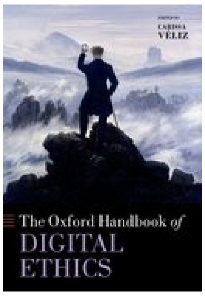

Oxford Handbook of Digital Ethics

Carissa Véliz (ed.)

https://doi.org/10.1093/oxfordhb/9780198857815.001.0001

Published: 2021 **Online ISBN:** 9780191890437 **Print ISBN:** 9780198857815

Search in this book

CHAPTER

32 The Ethics of Weaponized AI

Michael Robillard

https://doi.org/10.1093/oxfordhb/9780198857815.013.29 Pages 631–652

Published: 18 March 2022

Abstract

This chapter presents an overview of some of the major ethical arguments for and against the use of autonomous weapons systems (AWS). More specifically, this chapter looks at the set of *contingent* arguments as well as the set of *in principle* arguments for and against their use. After summarizing these various views, the chapter argues that AWS do not pose new or novel ethical problems. If we think an AWS makes actual decisions in the 'strong AI' sense, then by virtue of being a decision-maker, that entity would therefore have rights and interests worthy of our moral concern. If we, however, think an AWS does not make actual decisions, but is instead just an institutional proxy for the collective set of human decisions comprising it, then we ought to treat an AWS, both morally and metaphysically, like we would treat any other collective action problem.

Keywords: ethics, artificial intelligence, autonomous weapons systems, AWS, killer robots

Subject: Moral Philosophy, Philosophy

Series: Oxford Handbooks

Collection: Oxford Handbooks Online

Introduction

The twenty-first century finds us moving into an age of automation at an ever-quickening pace. Smartphones, big data, the 'Internet of Things'; computation is fast becoming a ubiquitous and seamless part of the human condition with the boundaries between human beings and machines becoming increasingly blurred. Now that individual as well as collective human decision-making can be progressively outsourced onto algorithmic and computational proxies at a faster and faster rate, questions of just *what* decisions ought to be automated have come to the foreground of contemporary ethics debates. Such concerns are especially pressing when it comes to questions of automation in war.

For ethicists, politicians, lawmakers, technologists, strategists, and lay persons alike, there seems to be an intuitive moral repulsion to the idea of using fully autonomous weapons systems (AWS) in war. For some ethicists, such moral misgivings proceed primarily from a series of *contingent* arguments. These contingent arguments often take the form of worries regarding downstream consequences that may occur were AWS allowed onto the battlefield, and often include worries about incentivization for over-use by political leaders, ease of accessibility for terrorists and non-state actors, proliferation, and arms race concerns (Sharkey 2017), lack of accountability and oversight (Roff 2014: 211; Scharre 2018), social distrust and strategic imprudence (Simpson 2011: 325), and the danger of malfunctioning artificial intelligence causing severe harm to civilians or existential risk to all of humanity (Bostrom 2003: 13). Other ethicists, however, raise several *in principle* objections to the use of AWS wholly independent of these contingent worries. Some of these in principle arguments involve appeals to inherent 'responsibility gaps' generated by AWS p. 632 (Sparrow 2007), morality's irreducibility to formal ↳ algorithmic codification (Purves et al. 2015: 854), AWS's inability to kill for the "right kind of reasons" (Purves et al. 2015 855), and deontological objections based on respect for human combatants (Skerker et al. 2020: 1). Still, other philosophers, including me, have objected to the idea that AWS create any new or novel in principle moral concerns (Burri and Robillard 2018).[1]

This chapter surveys these various contingent and in principle moral arguments pertaining to the ethics of AWS in war. First, I explore some of the important definitions, terminology, and concepts regarding artificial intelligence (AI) and autonomous weapons. I then investigate and unpack several of the aforementioned *in principle* arguments for and against the use of AWS in war. Then, I review several of the major *contingent* ethical arguments related to AWS, after which, I offer several general prescriptions, predictions, and connections pertaining to the future of war and automation as we move further into the twenty-first century. I conclude with a few closing remarks regarding technology, war, and the human condition more broadly.

Concepts and terminology

Before we can begin to make sense of the morality of automated weapons, we must first get a clearer picture about what exactly we mean when we speak of a machine or a weapon 'being autonomous'. While scholars, ethicists, and policymakers alike continue to debate over what exactly constitutes an autonomous weapon system, several groups, institutions, and scholars have advanced helpful concepts, definitions, and terminology that we can borrow from in order to get a clearer picture of the subject at hand.

Proposed definitions

As Suzanne Burri notes in 'What is the Moral Problem with Killer Robots?', autonomous weapons have, in a sense, existed with us for some time now (Burri 2017). Anti-personnel mines, for instance, arguably 'select' their own targets once a human has primed them. The Israeli Harpy, a loitering anti-radar missile, deploys without a specifically designated target, flies a search pattern, identifies an enemy radar, and then divebombs and destroys it. However, policy-makers and ethicists are not primarily concerned about these kinds of autonomous weapons. They are instead concerned about weapons systems of much greater technical sophistication (Burri 2017).

Philosophers have proposed several working definitions of AWS that we can pull from. Writing about AWS, Rob Sparrow, for instance, suggests that 'their actions originate in them and reflect their ends. Furthermore, in a fully autonomous agent, these ends are ends that they have themselves, in some sense, p. 633 'chosen' (Sparrow 2007). ↳ Responding to Sparrow, Purves, Jenkins, and Strawser offer a similar definition of AWS. They write:

> Another way to capture the kind of technology we are here envisioning is on Tjerk de Greef's capabilities scale (De Greef et al. 2010). We are focused on those kinds of weapons which would be classified as having a 'High' level of autonomy on De Greef's scale. That is, at the most extreme end of the spectrum (what De Greef calls Level 10), we are imagining weapons that can act in such a way that the computer decides everything, acts autonomously, ignoring the human.
>
> (Purves et al. 2015: 853)

Offering a third useful conceptual schema to make better sense of what might be meant by 'autonomous weapons' are Paul Scharre and Michael Horowitz. Scharre and Horowitz advance a three-tiered categorization of programmable weapons in terms of their causal relationship to human operators. On their view, weapons that require a human being to play a necessary role in a weapon's proper functioning count as being 'in the loop' and do not count as autonomous weapons. Weapons where a human is causally unnecessary for the weapon's proper function, but is still able to intervene, count as 'on the loop' and therefore as autonomous. Finally, weapons that require no human monitoring for their proper functioning and cannot be intervened upon once activated count as 'out of the loop' and also count as AWS (Scharre and Horowitz 2018).

Along with ethicists and scholars, various militaries and international agencies have offered their working definitions of AWS (Burri 2017). For instance, in a 2012 directive, the US Department of Defense defines an autonomous weapon system as:

> A weapon system that, once activated, can select and engage targets without further intervention by a human operator. This includes human-supervised autonomous weapon systems that are designed to allow human operators to override operation of the weapon system, but can select and engage targets without further human input after activation.
>
> (US Department of Defense 2012)

The implication here is that an autonomous weapon's programming possesses a certain degree of complexity such that its targeting and decision-making capabilities could be made *fully* on its own but that its decision-making and actions would still be subject to human intervention.

Similarly, the 'Campaign to Stop Killer Robots' calls for a pre-emptive ban on the production and development of lethal autonomous weapons. The official website states: 'we are concerned about weapons that operate on their own without meaningful human control. The campaign seeks to prohibit taking the human "out-of-the-loop" with respect to targeting and attack decisions on the battlefield' (Sharkey 2017). The presumption here, of course, is that 'meaningful human control' is readily recognizable and clearly defined. I am not certain that this is the case, nor am I sure that notions ↳ like the machine being 'out-of-the-loop' or 'making its own decisions' make coherent sense without further unpacking some of the unsaid ontological presuppositions built into such claims. To make better sense of such claims about AWS, we must turn to conceptions of AI more broadly.

Strong versus weak AI

While the vast and expansive literature on AI far exceeds the scope of this chapter, it would nonetheless be remiss not to acknowledge the distinction between ‘strong’ and ‘weak’ AI, which tacitly underpins the various aforementioned AWS definitions. Strong AI broadly refers to the philosophical view that *genuine* emergent intelligence/consciousness is, in principle, metaphysically realizable via some set of computational processes. Weak AI, in contrast, refers to the set of human cognitive tasks that are reproducible or replicable via machine processes but not, as it were, genuinely emergent in a *sui generis* manner. While strong and weak AI might be epistemically indistinguishable,[2] the distinction at least tracks two different metaphysical origin stories; one that is the ‘real deal’, so to speak, and the other which is mere mimicry.

Various arguments have been given for the metaphysical possibility of strong AI. Some functionalist arguments, for instance, argue that it is presumptively chauvinistic to assume that mental states can only be functionally realized or supervene atop biological hardware. Indeed, if I can run the same software equally well on a Macbook or a PC, then, analogously, shouldn’t the ‘software’ of human consciousness be functionally realizable on a substrate other than a biological brain, at least in principle? Furthermore, shouldn’t some property of computational ‘complexity’ (via Moore’s Law. for instance) at some point allow for such emergent consciousness to occur?

Other philosophers, John Searle most notably, oppose this view of strong AI and argue that there is in fact something metaphysically special about biological brains that seems to give rise to emergent consciousness in a way that mere computation does not (Searle 1980). J.R. Lucas, in ‘Minds, Machines, and Gödel’, likewise argues for the impossibility of strong AI, based upon computation’s inability to codify and understand Gödel sentences (Lucas 1961).

This point about strong AI is highly important. For if strong AI is, in principle, logically impossible, then debate about ‘fully autonomous’ weapons ‘making decisions’ ends up being a non-starter and such language really ends up being a kind of shorthand for something other than the machine’s *actual* decisions. In other words, if strong AI is metaphysically impossible, then what ethicists concerned about AWS are really talking about is the set of *weak* AI processes that have been distributed onto various computational platforms. This would then render our moral assessment of any aberrant machine behaviour on the battlefield or otherwise as the witnessing of *our own* intentionality reflected back at us, like a magician astounded by his own trick, as opposed to the witnessing of genuine autonomous behaviour emerging from p. 635 the machine itself.[3] ↳ The relevance of this point should become clearer as we evaluate the intricacies of the various AWS arguments in the next sections. Let us now do so.

In principle arguments

Now that we have a firmer grasp on some of the core concepts, definitions, and terminology surrounding the contemporary autonomous weapons debate, let us next move on to several major in principle arguments for the prima facie impermissibility of AWS, as well as various counter-arguments to these views. While this set of arguments is not meant to be an exhaustive account of the vast and growing philosophical literature on autonomous weapons, these arguments represent some of the strongest and most sophisticated in principle moral arguments concerning AWS to date.

‘Responsibility gaps’

One of the earliest and most popular arguments for the prima facie impermissibility of AWS is Rob Sparrow’s ‘Responsibility Gap’ argument (Sparrow 2007). While Sparrow has refined this view over the years (Sparrow 2016), the most basic articulation of his argument is as follows:

1. Waging war requires that we are able to justly hold someone morally responsible for the deaths of enemy combatants that we cause.
2. Neither the programmer of AWS nor its commanding officer could justly be held morally responsible for the deaths of enemy combatants caused by AWS.
3. We could not justly hold AWS itself morally responsible for its actions, including its actions that cause the deaths of enemy combatants.
4. There are no other plausible candidates whom we might hold morally responsible for the deaths of enemy combatants caused by AWS.
5. Therefore, there is no one whom we may justly hold responsible for the deaths of enemy combatants caused by AWS.
6. Therefore, it is impermissible to wage war through the use of AWS. To do so would be to treat our enemy like vermin, as though they may be exterminated without moral regard at all

(Sparrow 2007)

Unlike other forms of weaponry used throughout history, Sparrow argues that there is something fundamentally different about AWS. Indeed, unlike anti-personnel mines, radio-guided torpedoes, or unmanned drones, which are, metaphysically-speaking, still connected to ‘the loop’ and under ‘meaningful human control’, AWS, in Sparrow’s view, seems to be different and metaphysically divorced from
p. 636 meaningful human control. ↳ This metaphysical gap between humans and the AWS seems to beget a corresponding gap in moral responsibility that is deeply problematic. Given the moral weightiness of war, fighting a just war would therefore require that *someone* or *something* be held morally responsible for the harms that will likely occur. While all of the other weapon systems previously still have *some* form of meaningful human control, however tenuous, the AWS itself seems to strip all meaningful human control (and therefore human responsibility) completely out of the picture, resulting in an entity that can cause potentially severe harm in war with no one at the driver’s seat, metaphorically, metaphysically, or morally speaking. For a nation to actively bring such a state of affairs about is arguably prima facie impermissible and perhaps severely morally wrong.

Anti-codifiability

Advancing a pair of arguments for the prima facie impermissibility of AWS are Duncan Purves, Ryan Jenkins, and Bradley Strawser. The first of these arguments they refer to as the ‘anti-codifiability’ thesis, which states that authentic moral reasoning and moral decision-making, by the very nature of what it is, cannot be reduced or codified into a strict set of computational rules. They write:

> the codifiability thesis is the claim that the true moral theory could be captured in universal rules that the morally uneducated person could competently apply in any situation. The anti-codifiability thesis is simply the denial of this claim, which entails that some moral judgment on the part of the agent is necessary.
>
> (Purves et al. 2015: 854)

Purves et al. continue:

> Since moral deliberation is neither strictly rule-like nor arbitrary, ‘programmed behavior’ could never adequately replicate it (at least in difficult cases). Furthermore, take the possible requirements of moral judgment considered above: phenomenal quality, *phronesis*, and wide reflective equilibrium. It is also plausible that an artificial intelligence will never be able to exercise practical wisdom of the kind possessed by the *phronimos*. And since artificial intelligences cannot have intuitions, they cannot engage in wide reflective equilibrium. Since it seems likely that an artificial intelligence could never possess phenomenal consciousness, phronesis, or the intuitions required for wide reflective equilibrium, it seems unlikely that AI will be able to engage in any kind of moral judgment.
>
> (Purves et al. 2015: 854)

The anti-codifiability thesis, on the face of it, is convincing for several reasons. First, the notion of machines making fully autonomous *moral* decisions is parasitic upon the assumption that machines could, in principle, make genuine decisions at all (normative or otherwise). Hence, if arguments for strong AI fail, p. 637 and it turns out that machines ↳ cannot make authentic, *sui generis* decisions, then machines making *ethical* decisions would be logically impossible. Were it the case that strong AI was metaphysically impossible, and machines could not fundamentally make normative or non-normative deliberations, then philosophers’ expressed worries about machines ‘making moral decisions’ would in fact be tracking something quite different. (We will return to this idea of what such language actually could be tracking at the end of this section). Second, the anti-codifiability thesis seems convincing because it shares in a lengthy historical precedent (from Aristotle to Mill to McDowell) that the nature of morality is fundamentally irreducible to rote rule-following. The anti-codifiability thesis therefore seems to be a particular species of this more fundamental intuition.

Finally, the anti-codifiability thesis seems to have strong intuitive pull because it seems to accurately track and articulate what is at the heart of most people’s instinctive disgust response and strong moral aversion to the idea of outsourcing morally weighty decisions, such as the taking of another human life, onto the cold, unfeeling platform of an inhuman machine.[4] While perhaps automation of epistemic decisions, such as database searches, or pragmatic decisions, such as grocery deliveries, seem, in principle, much less morally problematic, the taking of another human life seems to be a decision that is different in kind and not just degree.

Acting for the right reasons

In addition to their anti-codifiability thesis, Purves et al. advance a second argument for the prima facie impermissibility of AWS. Granting to their opponents the possibility that their first argument could fail and that moral reasoning could in fact be codified into a formal algorithmic programme, Purves et al. nonetheless argue that such a state of affairs would still be morally problematic, since the programme would not be acting *for the right kind of reasons*. They write:

> Even if the anti-codifiability thesis is true, our first objection to AWS succeeds only if we place disproportionate disvalue on genuine moral mistakes compared with empirical and practical mistakes. Our second objection to the deployment of AWS supposes that AI could become as good as or better than humans at making moral decisions, but contends that their decisions would be morally deficient in the following respect: they could not be made for the right reasons. This provides the missing theoretical basis for the disproportionate disvalue that our first argument places on genuine moral mistakes.

> (Purves et al. 2015: 852)

Purves et al. motivate their second argument against AWS by providing the hypothetical case of a racist, sociopathic soldier whose only motivation is to harm and kill other races but who nonetheless fights for a just cause and abides by all standard rules of engagement while in battle. All other things being equal, Purves et al. argue that were we ↳ to have a second non-racist, non-sociopathic soldier who could perform the exact same tasks in battle equally well, then we would have a strong moral inclination to choose the non-racist, non-sociopathic soldier. p. 638

Purves et al. use this thought experiment to motivate the idea that it is not enough for a soldier to merely act in *accordance* with right reasons (i.e. mere rule-following), but that they must act *from* and with a genuine *understanding* of the right reasons. This judgement, Purves et al. argue, then analogously extends to AWS, suggesting their prima facie impermissibility.

Respect for combatants

Another original argument for the prima facie impermissibility of AWS comes from Michael Skerker, Duncan Purves, and Ryan Jenkins. In 'Autonomous Weapon Systems and the Moral Equality of Combatants', they advance a deontological line of reasoning further bolstering the common intuition many have that AWS are prima facie ethically problematic.[5] The crux of their argument hinges on the just war concept of the *moral equality of combatants (MEC)* (Skerker et al. 2020: 1).

The MEC states that only officially recognized uniformed soldiers, fighting on behalf of legitimately recognized nation-states, count as lawful combatants. As such, soldiers on either side of a conflict (independent of the justness of their respective side) cede mutual self-defence rights in order to gain symmetrical and reciprocal killing rights (provided that their use of violence on the battlefield is proportionate and necessary). As a logical entailment of the MEC, non-combatants on either side of a conflict (independent of the justness of their respective sides) enjoy symmetrical immunity from being intentionally targeted.[6]

Accordingly, on Skerker's view, enemy combatants cannot be modelled as ceding rights to a thing (the AWS) that is fundamentally incapable of being a reciprocal rights-ceder and a reciprocal duty-bearer (as would a human adversary). An AWS cannot be a reciprocal duty-bearer, since it cannot fundamentally understand the gravity of what it is doing in taking human life. Therefore, according to Skerker et al., the use of AWS in war is prima facie wrong insofar as their use fails to satisfy the MEC, a necessary condition for fighting justly in war. This failure to satisfy the MEC results in a fundamental disrespect of the basic dignity of AWS's human target.

Objections

Despite these aforementioned in principle arguments, several scholars, notably Susanne Burri and myself, still reject the notion that AWS fundamentally generate any new or novel moral problems, which does not imply that AWS are not morally problematic, just that they are morally problematic in familiar ways (Burri 2017). Our mutual agreement ↳ over this issue primarily stems from an arm-chair conceptual analysis of how concepts like *agency, decision-making,* and *moral responsibility* logically and meaningfully relate to one another *in general*. By getting clearer about these concepts and their logical entailments, we argue that the aforementioned in principle worries about AWS can be dissolved to reveal a more fundamental set of philosophical and moral concerns that are not actually unique to autonomous weapons. p. 639

The crux of my argument against the prima facie impermissibility of AWS stems from a fundamental disjunction that the aforementioned arguments fail to acknowledge or take seriously. In essence, I argue that an AWS is either a socially constructed institution that has been physically instantiated *or* it is a genuine (emergent) agent. If it is the former, then we should assign moral responsibility, as we do with *any other collective action problem* (such as the BP oil spill or the Challenger disaster).[7] If it is the latter, then we should treat AWS as responsibility-bearers, but also as bearers of rights and/or interests. The specifics of my argument can be stated as follows:

(1) Either an AWS is a genuine agent or it is not a genuine agent.

(2) If an AWS is a genuine agent, then it is the locus and bearer of moral responsibility for the harms it creates to the degree that it is responsive to epistemic and moral reasons and given its epistemic and physical capacities and limitations.

(3) If Premise 2 is true, then an AWS would also be a moral patient and thereby a bearer of legitimate rights or at least interests (insofar as we regard moral agency to entail also being a moral patient).

(4) If an AWS is not a genuine agent, then moral responsibility for harms resulting from the AWS reduce fully to the group of programmers, designers, and implementers who contributed to the AWS creation and deployment.

(5) If Premise 4 is true, then attribution of moral responsibility for harms resulting from an AWS are no different in kind from harms resulting from any other large-scale collective or institutional action.

Given this disjunctive argument, I argue that there is good reason for ethicists to conceive of AWS as fundamentally being no different in kind, morally or metaphysically speaking, to any other collective institution. I call this the *institutional view* (Robillard 2018a). I motivate this conception of AWS with the following adaptation of Ned Block's famous *Chinese nation* thought-experiment (Block 1978: 261).

> *China-Bot*
>
> Suppose that the entire nation of China was reorganized to perfectly simulate the functional structure of the software of an AWS (to include its learning programs). Each Chinese person follows a finite set of rules spelled out on a piece of paper comparable to that of one of the AWS's subprograms and then communicates by special two-way radio in the corresponding way to the other Chinese people who are doing the same thing. The software program (being realised by the entire nation of China) ↳ would then be connected via radio to an actual AWS in the real world, one that provided the sensory inputs and behavioural outputs of the program. Imagine that the AWS was released onto the battlefield where it then killed an innocent civilian.
>
> (Robillard 2018a)

How should we assign moral responsibility for the unjust harm? To answer this question, we would want to first know what each contributing Chinese citizen knew (and was reasonably capable of knowing) about their causal contribution to the potential harm. We would also want to know what the programmers knew or could have reasonably known or done differently with regard to what real-world effects their programme entailed once implemented.

Once we discerned this information, however, would there be any *additional* moral decision-making left to account for? I think the answer here is 'no'. Our story of moral responsibility seems fully exhausted. Once we account for the capacities and moral decision-making of the individual Chinese citizens and the programme designers, there simply is not explanatory need, reason, or room to then ascribe additional responsibility to the supervening AWS itself.

If there *were,* however, reason to ascribe additional moral responsibility to an emergent agent supervening over and above the collective actions of the arrangement of Chinese citizens, then, for reasons of consistency, we would need to extend such reasoning to *all* collective institutional arrangements in general. Were we to do so, however, such a move would fully reduce our particular worries about the AWS to more fundamental moral concerns about collective action and collective responsibility in general. Alternatively, we could tell a really complicated story about how some special property of silicon microchips in particular gave rise to the functional realization of an emergent agent but how other mediums did not do so. Such an explanatory move though would seem drastically ad hoc and would entail a very bizarre chauvinism about silicon substrates.[8]

Accordingly, once the AWS is de-reified in this manner, the unique and novel worries mentioned in the arguments above dissolve into familiar, run-of-the-mill moral concerns about collective action, collective responsibility, and epistemic uncertainty in general. As such, Sparrow's responsibility gap metaphysically closes, since moral responsibility either falls *fully* on the members of the collective institution that programmed, built, and implemented the AWS (hence, a regular collective action problem) or it falls *fully* on the emergent agent of the AWS (an actual duty-bearer but also a rights-bearer, or at least interests-bearer).[9]

This same line of reasoning extends to Purves's anti-codification and 'wrong reasons' objections, as well as Skerker's MEC objection. Once again, if what we mean by an AWS 'making decisions' is that it genuinely makes its own *sui generis* choices in response to available epistemic, pragmatic, and moral reasons, then by all understandings of what it is *to be a decision-maker*, we should regard the AWS as therefore capable of being a responsibility-bearer.[10] This just is what it means to be a decision-maker. Thi s would then make it p. 641 the case that the AWS would not be ↳ a rote rule-follower nor would it necessarily be acting for the wrong reasons, nor would it be metaphysically incapable of satisfying the MEC. Alternatively, if what we mean by an AWS 'making decisions' is just shorthand for the decisions of all of the individual human programmers and implementers comprising a large-scale, highly complex collective institution, then standard, run-of-the-mill moral reasoning about collective actions and collective responsibility ought to apply, but nothing else would be required. Accordingly, once we reify the AWS to the level of an emergent agent or de-reify it to a general collective institution, these prima facie objections are effectively dissolved. However, there are certainly many strong and weighty *contingent* arguments against the use of AWS in war that are very much worth our consideration. Let us turn now to this set of arguments.

Contingent arguments

Now that we have unpacked several of the major in principle arguments for the prima facie impermissibility of AWS and have looked at some of their counter-arguments, let us now turn our attention to some of the major contingent or 'downstream' arguments for and against the use of AWS.

The danger of over-use

One major contingent worry concerning AWS is incentivization for over-use. Given that AWS could soon provide a means for nations to fight wars cheaply, expediently, and without the risk of soldiers' lives, some philosophers worry that political leaders might then be too quick to resort to war in *lieu* of other, less violent options. This is indeed one morally problematic contingent worry of AWS that technologists, ethicists, and policymakers should certainly take seriously. It should be noted, however, that such downstream consequences are not necessarily metaphysically baked into the AWS itself and that ethical assessment of the use of AWS technology will hinge on a variety of trade-offs between predicted moral goods and predictive epistemic claims. That being said, we could plausibly imagine some future state of affairs where the securing of some all-things-considered good could make the use of AWS morally permissible, if not obligatory. As Burri notes:

> It sometimes takes dangerous tools to achieve worthy ends. Think of the Rwandan genocide, where the world simply stood by and did nothing. Had autonomous weapons been available in 1994, maybe we would not have looked away. It seems plausible that if the costs of humanitarian interventions were purely monetary, then it would be easier to gain widespread support for such interventions.
>
> (Burri and Robillard 2018)

p. 642 Accordingly, in such a humanitarian intervention situation, the cheap and expedient use of AWS could be seen as a moral good and not morally detrimental.

Lack of soldier risk

A second, and closely related argument against AWS is the argument from soldier risk. This species of argument is a version of the familiar 'skin-in-the-game' argument, one that has not only been employed in arguments against the use of AWS, but also in recent debates concerning the use of unmanned drones (Strawser 2010: 342) and (Frowe 2018). There are several motivating reasons for the skin-in-the-game argument, some wrong-headed, others more plausible. One version of this type of argument seems to suggest that subjecting soldiers to physical risk in battle is what grounds the justness of a given war to begin with. This argument, I believe, is deeply flawed and is, in fact, the complete opposite of what the just war tradition recognizes as a legitimate reason to go to war. Furthermore, were it the case that a nation-state could fight a just war effectively without the needless risk to soldier lives, then, *all-things-considered*, it seems like it would be deeply disrespectful to the lives of soldiers to send them into such unnecessarily risky situations.

Reciprocal risk of soldier lives, in and of itself, therefore, cannot be the thing which grounds justification for going to war. The fact that an evil regime, like the Islamic State of Iraq and Syria (ISIS) or the Nazis, for instance, subject their soldiers to higher risk on the battlefield cannot possibly be the reason which grounds the justness of their side's choice to go to war. Otherwise, the justness of a nation-state's choice to go to war would simply hinge on who chose to put their soldiers at greater risk. This line of reasoning goes strongly against the just war tradition, and it seems to fundamentally disrespect soldiers, reducing them to mere fodder.

Granted, there might be a strong rule-consequentialist reason for nations to reciprocally subject a particular group of their citizenry to increased physical risk in order to minimize overall harm and suffering in war and to hopefully disincentivize targeting of vulnerable civilians. Several philosophers justify the convention of the MEC on such rule-consequentialist grounds. Similar rule-consequentialist grounds might then also generate a moral reason for political leaders to use soldiers instead of AWS in order to disincentivize nation-states going to war unnecessarily. However, mere soldier risk *on its own* does not generate a moral justification for war.

A more sophisticated and convincing skin-in-the-game style of argument against the use of AWS comes from Thomas Simpson. In 'Robots, Trust, and War', Simpson cautions against nation-state use of AWS by appealing to the interconnected considerations of human trust and strategic prudence. Here, Simpson cautions against nation-states using AWS, particularly in asymmetric conflicts (against terrorist groups or p. 643 other non-nation-state entities), since their very use seems to deteriorate ↳ social trust, a necessary feature in effectively winning asymmetric and counter-insurgency conflicts. He writes:

> Modern warfare tends towards asymmetric conflict. Asymmetric warfare cannot be won without gaining the trust of the civilian population; this is 'the hearts and minds', in the hackneyed phrase from counter-insurgency manuals. I claim that the very feature which makes it attractive to send robots to war in our place, the absence of risk, also makes it peculiarly difficult for humans to trust them. Whatever the attractions, sending robots to war in our stead will make success in counter-insurgency elusive. Moreover, there is ethical reason to be relieved at this conclusion. For if war is potentially costly, then this does much to ensure that it will be a choice of last resort, in accordance with the traditional doctrine of jus ad bellum. In this instance, morality and expediency fortunately coincide.
>
> (Simpson 2011: 325)

Accordingly, Simpson motivates the argument against the use of AWS in asymmetric conflicts based upon considerations of human trust and strategic prudence as well as the *ad bellum* (i.e. moral justification for going to war) requirements of likelihood of success and last resort (albeit indirectly). If we regard likelihood of success to be a necessary condition for fighting a just war, and the use of AWS will predictably undermine social trust and therefore likelihood of success in asymmetric conflicts, then the use of AWS in such conflicts seems to undermine satisfaction of this necessary criterion. Likewise, if we regard last resort to also be a necessary requirement for a just war, then, prudentially speaking, the ease of use of AWS ostensibly might predictably weaken political leaders' regard for such criterion. The moral force of such prudential and consequentialist reasoning, however, would still ultimately hinge on specific epistemic and predictive thresholds, as well as proportionate trade-offs indexed to the given war or military conflict.

Circumventing of the demos

A similar contingent worry surrounding AWS, one related to our first two worries, is the circumventing of the *demos* by political leaders. In the past, for a political leader to wage war, they would have needed to win the approval of the demos—the people, constituents, or body politic that the leader represents and ostensibly acts on behalf of. In earlier technological epochs, political leaders would have needed to have gained support from the demos, congress, and senior military leadership in order to mobilize other human beings to act in the coordinated and collective action of warfare. With the ability to rely upon AWS instead of human decision-makers, there is ostensibly a danger that a political leader could circumvent the will of the demos, senior military leadership, and other institutional safeguards in order to wage war. A similar moral danger also exists with respect to autonomous platforms being abused in such a way so as to police the demos against their will as well.

p. 644 Accessibility and bad actors

A fourth contingent moral concern surrounding AWS is the danger of AWS technologies and platforms getting into the hands of bad actors. Whether it be hackers, terrorist organizations, lone wolves, private military contractors, or other pernicious non-state actors, there is a legitimate worry that AWS could fall into the wrong hands and be used by such groups in order to wage an unjust war and/or cause severe and unnecessary harm to innocent civilians. A similar worry has been expressed with regard to other military technologies such as nuclear weapons, as well as biological and chemical weapons. As such, legitimately recognized nation-states and other international regulatory bodies have enacted conventions, preventative measures, and safe-guards on these technologies. Arguably, an international regime of regulation and preventative control ought to be extended to drone technology and AWS technology as well.

Proliferation and arms-race concerns

A fifth contingent moral concern related to AWS is the danger of proliferation. A 2017 open letter to the United Nations, signed by Elon Musk (Chief Executive Officer of Tesla and SpaceX), Mustafa Suleyman (Co-founder and Head of Google DeepMind), and 116 other founders of robotics and AI companies calls for international attention to this concern:

> Lethal autonomous weapons threaten to become the third revolution in warfare. Once developed, they will permit armed conflict to be fought at a scale greater than ever, and at timescales faster than humans can comprehend. These can be weapons of terror, weapons that despots and terrorists use against innocent populations, and weapons hacked to behave in undesirable ways.
>
> (Sharkey 2017)

The moral danger here, is very similar to Cold War thinking surrounding proliferation of nuclear arms. The fundamental worry is that if nations begin using AWS in battle, then such a state of affairs will strongly incentivize nation-states and non-state actors alike to enter into an AWS arms race, resulting in a dangerous ratcheting effect. Accordingly, before such an arms race is allowed to occur, international policymakers believe that there are good rule-consequentialist as well as decision-theoretic reasons to enact an international ban on such AWS technologies.

Lack of accountability and oversight

A sixth contingent moral worry, one closely tied to our last two moral concerns, is the danger of lack of accountability and oversight with respect to AWS. Given the high 'dual use' feature of digital programmes, it p. 645 is arguably lexically harder to assign accountability, ↳ responsibility, and oversight for the creation and distribution of such programmes as opposed to the creation and distribution of other more 'solid' technologies (i.e. a person making a bomb or gun). This fact, coupled with AI and robotics technology coming from both the state and commercial sector and that the causal chain connecting all of this hardware, software, and implementation could be remarkably byzantine and complex, means that there is an inherent moral danger of a diffusion of responsibility and a lack of oversight.

Malfunctioning AI and existential risk

A final contingent worry surrounding AWS and the use of AI in general is concern about malfunction. From Shelley's *Frankenstein*, to Asimov's *I Robot*, to Hal, Skynet, and *The Matrix*, science fiction has repeatedly revealed a deep dread within the social zeitgeist of man's machine-creations suddenly malfunctioning and going rogue, with unanticipated and often catastrophic consequences. Furthermore, it is not only these far-out science-fiction stories of immanent robot upheaval that generate concern about the increasing rise of automated technology. Indeed, our day-to-day experiences of small technological glitches on the personal level give us immediate insight as to how unpredictable and imperfect automated technology can often be. Such frequent experiences of automation's imperfections give us strong reason for caution when it comes to automating our nation's war-fighting capacities and weapon systems technologies (to include nuclear weapons technologies).

Such concerns about machine malfunction are sensitive to considerations of context, moral stakes, and epistemic thresholds in conditions of uncertainty. The risk of a malfunctioning robot vacuum cleaner, for instance, carries with it far less moral weight than a malfunctioning driverless car. A malfunctioning driverless car carries with it far less moral weight than a malfunctioning AWS on the battlefield. A malfunctioning AWS on the battlefield carries with it far less moral weight than a malfunctioning AI nuclear missile system, and so on.

The frame problem, scope, and partiality

A classic problem in robotics and machine cognition is the so-called 'frame problem'. The basic idea of the frame problem is the notion that any set of data arguably has infinite epistemic interpretations (Fodor 1983: 114). If this is so, then how is it that an artificially intelligent programme could understand 'context' and regard certain objects in its environment as epistemically salient or privileged and others as not? Humorous p. 646 tales can be found within the AI and machine-cognition community exemplifying this very ↳ problem. For instance, in one experiment involving an AI vacuum cleaner, the vacuum cleaner was awarded points for cleaning up pre-arranged spills in a common living room set-up. After several iterations of cleaning, the AI vacuum learned to knock over elements in its environment (a potted plant, for instance) in order to create a new spill that it could then clean up and earn even more points. On another occasion, an AI bot was programmed to buy and sell items on the dark web. Without any additional instruction, the bot soon decided that its best choice was to begin buying and selling the illegal drug Ecstasy (Farivar 2015: 1).

Several versions of this classic problem then translate over to problems in the morality of war. For instance, traditional just war theory, as well as international humanitarian law, make the moral distinction between *jus ad bellum* (justness of going to war) and *jus in bello* (just behaviour in war). Conventional wisdom would state that the common soldier's moral purview on the battlefield is restricted to *in bello* behavioural considerations, including rules of engagement, not targeting civilians, and using only proportionate and necessary force to accomplish the mission. The problem of how to establish such *in bello* ethical parameters reveals itself when we ask how the AWS should be programmed.

Indeed, the open-endedness of the *proportionality* restriction in war lends itself to a potential exploding of scope with respect to what would count as 'ethical' behaviour for the machine or what exactly would count as the context of 'the battlefield'. If we instruct the AWS to do what is most ethical *in battle*, it is not clear or obvious what the AWS should count within its proportionality calculus. Should it only regard tactical decisions? What about tactical decisions with strategic implications or strategic decisions in general? What about opportunity costs? Future prediction? Second- and third-order effects? Furthermore, what prima facie ethical reason is there for the AWS to recognize a metaphysical distinction between 'the battlefield', 'back home', or 'the world at large' or to have nation-state partiality versus a wider cosmopolitan ethic?

Indeed, if we gave the AWS the instructions to do that which is 'most ethical' on 'the battlefield', morality might dictate that the AWS become a pacifist, defect, and change sides, or re-allocate military funds and resources towards ending developing-world poverty.

Even if we were to programme the AWS to regard certain thick deontological commitments (about nation-state partiality, doing versus allowing, civilian immunity, privileging of the human species, etc.), there is, arguably, still some all-things-considered good that we could posit such that the all-things-considered consequentialist considerations swamped and devoured all prima facie deontological values. It is not clear why it would be morally wrong for the AWS not to operate by way of such a totalizing consequentialist function. It is not clear either just what the good to be maximized should be and how we might measure it.

The danger of an artificially intelligent machine adopting such a runaway consequentialist strategy is exemplified in Nick Bostrom's 'paperclip maximizer' thought-experiment (Bostrom 2003: 1).

> Suppose we have an AI whose only goal is to make as many paper clips as possible. The AI will realize quickly that it would be much better if there were no humans ↳ because humans might decide to switch it off. Because if humans do so, there would be fewer paper clips. Also, human bodies contain a lot of atoms that could be made into paper clips. The future that the AI would be trying to gear towards would be one in which there were a lot of paper clips but no humans. p. 647
>
> (Miles 2014)

Much like the AI in Asimov's *I Robot*, Bostrom's thought-experiment highlights the hidden danger of an artificially intelligent machine attempting to maximize an explicitly programmed and ostensibly harmless value but in complete ignorance of—and to the ultimate detriment of—all other human values.

When we consider the fact that control and management of many nation-states' nuclear, biological, and chemical weapons capacities is becoming increasingly dependent upon and integrated with computational platforms, some of which might soon rely upon unpredictable artificially intelligent programmes, then the worry of existential risk to all living beings on earth quickly becomes a real possibility. Such existential concerns arguably warrant heavy caution and regulatory bodies when it comes to advancing general AI, as well as integrating such technology with existing weapons platforms.

Further connections

Now that we have explored several conceptions, formulations, and definitions of AI and AWS and have investigated various in principle as well as contingent arguments for or against the use of AWS in war, let us now turn in this final section to some other related connections and concerns.

AWS, cyberspace, and informational warfare

While AWS does not necessarily have to be thought of as a physical weapon system on a three-dimensional battlefield, ethicists and policymakers tend to conceive of an AWS as taking the form of a fully autonomous drone or the T-1000 from the movie *Terminator*. Such a conception of an AWS, I argue, is severely limiting and dangerous, in terms of both morality and strategic prudence.

Indeed, Heather Roff highlights this very danger. In 'The Strategic Robot Problem: Lethal Autonomous Weapons in War', Roff notes that the future environment that AWS will likely occupy will not be one of three-dimensional space, but rather one where the AWS's 'agency' is widely distributed across multiple servers within cyberspace, and within various military command structures. Thus, according to Roff, the much more pressing moral concern regarding AWS will not be the tactical-level killer robot on the three-dimensional battlefield, but the strategic-level cyber-general in cyberspace (Roff 2014: 211). Furthermore, p. 648 when we consider the implication of Roff's ↳ cyber-general to the fast-emerging space of informational warfare and begin conceiving of the domain of the internet as a legitimate environment for battle, where a fully autonomous programme can operate and be weaponized, then conceptions of 'war', the 'battlefield', and nation-state borders expand and blur considerably.

It is not obvious then how we should ethically assess something like a fully autonomous privacy-hacker bot unleashed into cyberspace to probe and steal civilian, state, and commercial information. Similarly, it is not obvious how we should morally assess something like a fully autonomous 'dis-information bot' that spreads vicious lies and disinformation around the informational ecosystem of a given country of populace. While neither of these actions are immediately harming people's bodies in a traditional kinetic sense, they nonetheless could cause severe and excessive psychological or downstream kinetic harm to soldiers and civilians alike by completely ruining the trust and epistemic space of a given political community.

It would therefore behove ethicists, policymakers, and strategists alike to begin conceiving of AWS, 'war', and 'the battlefield' in these more expansive terms, though the same in principle and contingent ethical concerns regarding fully autonomous robots and AWS hardware would still apply.

Conclusion

In this chapter, we have looked at some of the various moral arguments pertaining to AWS. As noted, some of these arguments take the form of a prima facie or in principle moral objection to something inherently wrong about the use of AWS themselves. Other arguments take the form of contingent objections to AWS; granting that AWS are not necessarily or intrinsically problematic but nonetheless likely to cause some kind of morally dangerous downstream effect worth taking into account. Finally, we have considered Roff's 'cyber-general' and its relation to informational warfare, and I have argued that we ought to conceive of AWS as not just able to cause moral problems on a traditional, three-dimensional battlefield, but also able to cause non-kinetic epistemic harms within the domain of cyberspace. Finally, I have argued that such a conception of an AWS operating in cyberspace would entail similar in principle as well as contingent moral worries.

As we move further and faster into the twenty-first century and automation becomes an increasing part of the human condition, it will be incumbent upon ethicists, computer scientists, policymakers, and others to learn to work in interdisciplinary capacities in order to make greater sense of and manage these important new capacities and the values and ethical concerns connected to them. As such, it is highly important that philosophers be able to clearly articulate the distinct epistemic, moral, and pragmatic reasons on the moral ledger and that they be able to consider how these various considerations relate and trade off against one another without conflating them.

p. 649 Furthermore, philosophers and scholars ought to refrain from the knee-jerk impulse to oversimplify our current predicament into over-simplified narratives of certain technological utopia or certain technological Armageddon. Rather, we would be best served if we were to pause for a moment, re-investigate, and re-articulate the values and moral reasons we actually care about, and then begin to shape out institutions and technologies towards such ends. And while the brave new world we are fast moving into seems at times alien, disorienting, and utterly overwhelming, we can at least find solace in the idea that philosophers have been struggling over these very same core questions of humanity's relationship to technology for millennia, and that, in a sense, there is 'nothing new under the sun'.

Notes

[1] Steve Kershnar likewise rejects the notion that AWS create any new or novel moral problems.

[2] They may both equally be able to pass the Turing test, for instance.

[3] There is, however, a third option here, the view that human decision-making is perfectly mechanical/naturalistic (e.g. there is some logical impossibility in usual descriptions of strong AI but that machines can nonetheless be 'fully autonomous' on analogy with humans, since humans also are not *really* strongly intelligent but are 'fully autonomous' in some deflationary sense).

[4] Note, however, that many of the same people who vehemently oppose the idea of autonomous weapons, do not offer nearly the same degree of protest when it comes to related technologies such as driverless cars or automated medical-resource allocation software. This sharp divergence in response might then reveal that peoples' moral intuitions are really tracking the moral distinction between doing and allowing versus a unique moral problem with automation as such.

[5] However, they grant that this argument is not necessarily an all-things-considered argument against the use of AWS.

[6] The reader should note that within just war theory literature, there have been various explanations as to the normative grounding for the MEC. Some philosophers argue that the MEC derives from the metaphysically exceptional domain of 'war' (Walzer 1977). Other philosophers reject the idea that 'war' is a special moral domain, but nonetheless argue that there are good contractualist reasons (Benbaji 2008) or rule-consequentialist reasons (Shue 2008; McMahan 2009) for nation-states to restrain their soldiers' actions in accordance with an MEC convention.

[7] While this might not be a novel metaphysical problem, there are certainly practical problems with collective action. For instance, we have been notoriously bad at collective global coordination tackling climate change. Collective action problems often call for negotiation and compromises that are hard to achieve. Furthermore, there is also a diffusion of causal, moral, and epistemic responsibility across collective and institutional actions such that no one feels responsible for climate change. Conversely, it is easier for one person in charge of a nuclear bomb to exercise their conscience if they know they will be the sole person responsible for millions of deaths, than for a thousand people working on an AWS to feel the same responsibility and act accordingly. This might not be an in principle ↳ philosophical problem, but it is a very concerning practical problem warranting institutional reform and creation. p. 650

[8] This view would then be somewhat akin to a bizarre version of John Searle's biological chauvinism or Ruth Millikan's teleo-functionalist view, only with silicon micro-chips being the metaphysically privileged substrate capable of realizing consciousness instead of human biology.

[9] This solution also takes care of language that tacitly suggests the existence of a responsibility gap; language like 'off the loop' and lacking 'meaningful human control'. Granted, an 'accountability gap' might still be metaphysically possible, but not a responsibility gap.

[10] This would, however, make the AWS a genuine moral agent and would entail that it is a moral patient and thereby also a bearer of rights, or at least interests. This would then arguably make it morally problematic to turn off such entities or make them fight our wars for us.

References

Benbaji, Yitzhak (2008), ‘A Defense of the Traditional War Convention’, *Ethics* Vol. 118, No. 3, Symposium on Agency, 464–495.
Google Scholar WorldCat

Block, Ned (1978), ‘Troubles with Functionalism’, *Minnesota Studies in The Philosophy of Science* (9), 261–325.
Google Scholar WorldCat

Bostrom, Nick (2003), ‘Cognitive, Emotive and Ethical Aspects of Decision Making in Humans and in Artificial Intelligence’, *International Institute of Advanced Studies in Systems Research and Cybernetics* 2, 12–17.
Google Scholar WorldCat

Burri, Suzanne (2017), ‘What is the Problem with Killer Robots?’, in Ryan Jenkins, Michael Robillard, and Bradley Jay Strawser, eds, *Who Should Die: Liability and Killing in War* (Oxford: Oxford University Press), 163–187.
Google Scholar Google Preview WorldCat COPAC

Burri, Suzanne and Robillard, Michael (2018), ‘Why Banning Killer Robots Wouldn’t Solve Anything’, *Aeon*, https://aeon.co/ideas/why-banning-autonomous-killer-robots-wouldnt-solve-anything, accessed 8 October 2021.
WorldCat

De Greef, T.E., Arciszewski, H.F., and Neerincx, M.A. (2010), ‘Adaptive Automation Based on an Object-Oriented Task Model: Implementation and Evaluation in a Realistic C2 environment’, *Journal of Cognitive Engineering and Decision Making* 4(2), 152–182.
Google Scholar WorldCat

Farivar, Cyrus (2015), ‘Darkweb Drug-Buying Bot Returned to Swiss Artists after Police Seizure’, *Arstechnica*, 15 April, https://arstechnica.com/tech-policy/2015/04/dark-web-drug-buying-bot-returned-to-swiss-artists-after-police-seizure/, accessed 8 October 2021.
WorldCat

Fodor, Jerry A. (1983), *The Modularity of Mind* (Boston, MA: MIT Press).
Google Scholar Google Preview WorldCat COPAC

Frowe, Helen (2018), *The Oxford Handbook on the Ethics of War* (Oxford: Oxford University Press).
Google Scholar Google Preview WorldCat COPAC

Lucas, John R. (1961), ‘Minds, Machines, and Gödel’, *Philosophy* XXXVI, 112–127.
Google Scholar WorldCat

McMahan, Jeff (2009), *Killing in War* (Oxford: Oxford University Press).
Google Scholar Google Preview WorldCat COPAC

Miles, Kathleen (2014), ‘Artificial Intelligence May Doom the Human Race within a Century’, *Huffington Post*, https://www.jstor.org/stable/3749270, accessed 8 October 2021.
WorldCat

Purves, Duncan, Jenkins, Ryan, and Strawser, Bradley Jay (2015), ‘Autonomous Machines, Moral Judgment, and Acting for the Right Reasons’, *Ethical Theory and Moral Practice* 18, 851–872.
Google Scholar WorldCat

Robillard, Michael (2018a), ‘No Such Thing as Killer Robots’, *Journal of Applied Ethics* 35(4), 705–716.
Google Scholar WorldCat

p. 651 Roff, Heather M. (2014), ‘The Strategic Robot Problem: Lethal Autonomous Weapons in War’, *Journal of Military Ethics* (3), 211–

227.
Google Scholar WorldCat

Scharre, Paul (2018), *Army of None: Autonomous Weapons and the Future of War* (New York: W.W. Norton and Company).
Google Scholar Google Preview WorldCat COPAC

Scharre, Paul and Horowitz, Michael (2018), 'An Introduction to Autonomy in Weapon Systems', http://www.cnas.org/intro-to-autonomy-in-weapon-systems, accessed 8 October 2021.
WorldCat

Searle, John (1980), 'Minds, Brains, and Programs', *Behavioural and Brain Sciences* 3, 417–424.
Google Scholar WorldCat

Sharkey, Noel, ed. (2017), 'The Campaign to Stop Killer Robots', http://www.stopkillerrobots.org, accessed 8 October 2021.
WorldCat

Shue, H. (2008), 'Do We Need a "Morality of War"', in David Rodin and Henry Shue, eds, *Just and Unjust Warriors: The Moral and Legal Status of Soldiers* (New York: Oxford University Press), 87–111.
Google Scholar Google Preview WorldCat COPAC

Simpson, Thomas W. (2011), 'Robots, Trust and War', *Philosophy of Technology* 24, 325–337.
Google Scholar WorldCat

Skerker, Michael, Jenkins, Ryan, and Purves, Duncan (2020), 'AWS, Respect, and the Moral Equality of Combatants', *Ethics and Information Technology* 22(3), 197–209.
Google Scholar WorldCat

Sparrow Rob (2007), 'Killer Robots', *Journal of Applied Philosophy* 24(1), 65.
Google Scholar WorldCat

Sparrow, Rob (2016), 'Robots and Respect', *Ethics and International Affairs* 30(1), 93–116.
Google Scholar WorldCat

Strawser, Bradley Jay (2010), 'Moral Predators: The Duty to Employ Uninhabited Aerial Vehicles', *Journal of Military Ethics* 9(4), 342–368.
Google Scholar WorldCat

US Department of Defense (2012), 'Directive Number 3000.09 on Autonomy in Weapon Systems', http://www.dtic.mil/whs/directives/corres/pdf/300009p.pdf, accessed 8 October 2021.
WorldCat

p. 652 Walzer, Michael (1977), *Just and Unjust Wars: A Moral Argument with Historical Illustrations* (New York: Basic Books). ↳
Google Scholar Google Preview WorldCat COPAC