Submission to the Department of Industry, Science and Resources

Supporting Responsible AI Discussion Paper

Outline and Summary

Thank you for the opportunity to make a submission to the public discussion paper on how the Australian Government can mitigate any potential risks of AI and support safe and responsible AI practices.

This submission has been prepared in our capacity as staff of the Law and the Future of War Research Group, sited within the T.C. Beirne School of Law at the University of Queensland. However, the views expressed below are entirely those of the individual authors and are not necessarily representative of the School, The University of Queensland or any other government, organisation or agency.

We have engaged only with certain questions in the discussion paper; however, we are willing to provide additional information on our views on other questions in the discussion paper if necessary.

We are happy to provide further clarification on any area of the submission.

Broader context

It is important to recognise the broader context of this submission.

Australia is not the only jurisdiction contemplating legislative and policy changes to regulate artificial intelligence (AI). The European Union (EU) for example, has recently passed both an *AI Act*[1] and the *AI Liability Directive*[2] designed to encapsulate and prescribe certain actions with respect to the development, testing and implementation of AI by both governmental and non-governmental actors.

Direct comparison of these initiatives in the EU with Australia would be useful, but practical comparison is extremely difficult. This is because the both the source of law-making power and the supporting legislative frameworks in Australia and the EU are vastly different. For example, Australia is a Federal system with three layers of government, whilst the EU is a confederation of Members States with their own varying sources of constitutional, statutory and/or common law. Further, Australia lacks many equivalent protections which exist in the European context, such as the General Data Protection Regulation[3] (GDPR), the *Data Act*[4] and *Data Governance Act*[5] (DGA), the *Digital Markets Act*[6] (DMA) and the *Digital Services Act* (DSA).[7]

[1] Proposal for a Regulation Of The European Parliament And Of The Council Laying Down Harmonised Rules On Artificial Intelligence (Artificial Intelligence Act) And Amending Certain Union Legislative Acts.

[2] Proposal for a Directive Of The European Parliament And Of The Council on adapting non-contractual civil liability rules to artificial intelligence.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[4] Proposal for a Regulation of The European Parliament and of the Council on harmonised rules on fair access to and use of data.

[5] Proposal for a Regulation of The European Parliament and of the Council on European data governance.

[6] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828.

[7] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC.

Regulation of AI for military and "national security" purposes

Separately, we note that this consultation process seeks to excise military use of AI, as well as uses related to "national security".[8] We submit that this approach risks creating a 'two-tier' approach to the development of AI in Australia, with this risk manifesting in military AI technologies not being designed in line with broader public expectations, and aligned to Australia's general AI use principles and policies. While many AI regulatory frameworks (such as the current approach adopted by the EU)[9] specifically excise military AI technologies specifically from its regulatory approach, there have been calls to ensure broader alignment in their adopted military AI principles, and homogeny in definitions of AI, and other AI acquisition and management processes.[10] The EU AI Act also still applies to "dual use" AI technologies – i.e., those that have both a civilian and a military application. If Australia were to adopt similar regulation without including military AI, this could lead to situations where near-identical military capabilities being used side-by-side by the ADF are regulated in significantly different ways.[11]

There are also dangers associated with discriminatory treatment of civilian AI and AI used for purposes related to "national security", where that term is not specifically defined. Firstly, a blanket application of national security protections has been rightly criticised by the Independent National Security Legislation Monitor, who stated the misuse of those provisions "should never happen again".[12] Secondly, differential legal treatment may create a situation of regulatory arbitrage, incentivising companies to market their AI capabilities to "national security" agencies to avoid costly regulation.[13] Thirdly, the use of AI capabilities by military, law enforcement or intelligence agencies is generally less open to scrutiny by the public, meaning instances of legal non-compliance (even inadvertently) are harder to detect.[14]

There is also a need to ensure that all AI regulation, particularly noting the broad scope of dual-use of AI technologies, aligns with Australian domestic legal requirements. In the same way that there are limited exemptions to the use of personal data by the ADF under the Privacy Act – even in situations of armed conflict[15] – there should be limited exceptions to the adopted Australian AI-regulatory approach in terms of military use. We recognise the need for slightly different approaches in the adoption of some AI technologies for use by the military, particularly in situations of armed conflict, however, these exceptions can be limited.

[8] Safe and responsible AI in Australia Discussion paper, June 2023 at 1.1 'Scope of this paper'.

[9] The EU Council's general Approach on the AI Act excises systems designed for defence and military purposes as subject to public international law: Council of the EU Press Release, 6 December 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/.

[10] Ronja Rönnback, 'Challenges of Governing AI for Military Purposes and Spill-Over Effects of the AI Act' European Commission, AI Alliance blob, 27 February 2023, https://futurium.ec.europa.eu/en/european-ai-alliance/blog/challenges-governing-ai-military-purposes-and-spill-over-effects-ai-act.

[11] Rosanna Fanni, "Why the EU must now tackle the risks posed by military AI" (CEPS, 8 June 2023) https://www.ceps.eu/why-the-eu-must-now-tackle-the-risks-posed-by-military-ai/.

[12] Grant Donaldson, *Review into the Operation of Part 3, Division 1 of the National security Information (Criminal and Civil Proceedings) Act 2004 as it Applies in the Alan Johns Matter* (Report, 17 June 2022) at 12.

[13] Monique Mann, Angela Daly, Adam Molnar, "Regulatory arbitrage and transnational surveillance: Australia's extraterritorial assistance to access encrypted communications" (2020) 9(3) *Internet Policy Review*.

[14] See for example the AFP's use of the Auror platform: Cam Wilson, "AFP under investigation over its use of Auror surveillance technology", *The Mandarin,* 23 July 2023, https://www.themandarin.com.au/226020-surveillance-technology-auror-afp-under-investigation/.

[15] *Privacy Act 1988* (Cth), ss 7(1)(c) and 16A.

Further, Australia, as a signatory to Additional Protocol I to the 1949 Geneva Conventions, has an obligation to ensure that the use of its weapons, means and methods of warfare comply with its international legal obligations.[16] Many of these international legal obligations are incorporated into Australian domestic law, and indeed, the current Australian weapons review process includes a consideration of compliance with domestic law before a capability may be certified for use in situations of armed conflict.[17]

Accordingly, we consider that there is merit in including military and "national security" AI use in the discussion of safe and responsible AI in Australia. There remains a need for the military, law enforcement and intelligence agencies to be accountable for its use of AI, not only to government, but also to the Australia population. The wholescale excision of these uses of AI from the consultation process may lead to unnecessary schisms between the military design, development and use of AI; and lessen the likelihood that regulatory lessons are shared amongst government in relation to lessons learned by the military, and vice versa. More importantly, the use of AI by any and all Australian government entities must be aligned to the Australian public's expectations, and compliant with Australia's legal obligations.

Definitions (Question 1)

The Discussion Paper takes the definition of AI to be:

> …an engineered system that generates predictive outputs such as content, forecasts, recommendations or decisions for a given set of human-defined objectives or parameters without explicit programming. AI systems are designed to operate with varying levels of automation. [18]

Within that definition, the Discussion Paper further defines "generative AI models" and also "machine learning".[19]

Under the EU's AI Act, AI is defined as:

> …software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.[20]

Annex I of the AI Act then includes machine learning[21] as well as logic- and knowledge-based approaches,[22] and statistical approaches.[23]

Immediately, the differences in definition can be identified, with the EU's AI Act including a wider number of systems and classes of system which can be referred to as AI. However, even this more inclusive definition does not include novel uses of AI with potentially significant human impacts such

[16] *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, opened for signature 8 June 1977, 1125 UNTS 3 (entered into force 7 December 1978) ('*AP 1*'), Article 36.

[17] Australia, *The Australian Article 36 Review Process*, UN Doc CCW/GGE.2/2018/WP.6 (30 August 2018) <https://undocs.org/CCW/GGE.2/2018/WP.6>

[18] Australian Government, *Safe and Responsible AI in Australia* (Discussion paper, 1 June 2023) <https://consult.industry.gov.au/supporting-responsible-ai> 5.

[19] Ibid.

[20] AI Act art 3(1)

[21] AI Act Annex III item (a) including 'supervised, unsupervised, reinforcement, and deep learning.'

[22] AI Act Annex III item (b) including 'knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems.'

[23] AI Act Annex III item (c) 'Bayesian estimation, search, and optimization methods.'

as recommendation[24] and dynamic pricing[25] algorithms, credit assessment tools,[26] and algorithmic trading platforms.[27] Further, it is possible that certain systems may conceal their nature as “AI” from scrutiny but which are nonetheless AI for the purposes of legal regulation in the same way that certain types of data-matching and algorithmic programs in use today can be (deliberately, negligently or accidentally) mischaracterised.

For example, the recent Report of the Royal Commission into the Robodebt Scheme noted that despite a clear legislative provision allowing the exchange of information between the Australian Taxation Office and the Department of Human Services,[28] the Scheme actually operated outside that legislative framework on the basis of additional “voluntary protocols”.[29] The Royal Commission also found that despite various deeming provisions regarding decisions made by the Robodebt system, the system was not considered problematic as it was not ‘fully automated’ (even in circumstances where it appears decisions were made by the automated matching program).[30]

It is also important to consider that a similar scheme to Robodebt operated in the Netherlands between 2013 and 2019. Although that system would also not be considered “AI”, it would – as a governmental program – not be regulated by the EU’s AI Act. Again, the definition of AI is extremely important to how regulation and enforcement will be operationalised.[31]

Risks not covered by Australian approaches (Question 2)

Current Australian approaches do not adequately appreciate the possibilities for harms arising out of the “decisions” possibly being made under AI systems or technologies.

The current legal authority for computers making decisions in Australia is the decision of the Full Court of the Federal Court of Australia in *Pintarich*.[32] In that case, the court was required to determine whether an algorithm of the Australian Taxation Office generating a template letter was a “decision” in relation to a client’s General Interest Charge (GIC) on their primary debt. The majority of court did not believe that a computer could be held to have made a decision in those circumstances, saying that “…for such a decision to be made, there needs to be both a conclusion reached on the application to remit as well as an overt act.”[33] The majority went on to agree that the results of their decision in *Pintarich* was be to promote “administrative uncertainty”, such that ‘taxpayers or others dealing with government may not be able to rely on letters from government agencies communicating decisions’.

[24] Sachin Banker, Salil Khetani. ‘Algorithm overdependence: How the use of algorithmic recommendation systems can increase risks to consumer well-being’ (2019) 38(4) *Journal of Public Policy & Marketing* 500.

[25] Tabrez Y. Ebrahim, ‘Algorithms in Business, Merchant-Consumer Interactions, & Regulation’ (2020) 123(1) *West Virginia Law Review* 123, 873.

[26] Pernille Hohnen, Michael Alexander Ulfstjerne, Mathias Krabbe, ‘Assessing creditworthiness in the age of big data: a comparative study of credit score systems in Denmark and the US’ (2021) 5(1) *Journal of Extreme Anthropology* 29.

[27] Ibid.

[28] *Data-matching Program (Assistance and Tax) Act 1990* (Cth).

[29] Catherine Holmes AC SC, *Report of the Royal Commission into the Robodebt Scheme* (Final report, 7 July 2023) 449-450.

[30] Ibid, 482-484.

[31] Melissa Heikkila, “Dutch scandal serves as a warning for Europe over risks of using algorithms”, *Politico*, 29 March 2022, https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/.

[32] *Pintarich v Deputy Commissioner of Taxation* [2018] FCAFC 79; 262 FCR 41; 108 ATR 31.

[33] Ibid at [151] (Moshinsky and Derrington JJ).

However, their Honours believed that this uncertainty was warranted on the "unique" nature of the case, saying:

> …the circumstances of this case are quite unusual. The letter resulted from Mr Celantano 'keying in' certain information into a computer-based 'template bulk issue letter'. This produced a letter that, in some respects, did not reflect his intentions. **This type of situation is unlikely to arise very often**.[34] (emphasis added)

Indeed, His Honour Justice Kerr wrote (in dissent):

> Given the growing inter-dependency of automated and human decision making I am skeptical of the latter proposition assuming, as the majority concludes, the indicia of a decision require a conclusion reached after a mental process and the outward expression of the decision to reflect that conclusion. There is reason, in my view, to be concerned with giving license to such unfairness.[35]

We do not believe that the statement of the Full Court in *Pintarich* should hold true in our highly digitised, increasingly interconnected economy. Government at all levels – local, State and Federal – looks to engage with constituents in ways which are inherently digital and increasingly complex. We cannot be in that same position in relation to the development of AI technologies. Therefore, the Government should consider – as part of its review of responsible AI development – the circumstances in which AI can be used to make decisions. On that basis, any AI regulation in Australia should also then very clearly and unambiguously grapple with the concept of where an AI system or technology is making a "decision", and capture that specific point in legislative form.

The Department should also consider ancillary amendments that might be made to the concepts of regulating civil litigation into harms caused by AI. In the EU for example, the AI Liability Directive addresses civil liability, which member states are obliged to incorporate into their domestic legislation.[36] The Directive creates a range of principles and presumptions concerning evidence disclosure and attribution of civil liability for harms arising from the use of AI. The Directive applies to both breaches of the AI Act, and existing rules of civil liability. [37] The Directive adopts the AI Act's definitions.[38] The Directive sets out requirements for disclosure of evidence concerning HR AI if a plaintiff can present a plausible claim[39] of some harm suffered by an AI user. Failure to meet these disclosure obligations creates a rebuttable presumption that a defendant failed to meet its duty of care.[40]

The directive also creates a rebuttable presumption of causation where the defendant has been found or presumed to have not complied with its duty of care. In such cases, the causal link between the fault of the defendant in failing to meet its duty and the output of the AI system that caused the damage will be presumed.[41] Where the claim is regarding a breach of the AI Act and involves HR AI System, fault will be demonstrated where the defendant failed to fulfil the data quality criteria, transparency, oversight, and corrective action requirements, or it failed to ensure adequate accuracy, robustness and cybersecurity of the system.[42]

[34] Ibid at [152] (Moshinsky and Derrington JJ).

[35] Ibid at [75] (Kerr J, in dissent).

[36] European Union, *Treaty on the Functioning of the European Union*, 26 October 2012, OJ L. 326/47-326/390.

[37] Liability Directive (n 2) Preamble.

[38] Ibid, art 2(1).

[39] Ibid, art 3(1).

[40] Ibid, art 3(5).

[41] Ibid, art 4(1).

[42] Ibid, art 4(2).

The Department should consider an Australian law – quite likely by subordinate legislation to enable flexibility and speed in making regulatory changes – which enacts provisions similar to the EU's AI Liability Directive. Such a Directive should be clearly pointed to providing the judiciary with boundaries on determining causation and the existence / breach of duty in cases of negligence arising from the use of AI systems.

Coordination of AI Governance (Question 4)

Given the issues identified above, there should be a clear consideration of the Recommendations 17.1 and 17.2 from the Robodebt Royal Commission, which stated:

> **Recommendation 17.1: Reform of legislation and implementation of regulation**
>
> The Commonwealth should consider legislative reform to introduce a consistent legal framework in which automation in government services can operate.
>
> Where automated decision-making is implemented:
>
> - there should be a clear path for those affected by decisions to seek review
> - departmental websites should contain information advising that automated decision-making is used and explaining in plain language how the process works
> - business rules and algorithms should be made available, to enable independent expert scrutiny.
>
> **Recommendation 17.2: Establishment of a body to monitor and audit automated decision-making**
>
> The Commonwealth should consider establishing a body, or expanding an existing body, with the power to monitor and audit automate decision-making processes with regard to their technical aspects and their impact in respect of fairness, the avoiding of bias, and client usability.

The Government should consider creating a body (or more likely, expanding one) in the terms recommended in the Robodebt report to appropriately establish, coordinate and monitor the use of AI in circumstances where "decisions" are being made, either by Government or actors empowered by government (i.e., contractors or service providers).

Responses suitable for Australia (Question 5)

One option that should be strongly considered is a discretionary power vested in the Minister for Industry, Science and Resources (or similar portfolio) to issue a determination that a particular system or class of systems should be regarded as "AI" for the purposes of Australia's legislation. Rather than needing statutory change to alter the definition of AI, the Minister should have the power – after consulting with the public – to include a particular system or class of system within Australia's regulatory framework. A similar "licensing" system for AI has been proposed (but not yet adopted) in the United Kingdom.[43]

The proposed scheme could operate in the same manner as the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act). Under the SOCI Act, the Home Affairs Minister may[44] – after consulting with the asset[45] and in some cases the First Ministers of the States and Territories[46] (as well as any other

[43] Kiran Stacy, 'AI should be licensed like medicines or nuclear power, Labour suggests', *The Guardian* (online, 6 June 2023) <https://www.theguardian.com/technology/2023/jun/05/ai-could-outwit-humans-in-two-years-says-uk-government-adviser>.

[44] *Security of Critical Infrastructure Act 2018* (Cth), s 51(1).

[45] Ibid, ss 9(1)(f) and 9(3).

[46] Ibid, s 9(4).

persons the Minister considers necessary[47]) – the Minister may prescribe an asset to be a 'critical infrastructure asset' or 'system of national significance'.[48] Upon prescription, the asset then becomes subject to various security obligations in the SOCI Act.

In a similar fashion, the EU Act delegates authority to the European Commission to add to the uses listed in the annex where a new use is envisaged, falls within one of the above categories, and 'poses a risk of harm to the health and safety, or a risk of adverse impact on fundamental rights'[49] that is equivalent or greater than the risk posed by one of the uses already included in the annex. This is in addition to the prescribed eight categories of "high risk AI system" which are:

- Biometric identification and categorisation;
- Operation of critical infrastructure - i.e., safety components for road traffic management and the supply of water, gas, heating and electricity;
- Education and vocational training - including entry exams, student assessments;
- Employment - recruitment, promotions, performance evaluations, and task allocation;
- Essential private services and public services and benefits such as welfare, credit assessments and operations of emergency services;
- Law enforcement and immigration control including individual risk assessments, profiling individuals, crime analytics and predicting offending; and
- Judicial administration, including systems intended to assist a judicial authority in factual and legal research.[50]

Another measure would be the imposition of "red lines" – areas of AI development which are considered too high risk to be developed in Australia. Under the EU's AI Act for example, certain uses of AI are deemed to be 'unacceptable'[51] and are therefore prohibited. These uses are, broadly, systems that create material 'behavioural distortion,'[52] social credit systems[53] like those already deployed in parts of China,[54] and real-time remote biometric surveillance for law enforcement purposes,[55] the latter prohibition being subject to a number of qualifications and exceptions.[56]

Risk-Based approaches to AI Regulation (Questions 14 and 15)

The Discussion Paper refers to the *UTS Model Facial Recognition Law* as one example of a risk-based regulatory scheme which could apply to AI. The EU AI Act (in Attachment B of the Discussion Paper) is another. The inherent principles in Canada's Bill C-27 are yet another.

However, each of these applications presupposes several questions which cannot be answered in the abstract. If risk is 'the effect of uncertainty on the achievement of objectives',[57] then it must be asked who does the risk affect? Whose objectives take priority in the assessment of risk? Who determines

[47] Ibid, s 9(6).

[48] Ibid, ss 51A(1) and 52B(1) respectively.

[49] AI Act art 7.

[50] Noting the breadth of the definition of AI - this could extend to using web search.

[51] AI Act art 5(1).

[52] AI Act arts 5(1)(a) and (b).

[53] AI Act art 5(1)(c).

[54] For a discussion of these systems in the context of China see M. Zalnieriute, L. Bennett Moses and G. Williams, 'Automating Government Decision Making: Implications for the Rule of Law,' in S. de Souza, M. Spohr (eds), *Technology, Innovation and Access to Justice: Dialogues on the Future of Law*, Edinburgh University Press, UK, 2021, at 91.

[55] AI Act art 5(1)(d).

[56] AI Act Arts 5(2) and (3).

[57] International Standards Organization, *ISO 31000: Risk management* (2018).

the risk appetite, i.e., what is an "acceptable" level of risk? And who owns the residual risk related to a given AI capability or program? The Discussion Paper does not confront those questions. Although a risk-based approach to AI regulation may be appropriate, it cannot be considered without determining the answer to each question, which raises a number of global issues.

The first issue relates again to the notion of regulatory arbitrage. Under the EU AI Act, there are certain technologies and capabilities which are simply "banned", i.e., those which have a 'significant potential to manipulate persons through subliminal techniques, exploit the vulnerabilities of specific vulnerable groups and AI-based social scoring done by public and private authorities'.[58] Yet who is responsible for determining compliance with this requirement? If the onus falls on the companies developing these technologies, they may be able to rely on semantics to defend their position, i.e.:

- The technology does not have a **significant** potential to manipulate persons (but the potential is still sufficient to generate concern);
- The technology does not exploit the vulnerability of a **specific** group (but perhaps multiples groups or the entirety of the public at large);
- The technology does not produce a **social score** (but does permit other forms of classification or ranking).

Secondly, the balance between individual rights and the "public interest" does not always resolve favourably in Australia (as we lack a constitutive Charter or Act on human rights). In recent cases of technology overreach by government – the use of Auror and ClearView AI by the Australian Federal Police, or the cases of the Robodebt or Dutch tax scandals – these actions have been justified by appeals to public interests such as detection of crime and prevention of fraud. Yet very clearly, there have been breaches of human dignity and privacy, and which often are the first victims in cases of State surveillance.[59]

Thirdly, companies operating in risk-based environments often have a vested interest in the rapid deployment of technologies (which will include AI technologies), even where they carry a potential compliance liability. The launch of Uber as a ride-sharing service in Australia in 2012 was known to be an illegal operation, running without permits required by State and Territory governments.[60] Uber also operated an algorithm known as "Greyball", helping them spot traffic inspectors trying to "sting" unlicensed drivers.[61] Companies are already racing ahead to develop and launch generative AI content without properly assessing the risks of those same technologies. [62]

Fourthly, in many instances of current technologies, government already carries a significant compliance burden which AI should not be seen as adding to. For example, under the Privacy Act there is no independent remedy for affected individuals for breach of privacy (such as a tort or private cause of action). This leaves the government, and in particular the Office of the Australian Information Commissioner, as the sole investigative and compliance body for ensuring companies do the right

[58] Attachment B to the Discussion Paper.

[59] Also see for example Brendan Walker-Munro, 'Hyper-Collection: A Possible New Paradigm in Modern Surveillance' (2023) 21(2) *Surveillance & Society* 120-138.

[60] Ben Butler, 'The Uber files: firm knew it launched illegally in Australia, then leaned on governments to change the law', *The Guardian* (online, 15 July 2022) https://www.theguardian.com/news/2022/jul/15/the-uber-files-australia-launched-operated-illegally-document-leak.

[61] Julia Carrie Wong, 'Greyball: how Uber used secret software to dodge the law", *The Guardian* (online, 4 March 2017) https://www.theguardian.com/technology/2017/mar/03/uber-secret-program-greyball-resignation-ed-baker.

[62] Natasha Lomas, 'Don't rush generative AI apps to market without tackling privacy risks, warns UK watchdog', *TechCrunch* (15 June 2023) https://techcrunch.com/2023/06/15/uk-ico-generative-ai-warning/.

thing. Nor should the responsibilities be solely left to the individual, acting as either citizen or customer, to have to determine whether their interactions with AI fall at the high-risk or low-risk end of the spectrum.

Conclusion

The policy and legislation settings of Australia will require significant consultation and discussion to properly enact a framework which respects both the technological but people-centred use of AI in the future. This submission has made only brief proposals in relation to specific areas of interest. Therefore, we would be happy to provide further details, or attend further consultation, as determined by the Department on any other issues that may arise during this process.

Thank you for the opportunity to make this submission.

Prof Rain Liivoja, Deputy Dean (Research) and Research Lead, Law and the Future of War Research Group, The University of Queensland

Email r.liivoja@uq.edu.au

Dr Brendan Walker-Munro, Senior Research Fellow, The University of Queensland

Email b.walkermunro@uq.edu.au

Dr Lauren Sanders, Senior Research Fellow, The University of Queensland

Email l.sanders@uq.edu.au

Dr Sam Hartridge, Senior Research Fellow, The University of Queensland

Email s.hartridge@uq.edu.au