/.

[86] Australian Government, "National Defence: Defence Strategic Review", p. 45, para 6.5.

Addressing gaps and uncertainty in Australian export control applied to EDT

In undertaking an independent review of the existing legislation dealing with Australian defense trade controls, the Thom Review made a general recommendation pertaining to emerging and disruptive technology and the inadequacy of the DTC Act in regulating them.[87] Specifically, it was accepted by the Australian government that:

> "a working group, led by an independent person, [will] develop options to address the identified gaps in the Defence Trade Controls Act 2012 (DTC Act) … to develop practical, risk-based legislative proposals to amend the DTC Act to enhance the government's ability to prevent the transfer of defence and dual-use technology to entities that may use it in a manner contrary to Australian interests or who are acting on behalf of a foreign power."[88]

As of December 2023, no further public information has been released in relation to the Working Group, or the status of this risk-based approach.

This section seeks to identify how this risk-based recommendation applies to the specific challenges presented by AI.

1. Firstly, in addition to the broader counter-proliferation objectives of export control noted earlier, a primary objective of any effective export control regime should be to address the proliferation of intangible technologies that present strategic risks.[89] To achieve this, a primary question is whether the export control needs to reorientate its focus from the Cold War era towards a more country-agonistic counter-weapons of

---

[87] Thom AM, *Independent Review of the Defence Trade Controls Act 2012*.

[88] The Defence Export Controls site has not been updated since 2018 in relation to the review (see Australian Department of Defence, Defence Trade Controls Act 2018, available at: https://www.defence.gov.au/about/reviews-inquiries/defence-trade-controls-act-review-2018); and the latest governmental publication relating to the implementation of the 2018 Defence Exports Controls Strategy contains no reference to the legislation updates, nor the working group established under the 2018 Thom Review: see Australian National Audit Office, "The Auditor-General Report No 6, 2020-21. Performance Audit, design and Implementation of the Defence Export Strategy: Department of Defence", (Australia: 2020), https://www.anao.gov.au/sites/default/files/Auditor-General_Report_2020-21_6.pdf#:~:text=The%20strategy%20sets%20out%20a%20strategic%20goal%20and,Strategic%20Goal%20and%20the%20Objectives%20of%20the%20Strategy%E2%80%99.

[89] "Defence Export Strategy", Department of Defence, accessed July 18, 2023, https://www.defence.gov.au/business-industry/export/strategy.

mass destruction proliferation strategy.[90]

Critically, the US has adopted this approach insofar as they have broadened their controls from general technology controls to include end-use and end-user controls focusing upon both states and companies (despite the preponderance of enforcement actions being on specific states).[91] The challenge for Australia's regime is that it is currently capability-oriented, and country-agnostic. That is, there would need to be an update to the underpinning implementation of controls, moving away from a list-based control, and applying assessments against broader policy considerations 'on a case-by-case basis', as is currently the case.[92]

2. Secondly, the regime should focus not only on national security but also more stringently comply with human rights objectives and balancing national innovation priorities.[93] This requires the inclusion of state-specific controls aimed not only at traditional dual-use technologies but also removing the requirement for a technology to have an inherently military nexus or end-use. In this way, the regime can address those states, such as China, whose threat to Australia's national security is derived from their policy of civil-military fusion and achieving economic strategic advantage.

The expansion of the dual-use definition to achieve this particular end-use definition could be readily achieved: the DTC Act is set up to create the DSGL based upon what is considered dual-use, or required to be controlled by the DSGL, rather it established who can add items to the list, and then what enforcement or permit requirements are associated with those items that are listed.[94] That is, the head legislation itself does not limit the requirements as to what can be listed. Accordingly, it is feasible that there could be additional entries to the list that describe both the item and its end-use locations, or simply that the definition of dual-use applied in the DSGL can be expanded to include goods utilized for breaches of human rights.

---

[90] Kevin Wolf and Emily S. Weinstein, "COCOM's Daughter?", *WorldECR*, 100 (June 2021), https://cset.georgetown.edu/wp-content/uploads/WorldECR-109-pp24-28-Article1-Wolf-Weinstein.pdf.

[91] Sibylle Bauer and Mark Bromley, "Detecting, Investigating and Prosecuting Export Control Violations: European Perspectives on Key Challenges and Good Practices", SIPRI, 2019, https://www.sipri.org/sites/default/files/2019-12/1912_sipri_report_prosecuting_export_control_violations_0.pdf.

[92] "Defence Export Strategy", Department of Defence.

[93] Australian National Audit Office, "The Auditor-General Report No 6, 2020-21", p. 37.

[94] Defence Trade Controls Act 2012, section 3: "This Act regulates dealings in items listed in the Defence and Strategic Goods List (the *DSGL*) and in items covered by the Defense Trade Cooperation Treaty between Australia and the United States of America".

The existing dual-use definition is found in the DSGL's description of Part 2 of the List (which deals with dual-use items): "Dual-use goods comprise equipment and technologies developed to meet commercial needs but which may be used either as military components, or for the development or production of military systems or weapons of mass destruction".[95] Neither this definition nor other provisions in the legal text expressly allow for the control of items used in violation of human rights concerns. In contrast, the EU, while not explicitly referring to human rights violations in the dual-use items definition, includes the so-called catch-all clause in the regulation. This clause can be invoked to control unlisted cyber-surveillance items that may be used for "internal repression and/or the commission of serious violations of international human rights and international humanitarian law [IHL]."[96]

Australia could incorporate in its legislation unilateral controls for the purpose of human rights compliance—rather than just having human rights compliance as one of many competing considerations in a decision to approve the export of an item on the DSGL. The item itself could be prohibited from export-based upon its ability to be utilized for purposes that breach human rights.

3. Thirdly, and building upon the second, incorporating in the list dual-use definitions that focus upon end-uses and uses will better enable a response to foreign appropriation strategies that further attempt strategic dominance in preparation for hostilities.[97] This allows national export control regulation to address both national security and human rights concerns. This pivot will also capture the types of technologies that are used by autocratic regimes for human rights abuses: items that are not inherently WMD or conventionally used for military applications but can be used to breach human rights. For example, capabilities used for mass surveillance of populations, or DNA tracking of individuals, might not be military-specific and trigger existing export control definitions but should be controlled to ensure that exported equipment is not used to commit human rights abuses. Here, the Australian example falls behind the EU

---

[95] Defence Strategic Goods List 2021, Division 2—Simplified outline of the Defence and Strategic Goods List.

[96] Mark Bromley, "The EU Dual-use Regulation, cyber-surveillance and human rights: the competing norms and organised hypocrisy of EU export controls", *Defence Studies*, 23:4, 2023, p. 657.

[97] Gregory Allen, Emily Benson, William Alan Reinsch, *Improved Export Controls Enforcement Technology Needed for U.S. National Security*, (Centre for Strategic and International Studies, November 2022), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/221130_Allen_Export_Controls.pdf?VersionId=xmB4Pqusa5lsBnQzNBh1RqebwJKcQvmr

regulations (relating to cyber-surveillance technologies in particular).[98]

In the same way that the DTC Act provides authority for a Ministerial direction to limit the supply of certain technologies on the basis of prejudice to security, defense, or international relations of Australia, more stringent criteria could be inserted in relation to the use of already listed critical technologies linked to potential human rights abuses.[99] While the Ministerial discretion is broad and lists many competing considerations, this list could easily be focused on specifying absolute bans on the provision of goods that carry a risk of end-use breaches of international human rights and international humanitarian law, rather than listing potential human rights abuses as one of many competing considerations. Given the Defence Export Control office states it undertakes a 'case-by-case' assessment of all export applications for advice to the Minister on any disapprovals,[100] this would be a readily achievable amendment, albeit one that came with a significant resourcing impost.

4. Finally, setting strategic priorities also assists in changing the domestic legislative effort: what is Australia's key aim in controlling sensitive technology? Is Australia's export control to be a focus for technology exchange with key allies, or is supporting Indo-Pacific states a greater national security outcome securing the loyalty of those states; therefore, is more risk in export to those states acceptable? Conversely, if the aim of the regime is focused on delaying the technological advancement of particular states, then the approach to control will necessarily be different. The recent DSR demonstrates the reliance that Australia's future defense strategy has upon interoperability with its allies. However, statements made regarding trade with China (and not following the US lead on semiconductor regulation) make it uncertain where the governmental priority in export control lies.[101]

---

[98] European Union, Council Common Position 2008/944/CFSP of 8 December 2008, Defining common rules governing control of exports of military technology and equipment, 2008, Official Journal (L 335/99); Mark Bromley, "A search for common ground: export controls on surveillance technology and the role of the EU", About Intel: European Voices on Surveillance, February 12, 2020, https://aboutintel.eu/surveillance-export-control-eu/.

[99] Defence Trade Controls Act 2012, section 33.

[100] "Defence Export Strategy", Department of Defence.

[101] Joseph Brooks, "Australian won't follow US with a China semiconductor trade wall", *InnovationAus,* November 14, 2022, https://www.innovationaus.com/australia-wont-follow-us-with-a-china-semiconductor-trade-wall/#:~:text=Australia%20has%20no%20plans%20to%20follow%20the%20United,Albanese%20secures%20a%20meeting%20with%20President%20Xi%20Jinping, citing Australian Trade Minister, Don Farrell, 'Australian APEC Centre Address', 14 November 2022.

Suggested amendments to the current Australian regime to properly account for EDT

While the Thom Review identified that the current regime is not fit for purpose, there remains a need for the Government-endorsed working group, established in 2019, to progress practical-based adjustments to the domestic export-control legislative regime.[102] This section seeks to identify a number of international practices that may be applied to rectify the four key gaps, identified above, in terms of what kind of legislative amendments could be considered, having regard to the policy objectives of the regime described above.

Considering the above four feeder issues related to addressing the Thom Review's recommendations to 'close the gap', the below commentary provides potential solutions to those issues in the Australian context.

1. In relation to the need to address the proliferation of intangible technologies that present strategic risks, the balancing requirement notated in the Thom Review can be achieved by introducing a requirement to consider more specifically the end-use and end-user of the sensitive goods, rather than just regulating the type of good on the DSGL.
2. Amending the dual-use definition from the existing definition will better enable a response to foreign appropriation strategies which further attempts at strategic dominance in preparation for hostilities. This could be achieved by duplicating the functions of the Australian Sanctions Office within the Department of Defence's Export Control Office; with the adoption of regulatory and legislative measures similar to the existing implementing sanctions regulations.[103] This adoption of the country-specific sanctions regulations could feasibly bolster cooperation with Five Eyes on enforcement by aligning end-use obligations more closely with the extra-territorial reach of US export controls in line with recent undertakings.[104]
3. Balancing human rights with national security and innovation priorities can be achieved through the introduction of purposive

[102] Thom AM, *Independent Review of the Defence Trade Controls Act 2012,* p. 13.

[103] See generally: Commonwealth of Australia, Charter of the United Nations (Dealing with Assets) Regulations 2008;and Commonwealth of Australia, Autonomous Sanctions Regulations 2011.

[104] Bureau of Industry and Security, US Department of Comments, "Press Release: Five Eyes Partners Agree to Formalize Cooperation on Export Control Enforcement", June 28, 2023, https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3294-2023-06-28-bis-press-release-five-eyes-export-enforcement-coordination/file.

> definitional criteria relating to the potential use of the technology, modeled upon the EU example dealing with cyber surveillance. The current language in section 25A of the DTC Act specifies that permits for the export of DSGL goods must consider competing criteria regarding whether the permit would "prejudice the security, defence or international relations of Australia". This list does not provide mandatory requirements to deny permits that would risk breaches of Australia's legal obligations. The specific criteria in the regulations, that the decision-maker 'must have regard to', is: "the risk that the DSGL technology or the goods may be used to commit or facilitate serious abuses of human rights".[105]

It is relevant to reinforce that it is unclear how many, if any, of the above considerations have been built into the Australian update to its export control regime, as there is yet to be any publicly released information detailing the progress of the status of the Working Group established by the Thom Review. That said, noting that it has been a number of years since the regime has been identified as being outdated, and there has been a significant change in the export control and sanctions landscape since this time, it is critical that any adopted changes must take into account country-specific adaptions, and a move from a static controlled items list to one that can be more readily adapted to respond to trends in EDT, as the potential uses of these technologies continue to crystalize as their development (and foreshadowed use cases) mature.

It should be further noted that the above changes are meaningful if undertaken by Australia unilaterally, however, will only be truly effective if they are adopted in a multilateral way. This paper supports the proposals of academics, and an emerging diplomatic effort from US Congress, to create a fifth international multilateral regime to add to the existing four export control arrangements;[106] and suggests that Australia's leadership in this field could be readily secured through adopting the above offered legislative amendments in anticipation of, and in alignment with, any

---

[105] Commonwealth of Australia, Defence Trade Controls Regulations 2013, Regulation 8.

[106] See Kevin Wolf fand Emily Weinstein, Center for Security and Emerging Technology Event, 'A New Export Control Regime for the 21st Century: How Russia's Invasion has Created an Opportunity for a Techno-Democracy Partnership', 28 May 2022, available at: https://cset.georgetown.edu/event/a-new-export-control-regime-for-the-21st-century/, citing Kevin Wolf and Emily S. Weinstein, "COCOM's Daughter?", WorldECR, 100 (June 2021), https://cset.georgetown.edu/wp-content/uploads/WorldECR-109-pp24-28-Article1-Wolf-Weinstein.pdf; Under Secretary of Commerce for Industry and Security Alan Estevez, 'Estevez: New export control regime needed for 'future scenarios' with China, Taiwan', World Trade Online, 20 July 2022, available at: www.insidetrade.com/daily-news/estevez-new-export-control-regime-needed-'future-scenarios'-china-taiwan

future 'fifth wave' of export control.

Conclusion

The proposed update to Australia's Defence Trade Controls Act could readily correct identified deficiencies in its current export control regime, as identified in the Thom Review. A few key adjustments to the legislation can considerably enhance its effectiveness: Australia's existing domestic legislation dealing with the Wassenaar Agreement's List of Dual-Use Goods and Technology, coupled with the Australia Group's catch-all clause, provide a promising starting point to address the challenges presented by export control regimes in managing new and disruptive technologies such as AI. The list is the starting point, but the ability to readily adjust it is critical to ensuring its relevance.

This paper has outlined the structure of Australia's export control legislation, and how it differs from other regimes. These differences mean that simply adopting other state solutions to export control practices will not work in the Australian context unless the entire system is reoriented. Despite the recent US relaxation of its export control arrangements to support the AUKUS deal and make trade with Australia easier, current Australian political statements, and the government's accepted recommendations relating to overhauling the Defence Controls Act in 2019 indicate that this will be unlikely. There will be ongoing tensions between reinforcing Australian sovereignty and enhancing trade freedoms focused on national defense.

The creation of an industry-engaged, flexible, and agile export control process will be critical to both empowering small and medium-sized enterprises and academia to support domestic innovation while countering national security threats and human rights abuses flowing from the proliferation of these technologies. Australia is in a unique position to make these bold adjustments, as a consequence of the current legislative review aligning with Defence's Strategic Review and the recent AUKUS agreement. It would be a reduction in the high esteem in which Australia's export control efforts have been held, through decades of leadership in this field, should this opportunity be squandered by only implementing incremental system change, rather than embracing this unique opportunity to lead in creating an enhanced and flexible export control regime.