Law and the Future of War Research Group
TC Beirne School of Law

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

Submission to the Inquiry into the Department of Defence Annual Report 2022–2023

Dr Lauren Sanders
Dr Sam Hartridge
Prof Rain Liivoja
Ms Natalie Nunn
Dr Brendan Walker-Munro
Mr Renato Wolf

The views contained in this submission reflect those of the authors and do not represent the official position of the University of Queensland or any other institution.

1. Overarching observations

1.1 Significant changes to Australia's defence legislative landscape

Any review of the functioning and efficacy of the Department must take into account major anticipated changes to the legislative landscape within which the Department operates. The ongoing reviews relate to central areas of Defence's operation. In addition to the Defence Act review project, impacts of the ongoing implementation of the Richardson Review and Privacy Act reform will have both anticipated and unanticipated impacts upon the Department, including in the implementation of novel technologies such as AI. These reforms have been running for several years and have, and will continue to, generate relative uncertainty in relation to their impacts upon Defence's future operational plans. Any consideration of Defence's future operational posture and capability implementation processes must also be closely aligned with assessing the legal and legal policy considerations associated with these reforms.

1.2 Accounting for legal and policy constraints during acquisition processes

Legal and policy evaluation and development should generally occur concurrent to investment in physical capability. In this vein, there should be further allocation of resources to understand and address the legal, ethical and social implications (ELSI)[1] of the novel technologies that form part of Defence's future strategic plans and attract significant investment by the Commonwealth Government. Without at least some investment in the development of policy associated novel technology, it is likely that ELSI will not be adequately addressed.

Further, any such investment to address ELSI is relatively small compared to the capability-focused investment currently underway. Allocating further resources to understanding and addressing ELSI at an early stage may be a worthwhile investment: addressing the issues identified through minor adjustments during design, development and early acquisition stages, when technical readiness levels (TRL) are lower, costs much less than undertaking corrective work at higher TRL once certain capability settings have been entrenched. As a practical example of such a value proposition, consider the EUR 430 million investment in the German Eurohawk autonomous drone. The project was

[1] Also frequently referred to as 'ethical, legal and social aspects' (ELSA) of novel technological development.

ultimately abandoned because it became prohibitively costly to adapt the drones to the airspace standards set by European Aviation Safety Agency

In addition to the obvious cost saving of the integration of ELSI across the capability acquisition life cycle, such integration provides broader organisational efficiencies in terms of policy realignment, training and inculturation requirements for novel technology, and more relevantly, creates a more robust compliance framework associated with that technology.

ELSI do not appear to feature in any of the Australian Strategic Capabilities Accelerator (ASCA) projects so far. The ELSI frameworks of the US and EU member states (the Netherlands in particular) offer good models to adopt to incorporate these considerations as explicit requirements for capability missions advertised by ASCA. While we are not party to the internal workings of ASCA, there has been no public-facing indication that ASCA processes have accounted for this need.

With this in mind, there is a need to build a framework to purposefully focus acquisition personnel on ELSI. Australia has an opportunity to lead in this field, noting its strong contributions to international debates, such as its participation in the Responsible AI in the Military Domain (REAIM) Summit in 2023, along with its commitment to the Summit's call to action.[2] The responsible adoption of military AI necessarily entails commitment to legal and ethical frameworks.

The integration of ELSI across the capability lifecycle aligns to Australia's contributions to the Group of Government Experts on Lethal Autonomous Weapon Systems ('GGE') on the 'system of controls' approach.[3] One of the six priority areas for Defence articles in the Defence Strategic Review was to focus upon 'lifting [Defence] capacity to rapidly translate disruptive new technologies into defence capability, in close partnership with Australian industry'.

Without concurrent policy and law considerations incorporated during the acquisition phases of novel technology, there is no efficacy in truncating acquisition timelines or focusing capability on adopting Minimum Viable Products (MVP), as foreshadowed in the Defence Strategic Review. Put simply, getting a piece of physical equipment in Defence faster, will not speed up getting it into operator's hands, unless the ELSI of that equipment have been considered throughout its acquisition.

1.3 Opportunity for regional leadership through international legal compliance and development

Australia has an opportunity to lead both regionally and internationally on these issues, given the substantial progress that has been made by academia, industry and government in progressing conceptions of responsible military use of AI. This is reflected in the aforementioned 'systems of control' contribution to the GGE, as well as the recent ADF-led Expert Meeting on Enhancing the Legal Review of Autonomous Weapon Systems.[4]

In addition, there are obvious training and knowledge transfer activities that could occur in an international engagement setting, which would be relatively low cost, but high yield, activities. There is an opportunity for the Australian government to continue to work closely with other technologically advanced states in the region, such as Singapore and the Republic of Korea, on progressing and

[2] REAIM 2023 Call to Action (16 February 2023) https://www.government.nl/binaries/government/documenten/publications/2023/02/16/reaim-2023-call-to-action/REAIM+2023+Call+to+Action.pdf.

[3] Australia, 'Australia's System of Control and applications for Autonomous Weapon Systems' (26 March 2019) UN Doc CCW/GGE.1/2019/WP.2/Rev.1.

[4] Netta Goussac, Natalia Jevglevskaja, Rain Liivoja and Lauren Sanders, *Enhancing the Legal Review of Autonomous Weapon Systems: Report of an Expert Meeting* (Brisbane: Law and the Future of War Research Group, TC Beirne School of Law, The University of Queensland, 2023) doi: 10.14264/2bbfd31.

aligning adoption of ELSI relevant to emerging and disruptive military technologies, and in particular, as it related to military AI policy.

More generally, there is an opportunity to expand the activities of Defence-related institutions that can influence regional actors with respect to international law and international humanitarian law compliance. Specifically, there is an opportunity to enhance the capacity and reach of the Indo-Pacific Centre for Military Law (IPCML) in undertaking instruction and training in international law. This model has been extremely successful in furthering States' positions and to influence the development of international law. Institutions such as the Lieber Institute for Law and Warfare at the US Military Academy, the Stockton Center for International Law at the US Naval War College, and the Centre for International and Operational Law at the Swedish Defence University, are examples of highly influential actors in terms of developing the understanding of international law in light of changes in military technology. From our experience working with the IPCML, there are real prospects in making the Centre more prominent regionally, but that will also require the IPCML to build stronger links with the many Australian and regional academic institutions that have strong research reputations in the laws of armed conflict.

2. Assistance to Ukraine

2.1 General observations

This Inquiry offers an opportunity to revisit Defence's gifting policy *writ large* in terms of passage and acceptance of risk. This is specifically the case in relation to the transfer of defunct ADF equipment to military forces, such as Ukraine. From an international law perspective, having regard to the principles of state responsibility, there are negligible legal concerns in relation to transferring such materials if the transfer occurs with adequate disclosure and knowledge of risk. In our view, the risk in such circumstances is borne by the receiving nation state, noting also that a nation state's level of risk acceptance is likely to reflect the extent of the existential threat that they are facing at the time of transfer. We are not advocating for such transfers to occur without the usual checks and balances pertaining to potential of misuse of transferred goods (as required under the Arms Trade Treaty and numerous other international instruments), nor for the materials to be transferred without having undertaken adequate testing and evaluation processes in Australia such that the use of the equipment *per se* would not be in breach of Australia's existing international law obligations. Rather, we suggest that the threshold for peacetime operations and training of equipment by the ADF is not necessarily the same risk criteria for a receiving state, in a situation of active armed conflict, to apply when considering such transfers.

2.2 Transparency of assistance

While not necessarily relevant in terms of the Ukrainian example, we consider that the transparency of assistance provided by the Australian Government to foreign states in general, should be considered by this Inquiry. We consider this is important in terms of understanding and facilitating proper assessments of the lawfulness of such assistance, transfers or ongoing use of foreign assistance and military sales. Specifically, without providing an opportunity for communities with relevant information about the human rights records of the receiving states to participate in the process, through enabling mechanisms for public input to facilitate decision-making, the assessment on the risk of transferred equipment being used to breach Australia's international legal obligations will be incomplete. This also aligns to the general principles of responsible and transparent government, noting the Commonwealth Government's commitment to pro-disclosure approach to decision-making.

There does not appear to be a consistent approach to the disclosure of information about support to different states. The support provided to Ukraine is well reported, and readily discoverable by the public, however, details of export control permits provided to states such as Israel and Saudi Arabia

appear to be more difficult to determine.[5] The disparity in relation to information provided about assistance to different states highlight different parts of the same problem: Australia has international legal obligations to ensure respect for the laws of armed conflict, and to ensure–in certain circumstances–that its actions do not contribute in a material way to the breach of other states' international legal obligations (particularly as they relate to potential breaches of *erga omnes* obligations). In light of these legal obligations, there is a requirement for robust assurance mechanisms pertaining to gifted or exported materials.

We note that there are higher degrees of end-use monitoring obligations in place by key allies, such as the United States, and consider that such end-use monitoring obligations could be mirrored in the Australian system.

We also note that existing diplomatic assurances on uses may not be sufficiently robust to meet ongoing use monitoring expectations arguably established by international law. This obligation is one that should read broadly, and treaty obligations such as that imposed under Article 6(2) of the Arms Trade Treaty, extend to positive actions (such as cancelation of export licences and cessation of arms transfers), to prevent potential breaches of international legal obligations where Australia has sufficient information to support such an assessment.

In undertaking this obligation in a holistic and bona fide manner, Australia should create a process by which information about which states it is considering transferring military equipment and arms to, is firstly made public, and secondly, accompanied by a process that allows the receipt of relevant information from the broader Australian community to inform its assessment of the likelihood of breach likely to flow from that transfer or export. We point the Inquiry to the findings of the UK High Court, in the matter brought by the Campaign Against Arms Trade (the judgement for which was released on 6 June 2023)[6] as an example of the interaction between domestic administrative decision making processes and international legal obligations pertaining to export and transfer of military equipment.

We acknowledge that there is a distinction between the process that must be in place to respond to allegations of systematic misuses and breaches of the law, as compared to instances of individual misuse. However, in both circumstances, assessments about whether a systemic breach has occurred and this threshold of misuse has been met, can only be achieve through robust and ongoing monitoring obligations, which necessarily require adequate resourcing.

2.3 Liability for the conduct of training and provision of material assistance

The current ADF practice in providing training in the use of gifted military equipment is representative of best practice and should continue. This is both in terms of export control and in discharging Australia's international legal obligations to ensure respect for the laws of armed conflict. In addition to making obvious sense in terms of maximising the utility of the gifted equipment, it mitigates risk in relation to potential misuse of capabilities and any subsidiary responsibility for Australia resultant from that misuse. We do not suggest that gifting to Ukraine gives rise to such a risk, but this model is one that should be continued for future gifting activities.

2.4 Support to war crimes investigation

We briefly note that Australia's own experience in Afghanistan, combined with the serious allegations of war crimes in Ukraine (and Gaza), suggest that there is a need to think proactively about a robust mechanism for investigating and prosecuting war crimes. There is more that Australia can do in this

[5] See, for example, the Federal Court application for pre-trial disclosure made by the Australian Centre for International Justice regarding export control permits issued to the State of Israel on or after 7 October 2023 and associated media coverage of this issue)

[6] *The King (on the application of Campaign against Arms Trade) v Secretary of State for International Trade* [2023] EWHC 1343 (Admin).

regard, in terms of upskilling Australian practitioners through secondments (as the NZDF has done in sending a senior NZDF Officer and an NZDF legal officer to the ICC to support their ongoing investigation into situation in Ukraine).[7]

This experience also raises questions about the current capacity of the ADF, AFP, CDPP (and the Australian government's interagency atrocity accountability actors more generally), to undertake similar investigations should Australia be required to do so. There are further lessons that should be assessed and learned in relation to processes, information management and use of information systems, including the use of social media platforms for the collection of evidence, which should be rehearsed and resourced within Australia.

2.5 Lessons to be learned in use of Commercial-Off-The-Shelf equipment (COTS)

The prevalence of the use of commercial-off-the-shelf (COTS) equipment in the Ukrainian conflict highlights the need to ensure that capability acquisition processes also consider how to regulate acquisition of COTS. While we are not able to speak about the rapidity of acquisition under current mechanisms, we note that such acquisition systems must also include a process for streamlining the accompanying legal obligations associated with acquisition. This includes a method to streamline assessment of Australia's international legal obligations, as well as general due diligence contracting and liability assessments. We consider this reliance on COTS equipment reinforces the need for better conceptualisation of spiral acquisition policies, that specifically incorporate legal considerations throughout the process.

3. Capability Assurance Mechanism

3.1 General observations

Assessment of domestic regulatory risk and international legal compliance should be integrated more broadly into processes intended to 'identify and manage the complexities associated with material procurement and sustainment including the acceptance of new capability into service'.

The selection of case studies, for the use of informing accountability and risk identification, should not be conducted as a singular activity, and we caution against adopting case studies that do not adequately incorporate different legal and policy risk profiles. Specifically, identifying different edge case testing scenarios must also contemplate the likely legal framework in which novel capabilities might be applied. For example, the use of a capability in a "grey zone" operation as compared to use during armed conflict have profoundly different risk outcomes from a legal perspective.

In our experience, there is no mandated assessment of legal risk in the current testing and evaluation process and consider that better integration of legal assessment processes such as the already mandatory legal review of new weapons, means and methods of warfare, should be adopted across the testing and evaluation landscape.

3.2 Assurance against foreign interference

As part of the Inquiry's evaluation of test and evaluation processes 'inform[ing] accountability and risk identification', consideration should be given to bolstering Defence's risk assessment capabilities to ensure that it adequately identifies, ranks and mitigates the hazards posed by foreign interference in Defence capability acquisition programs.

---

[7] New Zealand—Foreign Affairs and Trade, 'Russian invasion of Ukraine' (webpage) https://www.mfat.govt.nz/en/countries-and-regions/europe/ukraine/russian-invasion-of-ukraine/.

Current laws impose criminal penalties for persons engaging in 'foreign interference', which includes conduct to 'support intelligence activities of a foreign principal' and/or to 'prejudice Australia's national security' (*Criminal Code,* ss 92.2 and 92.3). It is entirely possible that a sophisticated threat actor, State-sponsored or otherwise, could exert interference with Australia's military capabilities by infiltrating, undermining, or sabotaging the procurement processes used to acquire them.

National security risks in procurement decisions are not unknown to the Australian security landscape. In February 2023, Shadow Home Affairs Minister James Paterson raised the issue that Chinese-made Hikvision and Dahua monitoring cameras - the same cameras being used to unlawfully segregate and isolate China's Uyghur minority in Xinjiang - were installed in numerous Australian government offices. The debate triggered a government-wide audit of the devices.

Similarly, in May 2023 the US Department of Defense suspended use of drones manufactured by Chinese-owned company DJI until a comprehensive security audit could be undertaken. Despite those concerns, the drones continue to be used across multiple other government agencies in other jurisdictions. Relevantly, DJI drones had already been the subject of a security audit in 2017 and bans by the US Pentagon in 2021 but were continuing to be used by Australia's Department of Defence.

Australia's allies have already taken steps to protect against foreign interference in their military supply chains, as shown in the following examples:

- The United States routinely publishes updated guidelines on how to counter foreign interference risks during defence procurement, most recently on 29 June 2023;
- The United Kingdom's House of Commons published a report on 14 February 2021 titled *Foreign Involvement in the Defence Supply Chain*. In that report, the House identified foreign involvement was 'widespread', leading the House to conclude the 'Ministry of Defence's open and country-agnostic approach has meant that the defence supply chain has been open to potentially hostile foreign involvement, with reports of companies being owned and influenced by foreign Governments whose values and behaviours are at odds with our own and who are known to engage in intellectual property theft';
- In the European Union, Member states have expressed concerns regarding the 'EU's dependence on foreign actors and foreign technologies in critical infrastructures and supply chains', such that they have issued calls 'to exclude the use of equipment and software from manufacturers from high-risk countries'.

The Inquiry should consider whether Defence's capability procurement mechanisms are adequately screening for possible foreign interference risk. The Inquiry should particularly consider how and to what level that risk screening occurs throughout the lifecycle of the procurement - i.e., from concept to prototype, and proof of concept to delivery - so that emerging risks are identified and dealt with in a timely fashion.

The Inquiry should also consider capability assurance mechanisms that extend due diligence obligations in relation to providers; however, note that these assurance measures go hand-in-hand with a need to maintain working relationship with industry and experts.

In our experience, the legal and policy requirements for Defence contracting and assurance are limited by other practical issues, such as:

- Policies on preferences for internal expert support for niche projects that necessarily require deep expertise in particular subject areas (and the predominant hiring of contractors from the 'primes' rather than small and medium enterprise);
- Delays of administrative support in undertaking such activities, through slow processing times for security clearances; and
- The unsuitability of the DISP process for large non-manufacturing organisations which partner with Defence, such as the university sector.

4. Artificial Intelligence and Autonomous Weapons related issues

4.1 General observations

The manner in which AI has been managed in Defence, from a policy perspective, has been confused and convoluted. In particular, we note the need for greater transparency in relation to Defence's AI policy, clarity on which section of Defence has ownership for that policy, and that in light of the CSIRO's excision of Defence from its Responsible AI public consultation process, that there should be an equivalent process undertaken in anticipation of broader adoption of military AI. The ADF's social licence to operate remains critically tied to its ability to successfully integrate community expectations into operating procedures, which also has obvious flow on effects for matters such as recruitment and defence industry support.

We reiterate that the use of cases studies in the understanding of risk for complex military technologies, and AI in particular, is unhelpful if it focuses on single use cases. This is particularly the case for AI because of the breadth of use cases for AI componentry in multiple capabilities; as well as the vastly different outcomes for use of AI in Defence capabilities (such as for example, the use of AI to augment human resource processes as compared to the manner in which AI software might control loitering ammunition in a LAWS).

This breadth of use has significant implications on the legal, ethical and moral frameworks relevant to AI's use. We consider that if the same capability use case is used, it is helpful, even, to understand how that same capability might be deployed across multiple mission sets – such as Non-International Armed Conflict, International Armed Conflict and Peacekeeping Operations.

We note that has been investment in the consideration of these legal and ethical factors in the past (such as through the now discontinued Trusted Autonomous Defence Cooperative Research Centre, which funded the Law and Future of War project), and that new initiatives, such as the DAIRNet, do not have allocated resources to specifically address the legal and ethical concerns connected to responsible AI use in the military.

Finally, borrowing the observations of a colleague who has worked in this field for over a decade (namely, Ms Netta Gousaac) it is key to understand that 'responsible use of military AI is more than the minimum'. It represents more than minimum legal compliance, and what is known about the use of LAWS in particular, is that the Australian public will expect that the ADF does more than the minimum when it comes to deploying such systems.

4.2 Australia's contribution to the GGE on LAWS

Our experiences as observers and participants in the GGE has been that Australia has had a very significant influence on GGE process when it comes to highlighting the importance of legal reviews of weapon systems in assuring compliance.

However, when it comes to regulation of autonomy and LAWS more generally, we consider that Defence can take a more proactive stance in conjunction with Australia's allies.

4.3 The Systems of Control approach and its influence on the debate

Australia's aforementioned paper on the 'system of control' represents a significant contribution to the debate on human control of LAWS and offers a viable course for the appropriate legal control of autonomous systems to be deployed.

In spite of its great utility, there is an opportunity to further investigate how to operationalise this concept, particularly considering this concept is in danger of being adopted as a panacea to broader sociolegal considerations regarding human control issues if it is not properly fleshed out. It could also risk become a shorthand for inaction and inertia in Australia's policy settings for the use of LAWS. As

it is now five years old, it could be reviewed and updated to reflect contemporaneous debate on this issue, with addition of much needed granularity in how it might be adopted in practical terms.

4.4 Australia's role for leadership in influencing the drafting of an instrument regulating LAWS

We reiterate our views, above, that Australia has played a leading role in the current debate at the CCW GGE; as well as in other for a such as the Responsible AI in the Military Summit (REAIM Summit). However, adopting the example of the Republic of Korea in its regional leadership in hosting the second REAIM Summit (to be held in Seoul this year), Australia could follow suit and be a more active participant, and host, of debate on the issue of military AI regulation.

Australia has previously had a resistance to the legally binding regulation of AWS. This viewpoint needs to be nuanced beyond a generic resistance to regulation to a conversation about what future regulation of AWS might look like. This can be readily achieved in a way that does not limit Australia's future operating options, or freedom of action, as this regulation should mirror other non-proliferation initiatives that Australia is party to, insofar as they reiterate and further entrench the banning and non-proliferation of capabilities that are incompatible with existing legal obligations.

Aligned to our adoption of the maxim, 'responsible use of military AI is more than the minimum', we consider that while existing laws of armed conflict are capable of regulating AWS, this is not an argument in and of itself to avoid future regulation.

4.5 Weapons review of AI-enabled capabilities

The conduct of legal reviews of AI-enabled capabilities, pursuant to Article 36 of Additional Protocol I, is one significant part of the broader assurance structure to enable lawful adoption of (L)AWS.

Australia's engagement with this issue offers opportunities for regional leadership and broadening compliance with an existing legal obligation that is historically not well adhered to by other states. This opportunity can extend beyond the LAWS debate to general adoption of emerging and disruptive technology, in terms of broadening general legal compliance and Australia's interoperability with its key allies, all of whom adopt similar review processes.

We note that this opportunity for leadership can be global, rather than merely regional, on the basis that Australia's approach to legal reviews as compared to other countries is exceptionally robust. We consider the Australian model could be one readily adopted by other states, and in addition to further international engagement through training and process adoption, offers enhanced opportunities for technology sharing with non-traditional regional and global allies.

4.6 Cybersecurity of AI-enabled capabilities

One area of debate which remains entirely unexplored, both in Australia and internationally, is the concept of ensuring cybersecurity on weapon systems and military hardware equipped with AI. In addition to the lack of identifiable guidelines on the deployment of military AI systems as a whole, there are no current (public) developments of minimum standards for cybersecurity which ought to protect AI-enabled capabilities from adversarial actions, such as instigation of crashes or other deliberate malfunctions, hacking, spoofing or remote takeover.

There are public reports that such attacks are already occurring – in 2011 it was alleged that Iran "hacked" the navigational systems of a US RQ-170 Sentinel drone, subsequently (crash) landing that drone inside Iranian borders where it could be captured. In 2015, members of the "Critical Engineering Working Group" launched a stratospheric balloon capable of intercepting communications between US and Coalition drones. Then in 2019, BBC News reported that US forces had launched a cyber-attack against computer systems controlling Iranian air defence systems, allegedly in retaliation for drone attacks against oil tankers in the region.

The Inquiry should consider what standards Australia's Department of Defence should adhere to in seeking to prototype (and eventually deploy) AI-enabled capabilities. This should involve a holistic assessment not only of the requirements for security around current and future AI-enabled capabilities, but also the skills and expertise of Defence personnel needed to maintain that robust security against electronic warfare countermeasures.

5. Armaments manufacture, procurement, and inventory.

5.1 Australia's export control regime

We note that there is no simple way to export, and that current education and outreach has supported broadening understanding of Australia's requirements. However, the interplay between Australia's export control systems and that of other, complex regimes, such as the US ITAR requirements, mean that the export control system creates significant administrative overheads for doing business with Defence in Australia. Further resourcing outreach, education and support to streamline these processes is likely to result in better compliance, but also in greater initiative to engage in Defence innovation and research.

Noting current Bills pertaining to exemptions under the *Defence Trade Controls Act*, we think that there is also a broader debate to be had in respect of the model of controls adopted by Australia. Adopting piecemeal adjustments reflective of the US approach to export controls is inadequate. The concurrent proposals to change the *Defence Trade Controls Act*, while undertaking the second legislatively mandated review of the regime, with no public indication of implementation of the previous report's findings that the system is not fit for purpose, is likely to reduce confidence in the strength of Australia's export system.

5.2 Transparency of Australian exports

As noted above, we consider that further transparency in relation to the countries to which approved export controls have been issued would enhance Australia's reputation for human rights compliance.

This could be readily achieved by allowing external submission on potential human rights abuses to aid decision makers to properly comply with international legal obligations. This is also likely to protect those decision makers from future criminal complaints regarding complicity, should information have been available to Government, but not brought before the relevant decision makers.

We also consider that a mechanism could be inserted into decision making where significant impacts on Australia's foreign relations are taken in consultation with the Minister for Foreign Affairs. We note that there are similar provisions in the *Intelligence Services Act* that could be modelled in this regard.

We also note that the bifurcation of sanctions decision versus export control decision making across multiple agencies has the potential to negatively impact the quality of both regimes. Specifically, the use of export controls as a tool of foreign policy and in relation to international legal compliance obligations could be more readily squared if this process was reviewed and realigned. We note that it is not readily apparent how this cooperation occurs and to what extend between DFAT and Defence, however given this decision making implicates international legal obligations this should be either publicly available information or set in the legislation.