*The character of war is changing fast and the ethics needs to keep pace with that change. These particular principles might well need revision. But we should not imagine the fundamental ethical issues have changed. It is still the case that in a sense war is inherently unethical. To be justified, significant ethical reasons are required and although imperfect Just War theory continues to be one way to seek such reasons. Heather Widdows, Professor of Glbal Ethics, Birminham UK.*

**The ethical design of AWS systems translated into practise.**

# Abstract

The discussion on the ethics of AWS use and the call for their ban in academic circles isn’t translating real-world AWS regulation. Firstly, AWS regulation inherently is impractical since its definition is too broad given the dual-purpose nature of AI and autonomous technologies in civilian systems, the affordability of hardware, and the lower barriers of expertise to integrate them. Secondly, circumstance is stymying AWS bans. The sunset of America’s global force projection and the rise of Great Power Competition are compelling Nation states and their defence companies to develop and field AWS systems at an accelerating rate. Thus, AWS development and operation is a fait accompli. But more concerning than AWS development and operations by nation states is the inevitable diffusion of this technology to unaligned actors, authoritarian states, private militaries, domestic police, terrorist groups and the like which will occur in the long term firstly by technology exports, natural decreases in cost or forcefully stolen via IP theft, actual capture and reverse engineered and redeployed beyond their intended usage (issue 9 and 10 of IEEE reframing AWS)[[1]](#footnote-1)

If AWS is a fait accompli then naturally the conversation must shift to the ethical design and operation of AWS. But surprisingly little has been said on the topic of ethical design and how to verify that ethical design is practised whereas much has been said on hypothetical operations of AWS in military and philosophy journals. All the while defence companies are busily prototyping and maturing the first wave of next generation AWS systems, in an R&D context that prioritises demonstration of functionality. The publically stated ethical policies by defence contractors are thin, the verification of ethical design is unclear at best, opaque at minimum, and not considered altogether at worst. More can be offered in the public domain to assure ethical engineering design practises in defence companies.

**What we need is urgent translation of ethical literature from into practice by companies. Don’t need more ethical and moral musings about AWS warfare. It is going to happen.** This paper calls for that defence companies imbue ethical gates into their engineering processes by proposing. Software and machine learning technologies changes so quickly that not even software engineers and university course work can keep up. Can’t wait on regulation those working in this area need to push their organisations to develop their own methodologies.

1. Start deriving ethical motherhood policies into actual, practical engineering processes. Incomplete is better than current state which is none.
2. Inject these processes at the beginning of the engineering lifecycle.
3. Introduce AWS workshops with senior leaderships. Many AWS engineers aren’t must be cognisant of the ramifications of their work.
4. Appoint AI ethicist or AI Safety Engineering role asap. *Tech companies have this but not defence companies.*
5. Publish their ethical verification strategies.

# Background - definitions

* Autonomous weapon systems are weapon systems that can perform their critical functions of selecting and engaging targets with some significant degree of [autonomy](https://law.uq.edu.au/research/future-war/autonomy).
* Attack is the focus of AWS – indeed the keyword is there. However, the function of defence is much larger than that: broadly consider two functions: warfighting/combat (which includes force application, force protection, situation understanding, force sustainment) and enterprise-level rear echelon functions (business process improvement, enterprise logistics, other, personnel). [DSTG]
* AI and autonomous weapons system (AWS) do not necessarily coincide.
* The prospects of reaching a meaningful international consensus at the UN-hosted meetings on AWS seem increasingly bleak. After nearly seven years of meetings, States have failed to even agree on a definition of the weapons to be regulated, much less the substance of any such regulations, or even a consensus on whether any additional regulation is needed

# literature review – law, ethics, psychology journals

Public discussion centred in legal, moral, ethical discussion about owning, operating and assigning accountability for their misuse in the case of nation states. However, ‘the literature fails to consider that practices related to the development, testing and training, or usage of AWS outpace public, governmental, and legal considerations. AWS may shape norms in practice by privileging procedural norms that are detached from deliberative processes’.

So so much on meaningful human control, legality

There has been media attention and civil society organisations or campaigns such as Article 36, the Campaign to Stop Killer Robots, or the International Committee for Robot Arms Control (ICRAC) seek to raise the issue’s profile.

Ondrej et al. (2022) surveyed 1006 US citizens on the question of ethicality of mliitry strikes resulting in collateral damage whose intiail findings suggest that ‘increasing weapon autonomy is assocated with … lower perception of ethicality’ than ‘conventional inhavited and remote-controlled systems’. But acknowledge limitation is that the public equate unethical with novelty of the technology and having limited experience with autonomous machines.

# Fait accompli

But AWS deployment is practical fait accompli in the near future. ‘dual-purpose technology’ supported by states UK, China, Korea, Russia, Australia [Cite robotics roadmap]. Failure of AWS ban because *autonomy* itself is ill-defined and too broad in scope [Scharre]. Furthermore, the development of AWS is *‘accelerating largely outside of public and academic attention in the discipline of International Relations’* (Bode). The widely unaccounted development of AWS has impeded deep public discourse on this issue.

# Literature review – Aus Government

DSTG A Method of Ethical AI in Defence (Feb 2021) developed an AI checklist for the development of defence AI systems, and an ethical AI risk matrix. The report summarised the outcomes form a 2 day workshop in 2019 with 104 people from 45 organisations. They also proposed ‘ For large programs a data item descriptor (DIR) for contractors to develop a formal Legal, Ethical and Assurance Program Plan (LEAPP) to be included in project documentation for AI programs where an ethical risk assessment is above a certain threshold’. However risk matrix two unuseable: literal laundry list. No method to solicit ethical issues, no analysis method. Traditional safety engineering has at minimum these two techniques.

Devitt *A second study of over 2500 respondents found that Australians have low trust in AI systems but generally ‘accept’ or ‘tolerate’ AI (Lockey, Gillespie, and Curtis 2020). They found that Australians trust research institutions and Defence organisations the most to use AI and trusted commercial organisations the least.*

Standards Australia’s Artificial Intelligence Standards Roadmap: Making Australia’s Voice Heard (2020). Standards Australia seeks to increase cooperation with the United States National Institute for Standards & Technology (NIST) and other Standards Development Organisations (SDOs). Australia has a stated aim to participate in ISO/IEC/JTC 1/SC 42, and the National Mirror Committee (IT-043) regarding AI

While Australia has not released an overarching AI governance framework for Defence, Australia is a founding partner in the US’s AI Partnership for Defense (PfD) that includes Canada, Denmark, Estonia, France, Finland, Germany, Israel, Japan, the Republic of Korea, Norway, the Netherlands, Singapore, Sweden, the United Kingdom, and the United States (JAIC Public Affairs 2021, 2020). In doing so, Australia has aligned its AI partnerships with AUKUS, five-eyes (minus New Zealand), the Quad (minus India) and ASEAN via Singapore 6 .In particular Australia is seeking to increase AI collaboration with the US and UK through AUKUS (Nicholson 2021).

Australia has stated that it considers a sweeping prohibition of AWS to be premature (Australian Permanent Mission and Consulate-General Geneva 2017; Commonwealth of Australia 2018; Senate Foreign Affairs Defence and Trade Legislation Committee 2019, 65) [Devitt 2012]

However, the 2015 Senate Committee Report on unmanned platforms said ‘the committee is not convinced that the use of AWS should be solely governed by the law of armed conflict, international humanitarian law and existing arms control agreements. A distinct arms control regime for AWS may be required in the future” (see para 8.30). The report recommended that: “8.33 … the Australian Government support international efforts to establish a regulatory regime for autonomous weapons systems, including those associated with unmanned platforms.”

# Literature review – Industry

Leader is IEEE Ethics in Action committee. Recently announced 7000-2021 standsr to address ethical concerns during systems design, which is ‘value-based engineering to mitigate risk and increase innovation’.

Initial draft outlined 10 challenges. 1. Establishing a common language. This is absolutely essential. Struggling in industry to effectively communicate ideas amongst technical people let alone with business functions and then acorss industry and countries. There is no precision in definitions about ‘autonomosu weapons’ and ‘human control’ recommendation ‘ should be grounded in technical realities of today but not limitated by disagreements over what technologies may or may not be successfully developed farther into the future’ (IEEE 2020 paper)

IEEE reframing AWS issue 3: conforming to individual and professional organisation code of ethics and conduct but acknowledge ‘existing codes of ethics may fail to properly address ethical responsibility for autonomous systems, or clarify ethical obligation of engineers with respect to AWS’. Professional organisation should undertake reviews and possible revisions or extensions to their codes of ethics with respect to AWS.

Issue 11: Learning systems compound the problem of predictable use. Adaptive systems modify functional operations which cannot be anticipated by designers or operators. Even ‘when a single system is predictable, or even deterministic, which such systems interact with other systems or …in large swarms… their collective behaviours can become intrinsically unpredictable’.

# literature review – engineering

Lots said on meaningful human control. Nothing about practice. Some are click-bait titiles without practical propsals that recycle the literature reviews on AWS regulation such as Seumas Miller’s Autonomous Weapons: Terminator-Esque Software Design.

In a first attempt to derive design requirements for a moral machine for autonomous weapons, Verdiesen et. al. (2018) conducted a large-scale study of the moral judgement of people regard are AWS deployment and concluded more work required, no requirements actually presented. Umbrello (2019) proposes a design framework for ethical development via the Value Sensitive Design (VSD) approach that ‘intends to embed stakeholder values intoa design, encourage stakeholder cooperation and coordination, and promote social acceptance of LAWS as a preferable future fact of war’. The approach requires ‘conceptaul, empirical and technical investigations’ to determine values of the skaholders, envision how those values can be construed as design requiremetns, and valuate how those design requirements can be supported’. Insufficient, too high level but is a good starting point. In fact, goes on to say programming LoW and RoE are more than sufficient to govern battlefield actions without expressing an understanding of the grim limitations of software robustness in benging environments like urban lanscapes notwithstanding the chaos of a battlefield environement.

Are standard risk assessments insufficient? Yes because extend up to the boundary of product safety, which is extremely rigorous.

# The Engineering Problem

There is a gulf between academic vs. government and industry. In public forums, general consensus among academics calling for a ban on AWS [cite]. UN Charter and Geneva Convention and Ban on Conventional Weapon Systems (CBRN, cluster bombs), Rules of War: norms on proportionality and rules of war.

In technical engineering journals, much has been said about design but limited to AWS safety for operators and maintainers. But nothing translates ethics into practice. Engineers working on AWS arent’ fully cognisant of the gravity of their work. Since AWS systems are so complex, engineers find themselves working on very small work packages and ethical implications seems far removed from their day-to-day experiences. How to inject ethical vigilance at this part of the process? How to promote ethical design methodologies and create procedural norms in the absence of strict regulation and strong guidelines from company that these engineers work in and the nation state that the defence companies work for?

Need for AWS outpaces call for restraint.

# Ethical arguments against AWS

1. Accounbility. *legitimacy is often linked to public demands of individual and political responsibility when force is used, particularly in cases that challenge norms of humanitarian law.65 The increasing autonomy of weapons systems raises the question to what extent different groups of individuals, engineers and programmers, political decision-makers, or military command and operating staff, are accountable for ‘decisions’ undertaken and mistakes committed by AWS*. Success here will be evaluated in real-time: regulation of big tech companies being held accountable for the side-effects of their products.
2. War requires human consciousness to imbue war with human dignity.
3. Appropriateness:

# Whose AWS Procedural Norm?

propose studying AWS in the context of two different, but interrelated normative spheres: the legal-public sphere – the primary realm of fundamental norms; and the procedural-organisational sphere – the primary realm of procedural norms.

‘a shared expectation about behavior, a standard of right or wrong’, 83 thereby linking norms to what is morally ‘right’. While this is certainly a key quality of norms, we argue for a broader understanding. Norms as standard of appropriateness can also comprise functional aspects such as efficiency and effectiveness in specific settings. A procedural norm in the military, for example, does not necessarily meet universal, public understandings of the morally ‘right’.

IEEE design methodology. Legal-public norms, including public expectations in terms of (political) accountability, lawfulness, or transparency.

For the military. . Operating AWS is very much based on procedural norms – they are governed by an emerging. As mentioned previously, the US drone program shows how new standards of ‘appropriate’ warfare may emerge in international relations.

Primary research

# Evaluation of Procedural Norms: BAE, Lockheed, Anduril, Boeing, AWS, Google, Microsoft, Palantir, Northrop, Kratos

# Evaluation of Procedural Norms: Chinese, Russian, Israeli, European, Australian, Middle Eastern. Countries (see response to AWS bans), See robotoics and autonomy strategies, see companies.

# Primary research

* Ethical procedures companies?

# Motivation

**Ethics of autonomous weapon systems (AWS).** Being ethical is not the same as doing whatever society accepts.

# \subsection{AS Ethical Risks Should be Elevated}\label{subsec2}

# The AWS ethical risks are obvious and much has been written about it in ethics, legal, engineering, military and political science journals and papers in support of the United Nations efforts for regulation. But there is inadequate discussion about how easy non-weapon based AS can be modified to become AWS systems. Consider the case of a seemingly benign autonomous logistics truck that is captured and re-purposed, packed with explosives and driven to a target location without human intervention. The ethical risks of non-weapon AS should be considered with more gravity than is currently afforded because it is only arms-length from becoming an AWS. Thus, companies working on non-weapon AS for defence should approach this activity with an awareness of their ethical responsibilities as if they were working on AWS.

# Citations

Bode (2018) *Autonomous weapons systems and changing norms in international relations*

<https://www.birmingham.ac.uk/research/perspective/ethics-of-warfare-heather-widdows.aspx>

Dipert (2010) The Ethics of Cyberwarfare, Journal of Military Ethics, 9:4, 384-410

Kania (2020) “AI Weapons” in China’s Military Innovation, Brookings Institute

Verdiesen I., Dignum V., Rahwan I. (2018) Design Requirements for a Moral Machine for Autonomous Weapons. In: Gallina B., Skavhaug A., Schoitsch E., Bitsch F. (eds) Computer Safety, Reliability, and Security. SAFECOMP 2018. Lecture Notes in Computer Science, vol 11094. Springer, Cham. https://doi.org/10.1007/978-3-319-99229-7\_44

1. AWS design and safety requiremetns [↑](#footnote-ref-1)