IN CORPORATE WE TRUST: THE RELUCTANT POWERS OF THE CIVILIAN TECH SECTOR AROUND AUTONOMOUS WEAPONS SYSTEMS

By Nikitha Margaret Vincent

Submitted to

Central European University Department of International Relations

In partial fulfilment of the requirements for the degree of Master of Arts in International Relations

Supervisor: Paul Roe

Vienna, Austria, 2023

Abstract

In 2020, Boston Dynamics commercially released 'Spot', a mobile robot with autonomous capabilities. To no one's surprise, many people were left unnerved by the uncanny semblance the bot bore to the ruthless, ever-evolving killer robot from the Black Mirror episode "Metalhead".

The civilian tech sector today is responsible for most of the cutting-edge developments in the field of autonomy and this is expected given that they build the AI that underpins autonomous systems. Yet there is a gap in literature exploring the civilian tech sector through the lens of power. Based on the work of Nik Hynek and Anzhelika Solovyeva in "Operations of power in autonomous weapons systems: ethical conditions and socio-political prospects" my paper aims to explore the kinds of power the civilian tech sector specifically possesses within the arena of AWS discourse, using the taxonomy of power proposed by Michael Barnett and Raymond Duvall in "Power in International Politics".

Over the course of this paper, to set up the required context and relevance of this discussion, there will also be an exploration of literatures about AWS, a brief review of the conversation on power as exerted by the private sector in security affairs and an exploration of existing work on the civilian tech sector and AWS. My aim with this paper is to engage with and expand upon the existing power literature on the civilian tech sector.

Acknowledgements

In 2019 I left Dubai for Budapest with packed bags and the brightest smile in a three-mile radius. The ensuing few years turned out to be almost nothing like I had hoped, and a global pandemic and broken bones unfortunately formed only part of the story. Mostly, the last years have been testing, not just to me, but to the patience of everyone who ever had faith in me. It has been a chaotic run and I have nothing but eternal gratitude and admiration for the people who have stayed and watched me stumble, roll and crash ungracefully into the finish line but still greet me warmly.

My special thank you-s to:

Zlata, who has responded to every frustrating email of mine with a solution for four years.

Professor Roe, who has been the closest thing to a guardian angel during my degree, bringing clarity to every rambling idea I've had and forgiveness to every failing of mine as a student.

Professor Fetzer, who gave me one last chance to get here.

Sara, who has been my strength and the sole witness of this entire journey.

Adam, Anna, Ushmayo and Sophiko whom I miss very much and are the reason I got through the first half of my degree.

My family, who just want to see me smile.

And God

Table of Contents

Introduction

> "Lethal autonomous weapons threaten to become the third revolution in warfare…We do not have long to act. Once this Pandora's box is opened, it will be hard to close."[1]

In 2017, a group of over a hundred private sector leaders in artificial intelligence (AI) and robotics including Elon Musk co-signed an Open Letter to the Convention on Certain Conventional Weapons (CCW) with the Future of Life Institute (FLI). It welcomed the creation of a Group of Governmental Experts (GGE) on Lethal Autonomous Weapon Systems (LAWS)[2] at the CCW while taking a cautionary tone towards LAWS development. The move to include such co-signatories is not just a result of their growing public influence[3] but also connected to their position as stakeholders in the conversation on AWS, since they create the AI[4] that is crucial to the development of AWS. This suggests that the civilian tech sector possesses a certain degree of influence and even power in the global conversation on the development of AWS today.

My paper aims to explore the kinds of power the civilian tech sector possesses within the arena of AWS discourse and development, by using the taxonomy of power proposed by

---

[1] Future of Life Institute. 'An Open Letter to the United Nations Convention on Certain Conventional Weapons'. August 20th, 2017. Accessed November 25th, 2021. Available at: https://futureoflife.org/open-letter/autonomous-weapons-open-letter-2017/.

[2] The definition of LAWS used in this paper corresponds to the one put forward by Paul Scharre and Michael Horowitz in "An Introduction to Autonomy in Weapon Systems" in 2015, which defines AWS as "[A] weapon system that, once activated, is intended to select and engage targets where a human has not decided those specific targets are to be engaged", with the specification in this case of an ability to engage in lethal attacks.

[3] Allison Morrow. 'Elon Musk Tweet Fuels Frenzied GameStop Surge'. *CNN*. January 27, 2021. Accessed November 25th, 2021. Available at: https://edition.cnn.com/2021/01/26/investing/gamestop-stock-elon-musk-reddit/index.html.

[4] Jayshree Pandya. 'The Dual-Use Dilemma of Artificial Intelligence'. *Forbes*. January 7th, 2019. Accessed November 25th, 2021. Available at: https://www.forbes.com/sites/cognitiveworld/2019/01/07/the-dual-use-dilemma-of-artificial-intelligence/?sh=4ead7e8a6cf0

Michael Barnett and Raymond Duvall in "Power in International Politics".[5] Over the course of this work, to set up the underlying context and relevance of this discussion, there will be an exploration of literature about AWS and whether, if any, inherent effects on power and the nature of society this new technology possesses. This is followed by a brief review of the conversation on power as exerted by the private sector in the field of security and military studies, after which I establish the theoretical base and relevance of discussing the civilian private tech sector today, and why with specific regards to AWS. Following this is an exploration of existing work on the civilian tech sector and AWS through the lens of power, and my responses and addition to this body which simultaneously engage with Barnett and Duvall's power taxonomy.

Literature Review: What's the Word on AWS so far?

Since the focus of this research paper is to look at the private sector's effects on AWS through a lens of power, it is also crucial to situate this work among literature that concerns the human and system structures surrounding AWS. The purpose of this is to trace how much of the literature implies a mutually constitutive element of control inherent to the nature of AWS. Literatures discussing these sensibilities include themes of whether AWS will fundamentally alter existing norms and how humans think about killing (or if we think at all) in the section "*Are Autonomous Weapons Systems Changing how we make Decisions?*", AWS' effect on global strategy in the section "*What changes in a War?*", the suggestion that AWS is the next

---

[5] Michael Barnett and Raymond Duvall. 'Power in International Politics.' *International Organization* 59, no. 1 (2005): 39-75

revolution in warfare[6] in the section "*Is AWS the next RMA?*" and counter to the other themes in the section "*Man, and Machine as Employed*" AWS is better understood as an agent employed within the current paradigm.

However, it would be remiss to ignore the central question plaguing academic and policy literature on AWS, which is whether AWS is legally (and by implication in many readings, 'morally') appropriate to deploy at all. Substantial portions of existing literature are dedicated to constructing arguments for and against AWS, sometimes centering the public consensus on AWS through the Martens Clause. This debate will be explored briefly in "*Should we Abort Mission?*" ahead of the themes about AWS' effects on human and strategic control.

Should we Abort Mission?

As mentioned earlier, though limited in discussion within this paper, several authors have written at great lengths in favor of or against AWS, but the conversation on deploying AWS is not the concern of policymakers[7] or researchers alone.

Early in 2021, research firm Ipsos in their 28-country survey of civilians found that 61% of adults surveyed opposed the use of fully autonomous weapons.[8] While the moral conviction that machines should not be allowed to kill humans formed the top reason for opposition, the

---

[6] Kai-Fu Lee. 'The Third Revolution in Warfare'. *The Atlantic*. September 11th, 2021. Accessed June 2nd, 2023. Available at: https://www.theatlantic.com/technology/archive/2021/09/i-weapons-are-third-revolution-warfare/620013/.

[7] Gabriele Giordano Caccia. "Joint Statement on Lethal Autonomous Weapons Systems First Committee, 77th United Nations General Assembly Thematic Debate – Conventional Weapons". *United Nations*. October 21st, 2022. Accessed April 3rd, 2023. Available at: https://estatements.unmeetings.org/estatements/11.0010/20221021/A1jJ8bNfWGlL/KLw9WYcSnnAm_en.pdf.

[8] Ipsos. 'Global Survey Highlights Continued Opposition to Fully Autonomous Weapons'. *Ipsos*. February 22nd, 2021. Accessed 30th May 2023. Available at: https://www.ipsos.com/en-us/global-survey-highlights-continued-opposition-fully-autonomous-weapons.

next most common reason was these machines would be "unaccountable".[9] Baobao Zhang et al.'s 2019 survey of AI/ML researchers in 2019, found that a majority of researchers opposed working on LAWS[10] and in a 2013 survey by Charli Carpenter it was found that 50% of American citizens surveyed were opposed to AWS.[11] Results like this are important because they indicate what direction law around AWS could take on the basis of principles such as the Martens Clause.[12]

In the academic sphere it is also clear that there is strong opposition to the deployment of LAWS on a number of grounds. The most cited reasons are the inability of LAWS to abide by principles such as distinction, proportionality and necessity which underpin International Humanitarian Law (IHL) and *jus in bello* doctrine. Robert Sparrow in "Robots and Respect: Assessing the Case Against Autonomous Weapon Systems" argues in favor of banning LAWS due to their inability to respect the "humanity of our enemies, which underlies the principles of *jus in bello* with focus on the principles of distinction and proportionality,[13] while warning against an excess of reliance on consequentialist ethics.[14] The work of Denise Garcia also warns strongly against AWS based on their potentially destabilizing effects on "Humanitarian Security Regimes".[15] Authors such as Elvira Rosert and Frank Sauer on the

---

[9] Ibid.

[10] Baobao Zhang et al. 'Ethics and governance of artificial intelligence: Evidence from a survey of machine learning researchers'. *Journal of Artificial Intelligence Research 71* (2021): 591-666.

[11] Charli Carpenter. 'How do Americans feel about Fully Autonomous Weapons?' *The Duck of Minerva*. June 19th, 2013. Accessed 25th May 2023. Available at: https://www.duckofminerva.com/2013/06/how-do-americans-feel-about-fully-autonomous-weapons.html.

[12] Michael C. Horowitz. 'Public opinion and the politics of the killer robots debate'. *Research & Politics* 3, no. 1 (2016): 1-8. DOI: https://doi.org/10.1177/2053168015627183.

[13] Robert Sparrow. 'Robots and Respect: Assessing the Case Against Autonomous Weapon Systems'. *Ethics & International Affairs* 30, no. 1 (2016): 110-111. DOI: 10.1017/S0892679415000647.

[14] Ibid., 100-101.

[15] Denise Garcia. 'Lethal Artificial Intelligence and Change: The Future of International Peace and Security'. *International Studies Review* 20, no. 2 (2018): 336-338. DOI: https://doi.org/10.1093/isr/viy029.

other strongly recommend against AWS based on the preservation of human dignity[16] while acknowledging that citing the principle of distinction, for example, may not always hold as valid criticism of AWS, especially if the softwares guiding targeting evolve to be better.[17]

However, while it is tempting to conclude that AWS is primed for a moratorium based on surveys,[18] the global visibility of coalition campaigns such as the Campaign to Stop Killer Robots[19] and the work of the Future Life Institute[20] and several researchers, opinions and conclusions on AWS are more diverse in the civilian sphere and may even be shifting. Public opinion on AWS in fact often seems to vary based on the justification and context of its usage. In 2016, in contrast to Carpenter's findings,[21] Michael Horowitz in "Public opinion and the politics of the killer robots debate" found that 61% of US citizens in a survey were willing to support AWS usage if it proved the most effective way of protecting US troops.[22] And there were significant increases in support for AWS development if "military necessity" or "foreign development" were cited.[23] Koki Arai and Masakazu Matsumoto in "Public perceptions of autonomous lethal weapons systems" also found their Japanese survey respondents largely willing to use AWS in 2023, with most of that share agreeing in light of the consideration that AWS could reduce civilian casualties.[24]

---

[16] Elvira Rosert and Frank Sauer. 'Prohibiting Autonomous Weapons: Put Human Dignity First'. *Global Policy* 10, no. 3 (2019): 372-373. DOI: https://doi.org/10.1111/1758-5899.12691.
[17] Ibid., 370-371.
[18] OHCHR. *A call for a moratorium on the development and use of lethal autonomous robots*. May 31st, 2013. Accessed May 19th, 2023. Available at: https://www.ohchr.org/en/stories/2013/05/call-moratorium-development-and-use-lethal-autonomous-robots.
[19] Stop Killer Robots. Accessed June 1st, 2023. Available at: https://www.stopkillerrobots.org/about-us/.
[20] Future of Life Institute. *FLI Open Letters*. Accessed May 20th, 2023. Available at: https://futureoflife.org/fli-open-letters/.
[21] Carpenter, 'How do Americans feel about Fully Autonomous Weapons?'
[22] Horowitz, 'Public opinion and the politics of the killer robots debate', 4.
[23] Ibid., 6.
[24] Koki Arai and Masakazu Matsumoto. 'Public perceptions of autonomous lethal weapons systems'. *AI and Ethics* (2023): 6. DOI: https://doi.org/10.1007/s43681-023-00282-9.

Similarly, there is also research that supports the use of AWS. Notably opposed by authors in the ban camp is the work of Ronald Arkin, who in "The Case for Ethical Autonomy in Unmanned Systems" argues that even trained humans, by nature, are unlikely to be able to adhere to the laws of warfare on the battlefield[25] and highlights potential merits autonomous systems could bring including their lack of need for self-preservation and ability to avoid emotional or biased judgement in the presence of rapidly changing information.[26] Anton Petrenko in "Between Berserksgang and the Autonomous Weapons Systems" addresses several arguments against AWS and concludes that using AWS may not just be a matter of efficiency but a moral prerogative if it saves the lives of forces[27] and suggests that accountability is "not a requirement for the moral permissibility of an action".[28] Michael Newton while less ardently in support of AWS suggests that AWS may in fact be better capable of adhering to the laws of war by "eliminating information barriers and ensuring instantaneous adjustment of tactics across linguistic or cultural boundaries" while improving military effectiveness.[29]

Are Autonomous Weapons Systems Changing how we make Decisions?

Ingvild Bode and Hendrik Huelss in their 2018 paper "Autonomous weapons systems and changing norms in international relations" propose that there can be a degree of normatively justified development and deployment of arms that occurs before the legal and public

---

[25] Ronald C. Arkin. 'The Case for Ethical Autonomy in Unmanned Systems'. *Journal of Military Ethics* 9, no. 4 (2010): 338. DOI: 10.1080/15027570.2010.536402.
[26] Ibid., 333.
[27] Anton Petrenko. 'Between Berserksgang and the Autonomous Weapons Systems.' *Public Affairs Quarterly* 26, no. 2 (2012): 86.
[28] Ibid., 89.
[29] Michael A. Newton. 'Back to the Future: Reflections on the Advent of Autonomous Weapons Systems.' *Case Western Reserve Journal of International Law* 47, no.1 (2015): 18.

codification of their moral appropriateness.[30] In Bode and Huelss' work, 'procedural norms' distinctly refer to norms imbued with "considerations of appropriateness in specific organizational settings, such as the armed forces".[31] Such values can include efficiency or competitive advantage. In parallel exist "fundamental norms" whose primary concern is with what is legally and publicly accepted, and to some degree what can be construed by consensus, as ethical. While Bode and Huelss' work suggests that both procedural and fundamental norms function on equal footing and akin to a feedback loop, it is also clear that procedural norming as they explore it, largely tends to takeover and change outcomes in the time that fundamental-ethical discourse about a topic is ongoing or unconcluded. A similar phenomenon in visible in Nina Tannenwald's explorations of the origin of the nuclear non-proliferation phenomenon in "Stigmatizing The Bomb: Origins of the Nuclear Taboo", where even after widespread global condemnation and grassroot level protests against atomic bombs and nuclear weapons testing, the US Government decided to return to relying on nuclear weapons as part of their defense strategy.[32] The Eisenhower government intentionally set out to portray atomic weapons as conventional and ordinary, while more nuclear weapons were steadily integrated after the Korean war. The US military adopted this policy as a result of wanting the nuclear deterrence threat to be more pronounced, in addition to the proposed cost effectiveness of tactical nuclear weapons.[33] Thus it was visible, that values more in line with procedural norms (as Bode and Huelss' define it)[34] such as cost effectivity promoted the continued development and procurement of nuclear weapons while the fundamental norm

---

[30] Ingvild Bode and Hendrik Huelss. 'Autonomous Weapons Systems and Changing Norms in International Relations.' *Review of International Studies* 44, no. 3 (2018): 393–413. DOI: 10.1017/S0260210517000614.

[31] Ibid., 409.

[32] Nina Tannenwald. 'Stigmatizing the Bomb: Origins of the Nuclear Taboo.' *International Security* 29, no. 4 (2005): 5–49.

[33] Ibid., 23-24.

[34] Bode and Huelss, 'Autonomous Weapons Systems and Changing Norms in International Relations.'

surrounding its non-use (as it exists today) was forming. Bode and Huelss argue that this phenomenon is primed to occur within the arena of AWS, where besides for cost factors,[35] AWS on fully autonomous modes could also process more information and make decisions quicker than humans[36] redefining what it means to possess more speed than the enemy. This concern about whether AWS development challenges the normative framework to favor itself or whether AWS perhaps possesses a 'constitutive quality'[37] when it comes to norms and decision-making continues to be a major concern for several authors in the literature, the bases of which will be expanded upon in the remaining portion of this section.

In touching on the procedural norm of competitive advantages, the work of Kalpouzos in "Double elevation: Autonomous weapons and the search for an irreducible law of war" also comes to mind, where they explore the role AWS may come to play in humanity's longstanding relationship with progress, as enabled by technology.[38] Kalpouzos suggests that humans have a need to both, firstly, elevate themselves above their enemies and secondly, elevate them above themselves. They usually pursue this with the conviction that mechanized judgement is more rational and thereby pushes the envelope on human improvement, in addition to covering for their failings.[39] Kalpouzos comes to rest on the notion that this is a futile, and potentially ill-advised endeavor because they suggest that algorithmic or machine intelligence will always be once, if not further, reduced from the situated knowledges of humans and the law.[40] This conversation is worth highlighting however, because it originates

---

[35] Ibid., 410.

[36] Ibid., 410.

[37] Hendrik Huelss. 'Norms Are What Machines Make of Them: Autonomous Weapons Systems and the Normative Implications of Human-Machine Interactions'. *International Political Sociology* 14, no. 2 (2020): 3. DOI: https://doi.org/10.1093/ips/olz023.

[38] Ioannis Kalpouzos. 'Double Elevation: Autonomous Weapons and the Search for an Irreducible Law of War'. *Leiden Journal of International Law* 33, no. 2 (2020): 289-312.

[39] Ibid., 291, 297 and 301.

[40] Ibid., 309-311.

from the unusual concern surrounding AWS which is that it could possess an intelligence that humans may come to trust more than their own. AWS in such an understanding is capable not simply of altering norms by changing our understanding of what is possible or convenient, it is very well capable of replacing human decision making on the battlefield with the explicit consent of its creators.

Hendrik Huelss takes a different approach exploring how AWS can come to alter our decisions not so much by replacing us as the final decision-making agents, but by shaping our understandings of normality, and thereby constituting the fabric of our decision-making schema.[41] Huelss takes conceptual roots from the ideas of Foucault who differentiates between the 'apparatus of discipline' and the 'apparatus of security'. The former is the phenomenon of using discipline and action to bring reality in line with norms that originate after deliberation and discourse. These norms do not need to be based on existing conceptions of normal and abnormal, but rather a desired outcome. With the apparatus of security, that which constitutes the statistical distribution of the normal in a setting, is observed and confirmed, and this understanding of the normal (and what is abnormal in relation) then informs the norms to be followed. Based on this, anomalies are dealt with in the manner deemed appropriate.[42] Huelss talks about the case of the SKYNET system deployed in Pakistan which observed the movement of several millions of phone users and started forming an understanding of what is normal or likely, thus, constructing the "normality" of movement in Pakistan for us. Once the 'normal' was established, people who displayed abnormal movement patterns became potential targets for drone attacks. The targets and

---

[41] Huelss, 'Norms Are What Machines Make of Them.'
[42] Ibid., 8-9.

conditions meriting the use of force in this case, are thus determined by the security apparatus and the normal it creates for us.[43] Huelss also emphasizes that the level of sophistication of the systems, or the parameters of autonomy in AWS, do not affect whether AWS shapes our normality, since even autonomous systems used for reconnaissance can alter our understandings of reality (as exemplified by SKYNET).[44]

There is an important conversation to be pursued on the basis of whether the intelligence possessed by AWS would be enough to classify them as a new form of being that deserve rights outside of their use to us. Authors such as Kate Devitt in "Normative Epistemology for Lethal Autonomous Weapons Systems" explore mechanisms of epistemology that might apply to AWS and comes to conclude that encoding a Bayesian Virtue Epistemology could potentially enable AWS to share in the human capability for reflexive thinking and ethically bound judgements (though likely still subject to channels of human control).[45] Heather Roff in "The Strategic Robot Problem: Lethal Autonomous Weapons in War" explores the status of robots as agents who must think strategically themselves.[46] Roff unpacks the decision-making systems and levels that commanders and combatants must go through before deciding on a target, including filtering them through the lens of distinction and then the necessity of attack.[47] The author comes to rest on the understanding that many militaries would prefer to allow AWS to "create and update their own lists once fielded" on account of operational speeds and reducing the inconvenience of back-and-forth communications but

---

[43] Ibid., 12.
[44] Ibid., 5.
[45] Kate S. Devitt. 'Normative Epistemology for Lethal Autonomous Weapons Systems'. In *Lethal Autonomous Weapons: Re-Examining the Law and Ethics of Robotic Warfare*. Eds. Jai Galliott, Duncan MacIntosh and Jens David Ohlin, 237-258. Oxford University Press, 2021. DOI: 10.1093/oso/9780197546048.003.0016.
[46] Heather M. Roff. 'The Strategic Robot Problem: Lethal Autonomous Weapons in War.' *Journal of Military Ethics* 13, no. 3 (2014): 211-227. DOI: 10.1080/15027570.2014.975010.
[47] Ibid., 215-216.

remains skeptical of employing a combatant who is also a commander.[48] Given that most commanders themselves make decisions plugged into a large network of informational updates and political understandings[49] however, it would be fair to consider that one of the ways AWS is employed in any tactical (or higher-level strategic capacity) could be such that they receive the same information and redline understandings that commanders do, thus potentially making the case that commanders may not be any more qualified than the AWS system when it comes to battlefield decisions.

However, most authors including Devitt and Roff acknowledge that AWS as they exist have not achieved this level of complexity, and implicitly seem to suggest that based on future testing and a deeper understanding of AWS, this may never even come to pass.

What changes in a War?

Moving away from debates on the nature of how AWS may alter human decision-making and norms lie debates about whether AWS will fundamentally alter strategy in times of conflict or the likelihood of conflict in light of the novelty and competitive advantages they bring. And as the authors in this section acknowledge, the civilian sector both facilitates and responds to these strategic changes.

Jurgen Altmann and Frank Sauer in "Autonomous Weapons Systems and Strategic Stability" discuss the effect that the proliferation of AWS could have on global security.[50] The authors see this proliferation as potentially accelerated by the dual-use nature of the AI that AWS is

---

[48] Ibid., 219-221.
[49] Ibid., 217.
[50] Jürgen Altmann and Frank Sauer. 'Autonomous Weapon Systems and Strategic Stability'. *Survival* 59, no.5 (2017): 117-142. DOI: 10.1080/00396338.2017.1375263.

built upon and its connection to the civilian sector.[51] This view is also in line with the research of Vincent Boulanin and Maaike Verbruggen who find that the civilian sphere is much quicker with respect to the development of AI technologies since they are subject to more competition but also less engineering challenges than the defense sector's research.[52] Altmann and Sauer posit that in this accelerated scenario, global security will be impacted along the lines of arms race and proliferation instability and crisis instability and escalation.[53] In the case of the former, horizontal and vertical proliferation of AWS can exacerbate the security dilemma between states at a risk of conflict. In the case of the latter, the reaction speeds that AWS are capable of, means that the escalation from war to peace or escalation of the combat forms during war time can hang on a very thin rope. Altmann and Sauer suggest that the solution to the potential rise of global security dilemmas is "regulating or prohibiting a defined military practice" or applications of technology to such ends, rather than prohibiting the technology itself.[54] Although this might not in practice seem very different from calls for the usage and deployment of AWS only after extensive testing and risk assessment, scholars in the vein of Altmann and Sauer seem skeptical about the possibility of comprehensive testing in a meaningful sense for military application at all, leading to the adoption of a strongly cautious approach towards AWS.[55]

In "When Speed Kills: Lethal autonomous weapon systems, deterrence and stability" Horowitz, while taking care to differentiate between arms races and proliferation,[56] discusses

---

[51] Ibid.

[52] Vincent Boulanin and Maaike Verbruggen. *Mapping the Development of Autonomy in Weapon Systems*. 125, 106-108. SIPRI, 2017. DOI: 10.13140/RG.2.2.22719.41127.

[53] Altmann and Sauer, 'Autonomous Weapon Systems and Strategic Stability'.

[54] Ibid., 133.

[55] Ibid.

[56] Michael C. Horowitz. 'When speed kills: Lethal autonomous weapon systems, deterrence and stability'. *Journal of Strategic Studies* 42, no.6 (2019): 776. DOI: 10.1080/01402390.2019.1621174

how an implicit demand, lowered costs and uncertainty about the weapons capability of other global actors may also motivate states to acquire arms even during times of peace, as was exemplified by the global increase in acquisition of tanks from the 1920s to the 1930s despite the lack of premonition about a war. Horowitz also acknowledges that the civilian sector's developments in AI could contribute to AWS proliferation.[57] Crucially, Horowitz highlights that the uncertainty surrounding the speed and capabilities of AWS creates a new force of pressure in the balance of strategic stability, recalling how the fear surrounding the automated nature of the Soviet Union's Dead Hand system incentivized unstable military positions during the Cold War.[58] Nonetheless, Horowitz acknowledges that while AWS can affect strategic stability, these effects are not so pronounced as to cause wars to spiral out of human control.

Is AWS the next RMA?

Strongly intertwined with the conversation on AWS potentially altering strategic stability is the debate on whether it is the next major revolution in military affairs (RMA). Kai-Fu Lee in their book "AI 2041: Ten Visions for Our Future" recently referred to AWS as being the potential third revolution in warfare after gunpowder and nuclear arms.[59] And while several authors consider AWS as being an integral part of a new RMA, opinions vary as to whether AWS is a third RMA, part of a larger information revolution or simply brings a revolution of its own. Patrick Morgan's understanding of an RMA is useful within the context of this literature.[60] Morgan suggests that an RMA contains elements of new technologies, an

---

[57] Ibid., 777 – 779.
[58] Ibid., 782.
[59] Lee, 'The Third Revolution in Warfare'.
[60] Patrick M. Morgan. 'The impact of the revolution in military affairs'. *Journal of Strategic Studies* 23, no.1 (2000): 132-162. DOI: 10.1080/01402390008437781.

accompanying shift in organizational and social arrangements and "a new strategic approach to the use of force".[61] And while their work predates the current sensibility surrounding AWS, Morgan was nonetheless tackling the matter of 'smart weapons' and how they fit into a broader "information" revolution that was changing how we do warfare.[62] Taking the view that such revolutions often take several decades to unfold, Morgan proposed that the current revolution including things such as smart weapons was in its first decade of five in the 2000s.[63] Given the estimated span one should presume it is still about thirty years too early to have the benefit of hindsight on confirming the RMA. Nonetheless, Morgan came to view that the current revolution would technologically change things by placing information processing and surveillance at the center of operations,[64] socially and organizationally by moving command structures towards decentralized modes of operation[65] and strategically by shifting the balance towards defensive and disruptive conflict styles.[66] Kenneth Payne in "Artificial Intelligence: A Revolution in Strategic Affairs?" draws parallels and distinctions between nuclear weapons and AI-based weapons and suggests that AI brings a much bigger revolution in strategic terms than nuclear weapons did.[67] Pertinent to this paper is Payne's consideration that part of the AI revolution's restructuring of society is the way the dual-use nature of AI[68] and its development by the corporate sector may distribute a disproportionate amount of power in their hands.[69] Payne also discusses the strategic impacts of AI from

---

[61] Ibid., 135.
[62] Ibid., 134.
[63] Ibid., 135.
[64] Ibid., 136.
[65] Ibid., 138.
[66] Ibid., 139.
[67] Kenneth Payne. 'Artificial Intelligence: A Revolution in Strategic Affairs?' *Survival* 60, no. 5 (2018): 7-32. DOI: 10.1080/00396338.2018.1518374.
[68] Ibid., 16.
[69] Ibid., 20.

shifting power balances to the potential chance of moving conflicts in the offensive direction.[70] Although Payne's opinion on the offensive versus defensive lean of AI-enabled weapons runs diametrically opposite to that of Morgan, their consideration on the strategic and social implications of AI fit the parameters of an RMA according to Morgan. Jacquelyn Schneider and Julia Macdonald in "Looking back to look forward: Autonomous systems, military revolutions, and the importance of cost" on the other hand make a distinction between RMAs and military revolutions with RMAs being more limited in scope to warfare and its operational characteristics, and military revolutions embodying more of the socio-organizational and strategic changes that authors such as Morgan view as part of an RMA.[71] However, Schneider and Macdonald suggest that focusing on characteristics such as the precision, range and speed of AWS may paint an inflated picture about its revolutionary effects.[72] They suggest rather, that based on historical review, new technologies are likelier to herald a military revolution depending on how much they can reduce political and economic costs.[73] The authors, however, do not reach a conclusion on whether AWS will trigger a revolution, because while they put forth several arguments for the conditions under which AWS could reduce costs, they also acknowledge that the pursuit of survivability might turn AWS into a politically costly option.[74]

---

[70] Ibid., 23-26.
[71] Jacquelyn Schneider and Julia Macdonald. 'Looking back to look forward: Autonomous systems, military revolutions, and the importance of cost'. *Journal of Strategic Studies* (2023): 5. DOI: 10.1080/01402390.2022.2164570.
[72] Ibid., 13.
[73] Ibid., 6.
[74] Ibid., 17-18.

Man, and Machine as Employed

In contrast to many of the previous standpoints, another portion of discourse on AWS maintains that while the adoption of AWS may introduce more complex factors when it comes to decision-making, AWS still fits within existing paradigms and does not fundamentally challenge our humanity or ability to control the battlefield. Such writing includes Kevin Schieman's "The Soldier's Share: Considering Narrow Responsibility for Lethal Autonomous Weapons"[75] and Tim McFarland and Jai Galliott in "Understanding AI and Autonomy: Problematizing the Meaningful Human Control Argument against Killer Robots"[76]. Schieman draws on the difference Roff emphasized between the Greek notions of *Autonomos* and *Exousia*. The former refers to the quality of being self-governing as attached to a conception of freedom (which machines are suggested not to possess), while the latter refers to "the power to act, empowerment or authority, authorization or delegation thereof".[77] Autonomous weapons are understood to act in an "exousious" capacity, as Schieman establishes that it is humans who decide how machines are allowed to operate on our behalf.[78] And thus there is a great degree of responsibility those who deploy these weapons (having assessed their risks of failure) bear if they do fail.[79] Schieman emphasizes that several existing "smart" weapons, such as the US Navy's Captor torpedo already embodied characteristics of autonomous knowledges and potential failure that echo the public concern about AWS. Their management gives us frameworks for attributing responsibility, most of

---

[75] Kevin Schieman. 'The Soldier's Share: Considering Narrow Responsibility for Lethal Autonomous Weapons'. *Journal of Military Ethics* 3 (2023): 228-245. DOI: 10.1080/15027570.2023.2166448.

[76] Tim McFarland and Jai Galliott. 'Understanding AI and Autonomy: Problematizing the Meaningful Human Control Argument against Killer Robots'. In *Lethal Autonomous Weapons: Re-Examining the Law and Ethics of Robotic Warfare*. Eds. Jai Galliott, Jens David Ohlin and Duncan MacIntosh. Oxford University Press, 2021. DOI: 10.1093/oso/9780197546048.003.0004.

[77] Heather Roff in Schieman, 'The Soldier's Share', 3-4.

[78] Schieman, 'The Soldier's Share', 14.

[79] Ibid., 9.

which is directed towards the humans in command.[80] In order to set up his case for the nature of distributed responsibility, regardless of the human or mechanical nature of combatants, Schieman explores the case of Steven Green who committed war crimes in a 2005 American deployment to Iraq. He exposes that Green's crimes were not just the result of an individual gone rogue, but crimes enabled as a result of systemic failure in the chain of individuals both commanding and surrounding Green, who despite his diagnosed and evident psychological unfitness, allowed him to continue on active duty.[81] Schieman suggests that much like Green who could not exercise appropriate discrimination while killing due to his mental conditions, the autonomous systems we build may also not be capable of exercising appropriate moral judgement. But in such a case, a large share of responsibility still falls to the military and commanding individuals within it, when they choose to employ AWS after having understood its limitations and risk factors in testing.[82]

McFarland and Galliott argue in a similar vein when they explore the concept of Meaningful Human Control (MHC) that several global actors have called for when it comes to AWS.[83] The authors find that much of the discourse on applying MHC to AWS is based on the erroneous assumption that AWS cannot be accommodated within existing principles of IHL. McFarland and Galliott find that commanders or those who plan attacks are required by IHL to "[t]ake all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects" indicating that if AWS were to be deployed at all, they would

---

[80] Ibid., 11.
[81] Ibid., 5-7.
[82] Ibid., 14.
[83] McFarland and Galliott, 'Understanding AI and Autonomy'.

most likely have to be tested and reviewed in order to ensure their compliance with IHL.[84] Much like Schieman's core argument, these authors also come to rest on the understanding that while AWS may bring runaway failures in a form or scale that we are not accustomed to the fundamental element of human control exists from the testing stages through to any calculated decision to employ these weapons knowing the risks involved.[85] Thus, in these readings AWS is to be treated akin to any other weapons system[86] that carries a risk of failure but does not completely alter the paradigm of human decision-making.

Based on the literature explored so far, while AWS could possess a certain decision-shaping power (if humans consider it superior in some moral, rational or perceptive capacity), outside of the theme of a larger revolution that is more connected to AI than AWS alone, it would seem that the reins of power can largely continue to rest in human hands. Especially if AWS are treated as tools that are selected and/or deployed based on their ability to serve and conform to human needs and interests.

New Power Centers

"The total influence-economic, political, even spiritual-is felt in every city, every state house, every office of the Federal government. We recognize the imperative need for this development. Yet we must not fail to comprehend its grave implications. Our toil, resources and livelihood are all involved; so is the very structure of our society. In the councils of government, we must guard against the acquisition of unwarranted influence, whether sought

---

[84] Ibid., 51.
[85] Ibid., 53.
[86] Ibid., 53.

or unsought, by the military-industrial complex. The potential for the disastrous rise of misplaced power exists and will persist."[87] – Farewell Address, Dwight D. Eisenhower

In a world increasingly populated by AI-enabled technologies from the household to the warzone, where the word "google" has become a verb[88] the words of outgoing US President Eisenhower in 1961 seem almost prophetic. And while the visible and tangible presence of private actors might not necessarily warrant fear as Eisenhower might have implied or understood,[89] understanding the working of private influence is now relevant, not just to understanding power in modern society but specifically in modern global security. As the proliferation of dual-use technologies continues, the companies that provide and produce the services with which we write essays, make video calls or shop online are also the same companies securing multibillion-dollar defense contracts that will shape the way the defense complex works. Tellingly, in 2022, Amazon, Oracle, Google and Microsoft were awarded contracts in order to create the Joint Warfighting Cloud Capability (JWCC) architecture for the US Department of Defense.[90] In this chapter I will set up the conversation on power and accountability surrounding private actors in the world of security, starting with the military-industrial complex (MIC), followed by conversations on Private Military Firms/Companies (PMF/PMCs) suspecting that they were accruing excessive power, followed by their relegation to lower urgency conversation as dual-use technologies rapidly grew in importance

---

[87] Dwight D. Eisenhower. 'President Dwight D. Eisenhower's Farewell Address'. Speech, Washington DC, January 17th, 1961. National Archives. Accessed June 15th, 2023. Available at: https://www.archives.gov/milestone-documents/president-dwight-d-eisenhowers-farewell-address.

[88] Barry Schwartz. 'Google Now A Verb In The Oxford English Dictionary'. *Search Engine Watch*. June 29th, 2006. Accessed June 22nd, 2023. Available at: https://www.searchenginewatch.com/2006/06/29/google-now-a-verb-in-the-oxford-english-dictionary/.

[89] Charles J. Dunlap. 'The Military-Industrial Complex.' *Daedalus* 140, no. 3 (2011): 136.

[90] Maureen Farrell. 'Pentagon Divides Big Cloud-Computing Deal Among 4 Firms'. *The New York Times*. December 7th, 2022. Accessed June 20th, 2023. Available at: https://www.nytimes.com/2022/12/07/business/pentagon-cloud-contracts-jwcc.html.

for modern security strategy, leading to the civilian tech companies that make them gaining a larger say in the future of security, ergo, exercising a measure of power.

The Military-Industrial Complex

Understanding the conversation on private actors exerting influence over security decisions in the modern era starts with the concept of the MIC and its evolution. Coined by Eisenhower in his farewell address, the MIC has since come to describe the nexus of vested interests working on defense projects, of which collaborating actors include private companies working on defense and/or civilian-use technologies, the military, and state legislature.[91] And while a MIC is largely spoken of in the US context and seen as an entity both conceptually and materially fleshed out in response to the Cold War,[92] the structure is not exclusive to the US and has persisted since.[93]

Charles Dunlap Jr. in "The Military-Industrial Complex" in 2011 suggested that the MIC was slowly starting to fade out of prominence and deliberately limited by the actions of US leaders.[94] Military spending had come to constitute much less of the GDP than decades prior, less high-technology strategies were being employed and Department of Defense (DoD) employees had started handling more of the work formerly delegated to external contractors.[95] Moreover, big business was viewed unfavorably by the public potentially dissuading the defense and legislative bases from working with them.[96] In the same year however, the work of authors such as John Paul Dunne and Elizabeth Sköns suggested that

---

[91] John Paul Dunne and Elisabeth Sköns. 'The Changing Military Industrial Complex.' Working Paper (2011): 2-3.
[92] Ibid., 3.
[93] Ibid., 6.
[94] Dunlap, 'The Military-Industrial Complex', 142-143.
[95] Ibid., 137-139.
[96] Ibid., 140.

the MIC had evolved, rather than begun to disappear, in response to changes in the global political climate as well as general technology and globalization trends.[97] The authors acknowledged major continuities in the operation style of the MIC including the presence of major contractor monopolies, high barriers to entry, marketing differences and lack of prior relationships for new commercial actors hoping to win contracts.[98] But the 1990s and 2000s had also seen warfare shift to prefer more surveillance and communication-oriented technologies in addition to more internationalized supply chains and dispersed small arms production.[99] And by 2021, Dunne and Sköns found a very different picture of how involved and integrated modern civilian tech companies were in the MIC.[100] If the barriers to entry were high in 2011 for small tech companies, by 2015 the US DoD had established the Defense Innovation Unit (DIU) to foster closer links with operations and developments in the private tech sector, including startups.[101] Civilian tech companies had actively begun to displace traditional defense contractors in the MIC as the DoD's priority, matching up if not exceeding both their influence and size as companies.[102] And while traditional defense contractors still received the largest contracts[103] civilian tech companies are increasingly integral due to their work on the technologies most relevant to modern DoD strategies.[104] In addition, both tech companies and individual leaders from the civilian tech industry had become increasingly involved in expert and advisory roles within the defense circuit.[105]

---

[97] Dunne and Sköns, 'The Changing Military Industrial Complex'.
[98] Ibid., 5.
[99] Ibid., 4.
[100] John Paul Dunne and Elisabeth Sköns. 'New technology and the U.S. military industrial complex.' *The Economics of Peace and Security Journal* 16, no.2 (2021): 5-17. DOI: http://dx.doi.org/10.15355/epsj.16.2.5.
[101] Ibid., 5.
[102] Ibid., 15.
[103] Ibid., 19.
[104] Ibid., 32.
[105] Ibid., 12, 28 and 33.

This close relationship the civilian tech sector has with the MIC has recently been featured in accountability discourse around LAWS. Isaac Taylor in "Who Is Responsible for Killer Robots? Autonomous Weapons, Group Agency, and the Military-Industrial Complex" proposes that a MIC may in fact be a suitable agent to assign responsibility for the actions of AWS and LAWS.[106] Taylor differentiates between moral, causal, and remedial responsibility and suggests that responsibility gaps result in costs including unfair remedial attributions and misdirected retributive actions.[107] Taylor goes on to suggest that an actor needs to meet two conditions to exercise control over the actions of another entity, one being causal efficacy (ability to limit or bring about certain outcomes) and the other being epistemological resources (knowledge about the outcomes and working).[108] But Taylor also finds that many actors involved in the production and deployment of AWS do not meet one or both of these conditions, both due to the nature of AWS itself, with its potential ability to evolve new capabilities in response to the battlefield, as well as the large and complicated network of relationships among those creating and deploying AWS.[109] Finding that a "group can possess capacities that exceed the sum of the capacities of the individuals that constitute it"[110] and using the concept of responsibility arising from organizational culture Taylor suggests that a MIC can potentially be held responsible for the actions of AWS if it does not develop the appropriate organizational culture.[111] This also echoes the work of Tetyana Krupiy who finds the drivers of organizational culture as possessing a particular kind of power, thus holding

---

[106] Isaac Taylor. 'Who Is Responsible for Killer Robots? Autonomous Weapons, Group Agency, and the Military-Industrial Complex.' *Journal of Applied Philosophy* 38, no. 2 (2021): 320-334. DOI: https://doi.org/10.1111/japp.12469.
[107] Ibid., 322-323.
[108] Ibid., 324.
[109] Ibid., 324-325.
[110] Ibid., 327.
[111] Ibid., 328.

the leaders of armed groups and corporate organizations who decide and organize the development of AWS as responsible for its actions.[112] Of particular interest to this paper's themes is Taylor's addressal of the possibility that the private sector sometimes has goals that diverge from that of the public sector, leading a MIC to become a fragmented actor in terms of motivations.[113] A proposed solution in this case would consider the notion of collective obligations that exists even in the absence of completely shared interests and resulting agency.[114]

Private Military Companies

The logic that underpins several strands of the conversation on private sector power with regards to AWS does not start in the realm of MICs alone but also has echoes in the discourse on PMFs or PMCs. Peter Singer defined PMFs as

> "profit-driven organizations that trade in professional services intricately linked
> to warfare. They are corporate bodies that specialize in the provision of military
> skills-including tactical combat operations, strategic planning, intelligence
> gathering and analysis, operational support, troop training, and military technical
> assistance."[115]

(I will be using this definition interchangeably to refer to PMCs as well.)

---

[112] Tetyana Krupiy. 'Unravelling Power Dynamics in Organizations: an Accountability Framework for Crimes Triggered by Lethal Autonomous Weapons Systems.' *Loyola University Chicago International Law Review* 15, no. 1 (2017): 60.
[113] Taylor, 'Who Is Responsible for Killer Robots?', 328.
[114] Ibid., 329.
[115] Peter W Singer. 'Corporate Warriors: The Rise of the Privatized Military Industry and Its Ramifications for International Security.' *International Security* 26, no. 3 (2001): 186.

Singer suggested that the intervention of private forces in wars is quite an old tradition with many kingdoms having hired mercenaries and other contracted forces. But PMFs and PMCs mark a shift in that these are primarily business profit-motivated ventures, which have a corporate hierarchy, and structured payment systems and contracts, unlike the comparatively ad hoc systems of traditional mercenary groups and individuals for hire.[116] And in tracing the reasons for the rise of PMFs one of the reasons Singer sees as integral is privatization because of neo-liberalization. While acknowledging that privatization is only one strand of broader economic neo-liberal policy[117] Aaron Ettinger also found that the private military industry was built up in response the initial roll back of excess bureaucratic barriers during the Reagan and Bush era from the 1980s through to the early 2000s.[118] This however was subsequently followed by a roll out of procedures meant to create greater accountability around contracting private firms from 2008 into 2011 at the time the paper was published.[119] But as the latest work of Dunne and Sköns indicates, despite authors such as Ettinger and Dunlap noticing the slow clamp down on defense firms, civilian tech companies have risen in the meanwhile.[120] A variation of this trend was also noted in the work of Charles Mahoney, who, though primarily focused on the work of defense firms such as Palantir who are also contracted for their software products, paid specific attention to the defense sector's turn towards Silicon Valley and a venture-capitalism inspired investment and engagement style with tech companies.[121]

---

[116] Ibid., 190-192.
[117] Aaron Ettinger. 'Neoliberalism and the Rise of the Private Military Industry.' *International Journal* 66, no. 3 (2011): 744.
[118] Ibid., 755.
[119] Ibid., 761-763.
[120] Ibid.; Dunlap, 'The Military-Industrial Complex'; Dunne and Sköns, 'New technology and the U.S. military industrial complex'.
[121] Charles W. Mahoney. 'United States defence contractors and the future of military operations' Defense & Security Analysis 36, no.2 (2020): 191-193. DOI: 10.1080/14751798.2020.1750182.

Many of the ways that Singer had found PMFs to operate are similar to the civilian tech sector companies that are the focus of this paper. PMFs often did not maintain many standing assets and drew on specialized subcontractors[122], not too unlike the tech sector. Additionally, research and reports have found that tech giants like Google and Amazon Web Services often secure awards through subcontracts.[123] Singer also discusses the phenomenon of PMFs altering the balance of power since they are not always bound by the state's control, in addition to potentially being hired by competing or opposing actors.[124] And many of these considerations can very well apply to civilian tech sector companies.

Literature on power exercised by PMCs is also valuable to understanding the influence exerted by civilian tech companies today. In this vein is the work of Anna Leander in "The Power to Construct International Security: On the Significance of Private Military Companies".[125] Leander proposes the concept of 'epistemic power' which PMCs exhibit by setting the security agenda and shaping the understandings and interests of security actors.[126] PMCs engage in selecting or defining security concerns through the gathering, selection, and analysis of private intelligence as well as the provision of suggestions on their basis. In this capacity, PMCs directly shape security discourse and understandings.[127] The other methods by which PMCs exercise epistemic power are through lobbying, as well as providing training and consulting. In all these cases PMCs not only shape the understandings and priorities of

---

[122] Singer, 'Corporate Warriors', 199.

[123] Dunne and Elisabeth Sköns. 'New technology and the U.S. military industrial complex', 16; Poulson, Jack. 'Reports of a Silicon Valley/Military Divide Have Been Greatly Exaggerated'. *Tech Inquiry*. July 7th, 2020. Accessed June 19th, 2023. Available at: https://techinquiry.org/SiliconValley-Military/.

[124] Singer, 'Corporate Warriors', 208 and 210.

[125] Anna Leander. 'The Power to Construct International Security: On the Significance of Private Military Companies'. *Millennium* 33, no. 3 (2005), 803–825. DOI: https://doi.org/10.1177/03058298050330030601.

[126] Ibid., 805.

[127] Ibid., 813-814.

their clientele but their capacities as well.[128] PMCs also possess power as an agent in the process of implementation by determining how operations are carried out on the ground, their handling of third parties, their interpretations of contracts as well as the leverage they possess depending on how reliant a military is on them.[129] PMCs, according to Leander, are moreover good at marketing themselves as competent and efficient.[130] While the power PMCs exert as agents may not be too relevant to the world of civilian private tech, the positioning of expertise as well as the ability to shape the knowledge of AWS for militaries and the public mean that such companies do possess a degree of epistemic power. This is in addition to the more active role several tech companies and their founders have taken to oppose LAWS from a moral standpoint.[131]

Åse Gilje Østensen's work in "In the Business of Peace: The Political Influence of Private Military and Security Companies [PMSCs] on UN Peacekeeping" also explores power and influence in the operations of PMCs.[132] There is a similar logic to the work of Taylor who refers to epistemological and practical power, in the work of Østensen who considers private company influence on operational and epistemological dynamics.[133] While exploring the operations of PMCs in direct, indirect, and diffuse capacities, Østensen also found that they exerted a substantial degree of control over United Nations Peacekeeping operations by

[128] Ibid., 815-818.
[129] Ibid., 809-810.
[130] Ibid., 822.
[131] Alexia Fernández Campbell. 'How tech employees are pushing Silicon Valley to put ethics before profit.' *VOX*. October 18, 2018. Accessed June 22nd, 2023. Available at: https://www.vox.com/technology/2018/10/18/17989482/google-amazon-employee-ethics-contracts; Future of Life Institute. 'Autonomous Weapons Open Letter: AI & Robotics Researchers'. February 9th, 2016. Accessed June 1st, 2023. Available at: https://futureoflife.org/open-letter/open-letter-autonomous-weapons-ai-robotics/.
[132] Åse Gilje Østensen. 'In the business of peace: the political influence of private military and security companies on UN peacekeeping.' *International Peacekeeping* 20, no. 1 (2013): 33-47. DOI: http://dx.doi.org/10.1080/13533312.2012.761872.
[133] Ibid., 33.

shaping the UN's perceptions to fit narratives that suit the desired realities of PMCs and direct action towards it.[134] They also take up a crucial role in the "knowledge formation" of those who hire them through arenas such as training.[135] This knowledge has both technical and performance components, as well as ethical and moral/potential political components which linger as they impact future understandings and operations of peacekeeping and peacekeeping forces. Østensen's conjecture about PMCs directing UN understandings and operations in a direction that suits them[136] connects in a way to Huelss' work on AWS constructing actors' understandings of normality.[137] PMCs, however, could both fit into the apparatus of discipline as well as the apparatus of security since they are both constructing a reality that suits them by prioritizing and working on issues that benefit them, but also define the normal for other actors in the process using the logics of the security apparatus.

Groundwork

Why talk about the Civilian Tech Sector

Much of the previous literature on the power of the private sector in the security arena has tended to focus on traditional defense companies, MICs, as well as PMCs. However, in recent years, and particularly in the US context, many of these works have alluded to the gradual rise of Silicon Valley, both inspiring the business model the US defense complex seeks to emulate, as well as being the umbrella term for tech companies that have become an active collaborator with the DoD. And this phenomenon runs concurrently with increasing focus in

---

[134] Ibid., 34 and 40.
[135] Ibid., 39.
[136] Ibid.
[137] Huelss, 'Norms Are What Machines Make of Them.'

literature on dual-use technologies and AI with authors exploring both the security[138] and market implications[139] of dual-use technologies. The work of Acosta et al, recently focused on the production of dual-use technologies by several major defense companies, finding that larger players in terms of sales, employees and better technological productivity often created more civilian use patents.[140] As the traditional production bastions of military technology themselves are turning towards civilian and dual-use technology,[141] it is imperative to explore the effects the civilian tech sector has on security discourses given their prolific role in the development of AI, which is increasingly important to military strategy today,[142] but also perhaps fundamentally changing civil society and the economy.[143]

One of the most visible areas of the civilian tech sector's effects on security would be the conversation on LAWS and AWS given the AI technology that powers the autonomy of these systems. As established earlier in the literature review on AWS, the conversation about autonomous weaponry has become a concern in civilian conversation, which means its importance to state policy would not lag far behind. However, much of the academic discourse in the social sciences on AWS and LAWS has tended to focus on the technology itself, exploring its capabilities as well as its implications for society and law. The work of authors such as Taylor exist at the intersection of the older conversations on MICs while

[138] Amir Lupovici. 'The dual-use security dilemma and the social construction of insecurity' *Contemporary Security Policy* 42, no. 3 (2021): 257-285. DOI: 10.1080/13523260.2020.1866845.
[139] Matthew Fuhrmann. 'Exporting Mass Destruction? The Determinants of Dual-Use Trade.' *Journal of Peace Research* 45, no. 5 (2008): 633–652.
[140] Manuel Acosta et al. 'Patents and Dual-use Technology: An Empirical Study of the World's Largest Defence Companies' *Defence and Peace Economics* 29, no.7 (2018): 821-839. DOI: 10.1080/10242694.2017.1303239.
[141] Ibid.
[142] CDAO – Chief Digital and Artificial Intelligence Office. *Chief Digital and Artificial Intelligence Office*. Accessed June 21st, 2023. Available at: https://www.ai.mil/index.html.
[143] Toh, Michelle. '300 million jobs could be affected by latest wave of AI, says Goldman Sachs.' *CNN Business*. March 29th, 2023. Accessed June 20th, 2023. Available at: https://edition.cnn.com/2023/03/29/tech/chatgpt-ai-automation-jobs-impact-intl-hnk/index.html.

contributing to modern accountability discourse on LAWS, exploring how the private sector as part of the MIC can be held jointly accountable for errant functions of AWS machinery.[144]

In the coming section, I will be focusing on academic literature that has explored the role of the civilian tech sector with regards to AWS, followed by those that have specifically focused on power concepts.

Spinning In with Difficulty

Maaike Verbruggen's work on the civilian tech sector's importance to AWS and the state has been cognizant of the limitations of the civilian private sector when it comes to influencing the operations of the military.[145] In their work with Vincent Boulanin in the report "Mapping the Development of Autonomy in Weapon Systems", Boulanin and Verbruggen note that the civilian sector has always led the curve when it comes to developing autonomy, but they also note that this may be a result of the civilian sector needing to take on less engineering difficulties than the military for their projects.[146] In continuation to this theme they also note that many civilian technologies need significant modification before they can truly spin in to defense use.[147] These difficulties were elucidated by Verbruggen in an earlier work on the phenomenon of technological transfer, which considered inherent difficulties to military transfer in the case of certain dual-use technologies,[148] suggesting that the civilian sphere is not always capable of providing complete systems to the military but rather components,

---

[144] Taylor, 'Who Is Responsible for Killer Robots?'

[145] Maaike Verbruggen. 'The Role of Civilian Innovation in the Development of Lethal Autonomous Weapon Systems'. *Global Policy* 10, no. 3 (2019): 338-342. DOI: https://doi.org/10.1111/1758-5899.12663.

[146] Boulanin and Verbruggen, *Mapping the Development of Autonomy in Weapon Systems*, 106-108.

[147] Ibid., 110 and 340.

[148] Verbruggen, 'The Role of Civilian Innovation in the Development of Lethal Autonomous Weapon Systems', 339.

materials, and process technologies.[149] However, while this may be true, it is also important to note that in modern day military process, especially in countries such as the US, contracts are typically awarded to civilian tech sector companies in order to custom-build architectures, systems and software for defense purposes (such as the JWCC or Project Maven)[150] thus avoiding of the issue of needing modifications. In addition, Verbruggen also noted that due to differences in business practices, innovation cultures, a lack of social ties and ethical differences, the military and civil companies don't always find it easy to cooperate.[151] However, as the work on the evolving nature of MICs has indicated, the military may very well be shifting its culture to better suit that of the private sector.

Power and the Private

More optimistic about the power prospects of the civilian tech sector in international security and an integral reason for my curiosity about the topic is the work of Kara Frederick in "The civilian private sector: part of a new arms control regime?"[152] Noting both the advanced developments in AI technologies by private sector companies as well as boycotts of defense projects in the US and South Korea by private actors, Frederick suggested that "the civilian private sector has already begun to articulate standards".[153] Frederick in fact urges for the

---

[149] Ibid., 341.

[150] Thomas Brewster. 'Project Maven: Startups Backed By Google, Peter Thiel, Eric Schmidt And James Murdoch Are Building AI And Facial Recognition Surveillance Tools For The Pentagon'. Forbes. September 8th, 2021. Accessed June 10th, 2023. Available at: https://www.forbes.com/sites/thomasbrewster/2021/09/08/project-maven-startups-backed-by-google-peter-thiel-eric-schmidt-and-james-murdoch-build-ai-and-facial-recognition-surveillance-for-the-defense-department/.

[151] Verbruggen, 'The Role of Civilian Innovation in the Development of Lethal Autonomous Weapon Systems', 339-340.

[152] Kara Frederick. 'The civilian private sector: part of a new arms control regime?' *Observer Research Foundation.* November 6th, 2019. Accessed September 28th, 2022. Available at: https://www.orfonline.org/expert-speak/the-civilian-private-sector-part-of-a-new-arms-control-regime-57345/.

[153] Ibid.

trend to continue by exploring the potential for civilian tech companies to become valuable

governance actors in the world of AWS. One of the ways Frederick suggests is for "human

capital standouts"[154] in the field to help design normative frameworks. Another is through

the formation of non-traditional partnerships between companies to act as forums or

supergroups with an ethical agenda. However, Frederick's work, while acknowledging the

potential of the civilian private tech sector to become a governance actor, does not explore

the phenomenon through a distinct power lens.

This is where the work of Tetyana Krupiy in "Unravelling Power Dynamics in Organizations:

an Accountability Framework for Crimes Triggered by Lethal Autonomous Weapons

Systems"[155] and Nik Hynek and Anzhelika Solovyeva's work in "Operations of power

in autonomous weapon systems: ethical conditions and socio-political prospects"[156] form

valuable additions to power literature about the role of private actors in the world of AWS.

Krupiy's work is not solely concerned with the power of civilian private tech companies but

rather seeks to understand how power informs accountability for crimes committed by AWS

or LAWS.[157] Krupiy finds the Doctrine of Command Responsibility insufficient for assigning

accountability due to the inability of several actors from programmers to operators (and

consequentially their superiors) to exert "effective control" over the actions of LAWS.[158]

Thus, Krupiy turns to the work of Foucault and specifically the Foucauldian understanding

of power as the ability to shape or limit an actor's understanding of the actions they can

---

154 Ibid.
155 Krupiy, 'Unravelling Power Dynamics in Organizations'.
156 Nik Hynek and Anzhelika Solovyeva. 'Operations of power in autonomous weapon systems: ethical conditions and socio-political prospects'. *AI & SOCIETY* 36 (2021): 79–99. DOI: https://doi.org/10.1007/s00146-020-01048-1.
157 Krupiy, 'Unravelling Power Dynamics in Organizations'.
158 Ibid., 21-34.

pursue.[159] Krupiy is particularly focused on the three mechanisms Foucault describes as being part of the exercise of power, which are technical capacity (which involves tasks directed at producing certain outcomes such as training), communication, and relations of power (which are often hierarchical and enable goal directed behavior).[160] And on exploring the power dynamics creating phenomenon such as organizational cultures through the lens of the three mechanisms, Krupiy comes to find that it is individuals who have "control over the deliberative process of the collective" that should be held responsible for the actions of LAWS.[161] Thus, Krupiy finds the most accountable parties to be the leaders of armed forces and/or organizations that push for the development of AWS, as well as senior corporate officials of the companies that produce essential components for AWS such as AI software.[162] However, Krupiy's work is primarily focused on the power dynamics internal to organizations and does not focus on the macro perspective of power actors in the world of AWS relative to each other or the global system.

This is where Hynek and Solovyeva's work is a good starting guide to the major power player archetypes in the world of AWS today. The authors explore the nature of power exercised by several actors from states, to IGOs and civil-society actors using Barnett and Duvall's framework[163] of power that puts a focus on social structures and processes[164] in the arena of the actors' positions on banning LAWS. In "Power in International Politics" Barnett and Duvall suggest that most existing conceptions of power can be aggregated into four types:

---

[159] Ibid., 36.
[160] Ibid., 38-39.
[161] Ibid., 50-51.
[162] Ibid., 59.
[163] Hynek and Solovyeva, 'Operations of power in autonomous weapon systems', 79.
[164] Barnett and Duvall, 'Power in International Politics', 42.

Compulsory, Institutional, Structural and Productive Power.[165] They find these power types existing along two dimensions. One based on how power is expressed through either interaction or constitution, following the logic of "power over" and "power to".[166] And the second dimension dealing with the specificity of the social relations of power, where power is either direct or indirect/diffuse.[167] Along both these dimensions arise the four categories. Compulsory Power which refers to power as direct interactions that "focuses on a range of relations between actors that allow one to shape directly the circumstances or actions of another".[168] Institutional Power which refers to power as diffuse interactions where actors exert effects on each other within an institutional framework despite possessing spatial or temporal distance.[169] Structural Power which refers to direct and constitutive effects determining the interests and social capacities of actors as power.[170] And lastly, Productive Power which as a diffuse but constitutive understanding of power refers to the "constitution of all social subjects with various social powers through systems of knowledge and discursive practices of broad and general social scope".[171]

Hynek and Solovyeva pay particular attention to the scheme of Productive Power as the place where "everything starts" given that framing and discursive practices are integral to the ethical framing of LAWS by the actors they study.[172] When it comes to private civilian tech companies Hynek and Solovyeva view them through the lens of Structural and Compulsory Power. Acknowledging that they are often viewed as experts in the field, within the domain

---

[165] Ibid.
[166] Ibid., 45-46.
[167] Ibid., 47-48.
[168] Ibid., 49.
[169] Ibid., 51.
[170] Ibid., 53.
[171] Ibid., 55.
[172] Hynek and Solovyeva, 'Operations of power in autonomous weapon systems', 82.

33

of Structural Power logics, Hynek and Solovyeva note that private tech companies in the US have often shown disaggregated or even hypocritical stances when it comes to their ethical position on LAWS. However, when it comes to both Structural and Compulsory Power the authors seem to espouse a sense that given the case of states such as Russia and China, it may be difficult for civilian tech sector actors to operate outside of the bounds of the state.[173] Moreover, even within exploring the Structural Power of the civilian tech sector, the authors focus on the ethical positions of the actors over their power capabilities.

The Powers of the Civilian Tech Sector

This section explores how the civilian private tech sector fits into Barnett and Duvall's framework of types of power, using the work of Hynek and Solovyeva as a launch pad and inspiration. As part of this process, I suggest that the civilian tech sector is both a stronger player than implied in the work of Hynek and Solovyeva and find that the sector occupies strands of power logics that the authors had not yet attributed to the civilian tech sector.

Compulsory Power

Leander noted that several PMCs often made it a point to take contracts from other actors only after receiving their concerned home state's approval.[174] And in line with this trend, it would seem many tech companies still seem to prefer collaborating with the militaries of their home government. Several companies based in or originating out of the US such as Microsoft or Google regularly take on contracts for their home state,[175] similar to companies

---

[173] Ibid., 85-89.
[174] Leander, 'The Power to Construct International Security', 807.
[175] Poulson, 'Reports of a Silicon Valley/Military Divide Have Been Greatly Exaggerated'.

such as Hong Kong's SenseTime which closely work with the Chinese government.[176] However while the process of collaborating with organizations or institutions that may have links to other states may not necessarily be treasonous as some strands of thought might imply,[177] the decision to work strictly with one's home state is potentially a matter of preference for some tech sector companies. While it is valid that state control may be more difficult to escape for private companies in countries such as China and Russia, tech companies from the US tend to dominate global charts regularly[178] giving them a degree of economic clout, and high-profile companies such as Google have sometimes expressed reluctance to work with their home state on ethical grounds.[179] While it is more typical for other companies to competitively bid over the same contract another company might have withdrawn from,[180] at least in principle, it is possible for the companies of the private tech sector to halt or at least slow down an AWS project by taking a united stance against a contract on ethical or other grounds. Since civilian tech companies are already large entities of their

---

[176] Gregory C. Allen. 'China's Pursuit of Defense Technologies: Implications for U.S. and Multilateral Export Control and Investment Screening Regimes.' Congressional Testimony, Washington DC, USA, April 13th, 2023. *Center for Strategic and International Studies*. April 13th, 2023. Accessed June 21st, 2023. Available at: https://www.csis.org/analysis/chinas-pursuit-defense-technologies-implications-us-and-multilateral-export-control-and.

[177] Kif Leswing. 'Peter Thiel criticizes Google and Apple for being too close to China.' CNBC. April 7th, 2021. Accessed June 22nd, 2023. Available at: https://www.cnbc.com/2021/04/07/peter-thiel-criticizes-google-and-apple-for-being-too-close-to-china-.html.

[178] Jeff Desjardins. 'Visualizing The World's 20 Largest Tech Giants.' *Visual Capitalist*. July 6th, 2018. Accessed June 20th, 2023. Available at: https://www.visualcapitalist.com/visualizing-worlds-20-largest-tech-giants/; Jonathan Ponciano. 'The World's Largest Technology Companies In 2023: A New Leader Emerges'. *Forbes*. June 8th, 2023. Accessed June 20th, 2023. Available at: https://www.forbes.com/sites/jonathanponciano/2023/06/08/the-worlds-largest-technology-companies-in-2023-a-new-leader-emerges/

[179] Scott Shane and Daisuke Wakabayashi. 'Google Will Not Renew Pentagon Contract That Upset Employees'. The New York Times. June 1st, 2018. Accessed June 19th, 2023. Available at: https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html.

[180] Aaron Gregg and Jay Greene. 'Pentagon awards controversial $10 billion cloud computing deal to Microsoft, spurning Amazon'. *The Washington Post*. October 25th, 2019. Accessed June 20th, 2023. Available at: https://www.washingtonpost.com/business/2019/10/25/pentagon-awards-controversial-billion-cloud-computing-deal-microsoft-spurning-amazon/; Rosalie Chan. 'Google drops out of contention for a $10 billion defense contract because it could conflict with its corporate values'. *Business Insider*. October 9th, 2018. Accessed June 20th, 2023. Available at: https://www.businessinsider.com/google-drops-out-of-10-billion-jedi-contract-bid-2018-10?r=US&IR=T.

own,[181] many of them can afford to continue operating profitably in the absence of military contracts. Moreover, away from the domain of the world's largest tech players based in the US, other civilian tech companies such as Vision Labs of the Netherlands and Japan's SoftBank have stated their commitment to not creating LAWS.[182] Barnett and Duvall clearly acknowledge in their work on Compulsory Power that some of the exercises of this kind of power can include the actions of entities, including multinational corporations, to shape decision-making by exerting symbolic (if not direct material pressure).[183] While many tech companies may not directly demand a reform or a ban, a refusal to reap the material rewards of working on AWS-linked projects with governments, or refusing to pour their resources into such projects can convey symbolic pressure, whose ramifications may be felt down the line in economic terms as well.

Structural and Productive Power

In addition, the economic size of several civilian tech sector companies, as well MICs increasingly integrating and consulting tech sector companies in response to strategic and economic changes (as discussed earlier in the paper), lends greater credibility to the idea that private tech sector companies may not be insignificant actors in terms of possessing Structural Power, especially on the matter of AWS. Lastly, as Frederick suggested[184] many of these companies can band together and take specific positions, create campaigns, or push certain ethical stances.[185] While the ability to do this in itself does not guarantee that the

[181] Dunne and Sköns, 'The Changing Military Industrial Complex.'
[182] PAX. 'Major Tech Companies may be putting world at risk from Killer Robots'. *PAX*. August 19th, 2019. Accessed June 1st, 2023. Available at: https://paxforpeace.nl/news/major-tech-companies-may-be-putting-world-at-risk-from-killer-robots/.
[183] Barnett and Duvall, 'Power in International Politics', 50.
[184] Frederick, 'The civilian private sector.'
[185] Google AI. Responsibility: Our Principles. Accessed June 23rd, 2023. Available at: https://ai.google/responsibility/principles/; PAX. 'Lethal autonomous weapon systems and the tech sector:

civilian private tech sector possesses strong degrees of productive power, if we retrace the underpinnings of "epistemic power" in the work of Leander,[186] it becomes clear that one of the things modern tech companies have in common with PMCs, are support for the notion that they are more competent actors than governments.[187] While the merits of this claim are debatable, the impression that these companies are competent in itself assures that they carry a discursive power which has effects when they speak. Tech leaders such as Elon Musk have been known to cause stock performances to plummet or rise overnight.[188] And while both these instances could be attributed to the scrutinous following around Musk alone, much of the research referenced in this paper also finds similar trends. Civil society campaigns have been so eager to feature endorsements from major players in the tech industry, that some have resulted in false claims.[189] Thus it might not be far-fetched to suggest that based on Barnett and Duvall's criteria,[190] civilian tech companies may also be actors who possess a measure of productive power. The tech industry category in itself has come to possess a certain connotation of leadership, knowledge and competence in the conversation on AI and AWS,

---

some examples of best practices'. PAX. August 19th, 2019. Accessed June 22nd, 2023. Available at: https://paxforpeace.nl/news/lethal-autonomous-weapon-systems-and-the-tech-sector-some-examples-of-best-practices/.

[186] Leander, 'The Power to Construct International Security'.

[187] Byrne Hobart. 'Why Big Tech Is More Competent Than the US Government'. Palladium. July 1st, 2020. Accessed June 20th, 2023. Available at: https://www.palladiummag.com/2020/07/01/why-big-tech-is-more-competent-than-the-us-government/; Liz Wolfe. 'The New York Times Is Wrong About the 'Myth of Big Tech Competence'. Still, Facebook should not have allowed its VIPs to flout the rules it claimed applied to everyone.' Reason. September 9th, 2021. Accessed June 20th, 2023. Available at: https://reason.com/2021/09/16/the-new-york-times-is-wrong-about-the-myth-of-big-tech-competence/.

[188] Paul A. Eisenstein. 'Tesla stock plummets after Elon Musk smokes weed on live show and two execs quit in one day.' NBC News. September 7th, 2018. Accessed June 21st, 2023. Available at: https://www.nbcnews.com/tech/tech-news/tesla-stock-plummets-after-elon-musk-smokes-weed-live-show-n907476.Yun Li and Leslie Picker. 'The fund that made $700 million on GameStop knew it was time to sell after an Elon Musk tweet.' CNBC. January 27th, 2022. Accessed June 21st, 2023. Available at: https://www.cnbc.com/2022/01/27/the-fund-that-made-700-million-on-gamestop-knew-it-was-time-to-sell-after-an-elon-musk-tweet.html.

[189] Kari Paul. 'Letter signed by Elon Musk demanding AI research pause sparks controversy.' The Guardian. Accessed June 21st, 2023. Available at: April 1st, 2023. https://www.theguardian.com/technology/2023/mar/31/ai-research-pause-elon-musk-chatgpt.

[190] Barnett and Duvall, 'Power in International Politics'.

not just by virtue of being the producers of much of AWS tech, but thanks to the general categorical regard in society for their competence. Institutional Power seems to be the least relevant category of power to civilian tech sector companies since they are often not regarded as major players in IGO-led fixtures such as the CCW and are rarely a direct part of state instruments. A case could be made through their economic linkages to the market, but the global and state markets are not institutions in a conventional sense. Nonetheless, the literature reviewed in this paper, as well as the specific explorations of this section reveal that even when one changes out the lenses of power, the civilian tech sector today is an undeniably important power in the traditional domain of the military and security.

Conclusion

The "reluctant" in the title of this paper may seem somewhat obtuse given the overall contents of the work. After all, what does reluctance have to do with possessing power. As the work of Barrett and Duvall points out however, there is a class of actors that may not be aware of their own power,[191] or perhaps may not understand or be ready to handle the ways in which they exercise power in a consistent manner. And this might partially hold true in the case of several civilian tech sector actors, who, over the course of this paper, have been established as possessing at least three kinds of power.

As developers of dual-use technology, AI and machine-learning tech sector leaders are also answerable to the civilian public. Given this context, private sector leaders taking a cautionary stance on LAWS, as evidenced in the Open Letter from the introduction, can be interpreted not just as a matter of the organization's ethical beliefs but one of optics and a

---

[191] Ibid., 53.

matter of their survival in the global market. However, despite Google's decision to withdraw from Project Maven as well as the JEDI project on ethical grounds, the JWCC contract that Google was eventually awarded is known as a successor to the JEDI project. Moreover, this was taken up despite employees flagging concerns.[192] Microsoft, though criticizing an AI arms race in previous years[193] has continued to be one of the US Government's most consistent collaborators on security and defense projects.[194] Such inconsistencies, though these actors possess power, indicate these companies are reluctant moral leaders at best, and manipulative opportunists at worst. And while it is important enough to understand the actors that influence the sphere of AWS for the purpose of theoretical cohesion alone, in a world that has witnessed a devastating war between Ukraine and Russia in the last years, and had to contend with the fact that autonomous weapons were likely already part of this war,[195] understanding who has the power to decide the future of how we do warfare, and how much they care to do so, is perhaps a matter of life and death.

---

[192] Colin Demarest. 'Amazon, Google, Microsoft and Oracle picked for $9B JEDI successor'. *Defense News*. December 8th, 2022. Accessed June 22nd, 2023. Available at:
https://www.defensenews.com/industry/2022/12/07/amazon-google-microsoft-and-oracle-picked-for-9b-jedi-successor/; Jennifer Elias. 'Google's pursuit of military cloud deal was among top issues at last week's all-staff meeting.' *CNBC*. November 15th, 2021. Accessed June 23rd, 2023. Available at:
https://www.cnbc.com/2021/11/15/google-pursuit-of-jwcc-among-issues-of-top-concern-at-tgif-meeting-.html.
[193] Alice Beck et al. '*Don't be evil?*': 46. 2019. ISBN: 978-94-92487-44-5. Available at:
https://paxforpeace.nl/wp-content/uploads/sites/2/import/import/pax-report-killer-robots-dont-be-evil.pdf
[194] Poulson, 'Reports of a Silicon Valley/Military Divide Have Been Greatly Exaggerated'.
[195] Morgan Meaker. 'Ukraine's War Brings Autonomous Weapons to the Front Lines'. *WIRED*. February 24th, 2023. Accessed June 22nd, 2023. Available at: https://www.wired.co.uk/article/ukraine-war-autonomous-weapons-frontlines.

Bibliography

Acosta, Manuel, et al. 'Patents and Dual-use Technology: An Empirical Study of the World's Largest Defence Companies' *Defence and Peace Economics* 29, no.7 (2018): 821-839. DOI: 10.1080/10242694.2017.1303239.

Allen, Gregory C. 'China's Pursuit of Defense Technologies: Implications for U.S. and Multilateral Export Control and Investment Screening Regimes.' Congressional Testimony, Washington DC, USA, April 13th, 2023. *Center for Strategic and International Studies*. April 13th, 2023. Accessed June 21st, 2023. Available at: https://www.csis.org/analysis/chinas-pursuit-defense-technologies-implications-us-and-multilateral-export-control-and.

Altmann, Jürgen and Frank Sauer. 'Autonomous Weapon Systems and Strategic Stability'. *Survival* 59, no.5 (2017): 117-142. DOI: 10.1080/00396338.2017.1375263.

Arai, Koki and Masakazu Matsumoto. 'Public perceptions of autonomous lethal weapons systems'. *AI and Ethics* (2023): 1-12. DOI: https://doi.org/10.1007/s43681-023-00282-9.

Arkin, Ronald C. 'The Case for Ethical Autonomy in Unmanned Systems'. *Journal of Military Ethics* 9, no. 4 (2010): 332-341. DOI: 10.1080/15027570.2010.536402.

Barnett, Michael and Raymond Duvall. 'Power in International Politics.' *International Organization* 59, no. 1 (2005): 39–75.

Beck, Alice et al. 'Don't be evil?': 46. 2019. ISBN: 978-94-92487-44-5. Available at: https://paxforpeace.nl/wp-content/uploads/sites/2/import/import/pax-report-killer-robots-dont-be-evil.pdf

Bode, Ingvild and Hendrik Huelss. 'Autonomous Weapons Systems and Changing Norms in International Relations.' *Review of International Studies* 44, no. 3 (2018): 393–413. DOI: 10.1017/S0260210517000614.

Boulanin, Vincent and Maaike Verbruggen. *Mapping the Development of Autonomy in Weapon Systems*. SIPRI, 2017. DOI: 10.13140/RG.2.2.22719.41127.

Brewster, Thomas. 'Project Maven: Startups Backed By Google, Peter Thiel, Eric Schmidt And James Murdoch Are Building AI And Facial Recognition Surveillance Tools For The Pentagon'. *Forbes*. September 8th, 2021. Accessed June 10th, 2023. Available at: https://www.forbes.com/sites/thomasbrewster/2021/09/08/project-maven-startups-backed-by-google-peter-thiel-eric-schmidt-and-james-murdoch-build-ai-and-facial-recognition-surveillance-for-the-defense-department/.

Britannica, T. Editors of Encyclopaedia. 'doomsday machine.' *Encyclopedia Britannica*. January 30th, 2014. Accessed April 3rd, 2023. Available at: https://www.britannica.com/technology/doomsday-machine.

Caccia, Gabriele Giordano. 'Joint Statement on Lethal Autonomous Weapons Systems First Committee, 77th United Nations General Assembly Thematic Debate – Conventional Weapons'. *United Nations*. October 21st, 2022. Accessed April 3rd, 2023. Available at: https://estatements.unmeetings.org/estatements/11.0010/20221021/A1jJ8bNfWGlL/K Lw9WYcSnnAm_en.pdf.

Campbell, Alexia Fernández. 'How tech employees are pushing Silicon Valley to put ethics before profit.' *VOX*. October 18, 2018. Accessed June 22nd, 2023. Available at: https://www.vox.com/technology/2018/10/18/17989482/google-amazon-employee-ethics-contracts.

Carpenter, Charli. 'How do Americans feel about Fully Autonomous Weapons?' *The Duck of Minerva*. June 19th, 2013. Accessed 25th May 2023. Available at: https://www.duckofminerva.com/2013/06/how-do-americans-feel-about-fully-autonomous-weapons.html.

CDAO – Chief Digital and Artificial Intelligence Office. *Chief Digital and Artificial Intelligence Office*. Accessed June 21st, 2023. Available at: https://www.ai.mil/index.html.

Chan, Rosalie. 'Google drops out of contention for a $10 billion defense contract because it could conflict with its corporate values'. *Business Insider*. October 9th, 2018. Accessed June 20th, 2023 . Available at: https://www.businessinsider.com/google-drops-out-of-10-billion-jedi-contract-bid-2018-10?r=US&IR=T.

Demarest, Colin. 'Amazon, Google, Microsoft and Oracle picked for $9B JEDI successor'. Defense News. December 8th, 2022. Accessed June 22nd, 2023. Available at: https://www.defensenews.com/industry/2022/12/07/amazon-google-microsoft-and-oracle-picked-for-9b-jedi-successor/.

Desjardins, Jeff. 'Visualizing The World's 20 Largest Tech Giants.' *Visual Capitalist*. July 6th, 2018. Accessed June 20th, 2023. Available at: https://www.visualcapitalist.com/visualizing-worlds-20-largest-tech-giants/.

Devitt, S. Kate. 'Normative Epistemology for Lethal Autonomous Weapons Systems'. In *Lethal Autonomous Weapons: Re-Examining the Law and Ethics of Robotic Warfare*. Eds. Jai Galliott, Duncan MacIntosh and Jens David Ohlin, 237-258. Oxford University Press, 2021. DOI: 10.1093/oso/9780197546048.003.0016.

Dunlap, Charles J. 'The Military-Industrial Complex.' *Daedalus* 140, no. 3 (2011): 135-47.

Dunne, John Paul and Elisabeth Sköns. 'New technology and the U.S. military industrial complex.' *The Economics of Peace and Security Journal* 16, no.2 (2021): 5-17. DOI: http://dx.doi.org/10.15355/epsj.16.2.5.

Dunne, John Paul and Elisabeth Sköns. 'The Changing Military Industrial Complex.' Working Paper (2011): 1-9.

Eisenhower, Dwight D. 'President Dwight D. Eisenhower's Farewell Address'. Speech, Washington DC, January 17th, 1961. *National Archives*. Accessed June 15th, 2023. Available at: https://www.archives.gov/milestone-documents/president-dwight-d-eisenhowers-farewell-address.

Eisenstein, Paul A. 'Tesla stock plummets after Elon Musk smokes weed on live show and two execs quit in one day.' *NBC News*. September 7th, 2018. Accessed June 21st, 2023. Available at: https://www.nbcnews.com/tech/tech-news/tesla-stock-plummets-after-elon-musk-smokes-weed-live-show-n907476.

Elias, Jennifer. 'Google's pursuit of military cloud deal was among top issues at last week's all-staff meeting.' *CNBC*. November 15th, 2021. Accessed June 23rd, 2023. Available at: https://www.cnbc.com/2021/11/15/google-pursuit-of-jwcc-among-issues-of-top-concern-at-tgif-meeting-.html.

Ettinger, Aaron. 'Neoliberalism and the Rise of the Private Military Industry.' *International Journal* 66, no. 3 (2011): 743–764.

Farrell, Maureen. 'Pentagon Divides Big Cloud-Computing Deal Among 4 Firms'. *The New York Times*. December 7th, 2022. Accessed June 20th, 2023. Available at: https://www.nytimes.com/2022/12/07/business/pentagon-cloud-contracts-jwcc.html.

Frederick, Kara. 'The civilian private sector: part of a new arms control regime?' *Observer Research Foundation*. November 6th, 2019. Accessed September 28th, 2022. Available at: https://www.orfonline.org/expert-speak/the-civilian-private-sector-part-of-a-new-arms-control-regime-57345/.

Fuhrmann, Matthew. 'Exporting Mass Destruction? The Determinants of Dual-Use Trade.' *Journal of Peace Research* 45, no. 5 (2008): 633–652.

Future of Life Institute. 'An Open Letter to the United Nations Convention on Certain Conventional Weapons'. August 20th, 2017. Accessed November. 25th, 2021. Available at: https://futureoflife.org/open-letter/autonomous-weapons-open-letter-2017/.

Future of Life Institute. 'Autonomous Weapons Open Letter: AI & Robotics Researchers'. February 9th, 2016. Accessed June 1st, 2023. Available at: https://futureoflife.org/open-letter/open-letter-autonomous-weapons-ai-robotics/.

Future of Life Institute. *FLI Open Letters*. Accessed May 20th, 2023. Available at: https://futureoflife.org/fli-open-letters/.

Galliott, Jai and McFarland, Tim. 'Understanding AI and Autonomy: Problematizing the Meaningful Human Control Argument against Killer Robots'. In *Lethal Autonomous Weapons: Re-Examining the Law and Ethics of Robotic Warfare*. Eds. Jai Galliott, Jens

David Ohlin and Duncan MacIntosh. Oxford University Press, 2021. DOI: 10.1093/oso/9780197546048.003.0004.

Garcia, Denise. 'Lethal Artificial Intelligence and Change: The Future of International Peace and Security'. *International Studies Review* 20, no. 2 (2018): 334-341. DOI: https://doi.org/10.1093/isr/viy029.

Google AI. *Responsibility: Our Principles*. Accessed June 23rd, 2023. Available at: https://ai.google/responsibility/principles/.

Greene, Jay and Gregg, Aaron. 'Pentagon awards controversial $10 billion cloud computing deal to Microsoft, spurning Amazon'. The Washington Post. October 25th, 2019. Accessed June 20th, 2023. Available at: https://www.washingtonpost.com/business/2019/10/25/pentagon-awards-controversial-billion-cloud-computing-deal-microsoft-spurning-amazon/.

Hobart, Byrne. 'Why Big Tech Is More Competent Than the US Government'. *Palladium*. July 1st, 2020. Accessed June 20th, 2023. Available at: https://www.palladiummag.com/2020/07/01/why-big-tech-is-more-competent-than-the-us-government/.

Horowitz, Michael C. 'Public opinion and the politics of the killer robots debate'. *Research & Politics* 3, no. 1 (2016): 1-8. DOI: https://doi.org/10.1177/2053168015627183.

Horowitz, Michael C. 'When Speed Kills: Autonomous Weapon Systems, Deterrence, and Stability'. SSRN (2019, under review): 1-27. Available at: https://ssrn.com/abstract=3348356.

Huelss, Hendrik. 'Norms Are What Machines Make of Them: Autonomous Weapons Systems and the Normative Implications of Human-Machine Interactions'. *International Political Sociology* 14, no. 2 (2020): 1-18. DOI: https://doi.org/10.1093/ips/olz023.

Hynek, Nik and Anzhelika Solovyeva. 'Operations of power in autonomous weapon systems: ethical conditions and socio-political prospects'. *AI & SOCIETY* 36 (2021): 79–99. DOI: https://doi.org/10.1007/s00146-020-01048-1.

Kalpouzos, Ioannis. 'Double Elevation: Autonomous Weapons and the Search for an Irreducible Law of War'. *Leiden Journal of International Law* 33, no. 2 (2020): 289-312.

Krupiy, Tetyana. 'Unravelling Power Dynamics in Organizations: an Accountability Framework for Crimes Triggered by Lethal Autonomous Weapons Systems.' *Loyola University Chicago International Law Review* 15, no. 1 (2017): 1-61.

Ipsos. 'Global Survey Highlights Continued Opposition to Fully Autonomous Weapons'. *Ipsos*. February 22nd, 2021. Accessed 30th May 2023. Available at: https://www.ipsos.com/en-us/global-survey-highlights-continued-opposition-fully-autonomous-weapons.

Leander, Anna. 'The Power to Construct International Security: On the Significance of Private Military Companies'. *Millennium* 33, no. 3 (2005), 803–825. DOI: https://doi.org/10.1177/03058298050330030601.

Lee, Kai-Fu. 'The Third Revolution in Warfare'. The Atlantic. September 11th, 2021. Accessed June 2nd, 2023. Available at:

https://www.theatlantic.com/technology/archive/2021/09/i-weapons-are-third-revolution-warfare/620013/.

Leswing, Kif. 'Peter Thiel criticizes Google and Apple for being too close to China.' *CNBC*. April 7th, 2021. Accessed June 22nd, 2023. Available at: https://www.cnbc.com/2021/04/07/peter-thiel-criticizes-google-and-apple-for-being-too-close-to-china-.html.

Li, Yun and Leslie Picker. 'The fund that made $700 million on GameStop knew it was time to sell after an Elon Musk tweet.' *CNBC*. January 27th, 2022. Accessed June 21st, 2023. Available at: https://www.cnbc.com/2022/01/27/the-fund-that-made-700-million-on-gamestop-knew-it-was-time-to-sell-after-an-elon-musk-tweet.html.

Lupovici, Amir. 'The dual-use security dilemma and the social construction of insecurity' *Contemporary Security Policy* 42, no. 3 (2021): 257-285. DOI: 10.1080/13523260.2020.1866845.

Macdonald, Julia and Schneider, Jacquelyn. 'Looking back to look forward: Autonomous systems, military revolutions, and the importance of cost'. *Journal of Strategic Studies* (2023): 1-23. DOI: 10.1080/01402390.2022.2164570.

Mahoney, Charles W. 'United States defence contractors and the future of military operations' *Defense & Security Analysis* 36, no.2 (2020): 180-200. DOI: 10.1080/14751798.2020.1750182.

Meaker, Morgan. 'Ukraine's War Brings Autonomous Weapons to the Front Lines'. *WIRED*. February 24th, 2023. Accessed June 22nd, 2023. Available at: https://www.wired.co.uk/article/ukraine-war-autonomous-weapons-frontlines.

Morgan, Patrick M. 'The impact of the revolution in military affairs'. *Journal of Strategic Studies* 23, no.1 (2000): 132-162. DOI: 10.1080/01402390008437781.

Morrow, Allison. 'Elon Musk Tweet Fuels Frenzied GameStop Surge'. *CNN*. January 27, 2021. Accessed November 25th, 2021. Available at: https://edition.cnn.com/2021/01/26/investing/gamestop-stock-elon-musk-reddit/index.html.

Newton, Michael A. 'Back to the Future: Reflections on the Advent of Autonomous Weapons Systems.' *Case Western Reserve Journal of International Law* 47, no.1 (2015): 5-23.

OHCHR. *A call for a moratorium on the development and use of lethal autonomous robots*. May 31st, 2013. Accessed May 19th, 2023. Available at: https://www.ohchr.org/en/stories/2013/05/call-moratorium-development-and-use-lethal-autonomous-robots.

Østensen, Åse Gilje. 'In the business of peace: the political influence of private military and security companies on UN peacekeeping.' *International Peacekeeping* 20, no. 1 (2013): 33-47. DOI: http://dx.doi.org/10.1080/13533312.2012.761872.

Pandya, Jayshree. 'The Dual-Use Dilemma of Artificial Intelligence'. Forbes. January 7th, 2019. Accessed November 25th, 2021. Available at: https://www.forbes.com/sites/cognitiveworld/2019/01/07/the-dual-use-dilemma-of-artificial-intelligence/?sh=4ead7e8a6cf0

Paul, Kari. 'Letter signed by Elon Musk demanding AI research pause sparks controversy.' *The Guardian*. Accessed June 21st, 2023. Available at: April 1st, 2023.

https://www.theguardian.com/technology/2023/mar/31/ai-research-pause-elon-musk-chatgpt.

Payne, Kenneth. 'Artificial Intelligence: A Revolution in Strategic Affairs?' *Survival* 60, no. 5 (2018): 7-32. DOI: 10.1080/00396338.2018.1518374.

PAX. 'Lethal autonomous weapon systems and the tech sector: some examples of best practices'. *PAX*. August 19th, 2019. Accessed June 22nd, 2023. Available at: https://paxforpeace.nl/news/lethal-autonomous-weapon-systems-and-the-tech-sector-some-examples-of-best-practices/.

PAX. 'Major Tech Companies may be putting world at risk from Killer Robots'. *PAX*. August 19th, 2019. Accessed June 1st, 2023. Available at: https://paxforpeace.nl/news/major-tech-companies-may-be-putting-world-at-risk-from-killer-robots/.

Petrenko, Anton. 'Between Berserksgang and the Autonomous Weapons Systems.' *Public Affairs Quarterly* 26, no. 2 (2012): 81–102.

Ponciano, Jonathan. 'The World's Largest Technology Companies In 2023: A New Leader Emerges'. *Forbes*. June 8th, 2023. Accessed June 20th, 2023. Available at: https://www.forbes.com/sites/jonathanponciano/2023/06/08/the-worlds-largest-technology-companies-in-2023-a-new-leader-emerges/.

Poulson, Jack. 'Reports of a Silicon Valley/Military Divide Have Been Greatly Exaggerated'. *Tech Inquiry*. July 7th, 2020. Accessed June 19th, 2023. Available at: https://techinquiry.org/SiliconValley-Military/.

Roff, Heather M. 'The Strategic Robot Problem: Lethal Autonomous Weapons in War.' *Journal of Military Ethics* 13, no. 3 (2014): 211-227. DOI: 10.1080/15027570.2014.975010.

Rosert, Elvira and Frank Sauer. 'Prohibiting Autonomous Weapons: Put Human Dignity First'. *Global Policy* 10, no. 3 (2019): 370-375. DOI: https://doi.org/10.1111/1758-5899.12691.

Schieman, Kevin. 'The Soldier's Share: Considering Narrow Responsibility for Lethal Autonomous Weapons'. *Journal of Military Ethics* 3 (2023): 228-245. DOI: 10.1080/15027570.2023.2166448.

Schwartz, Barry. 'Google Now A Verb In The Oxford English Dictionary'. *Search Engine Watch*. June 29th, 2006. Accessed June 22nd, 2023. Available at: https://www.searchenginewatch.com/2006/06/29/google-now-a-verb-in-the-oxford-english-dictionary/.

Shane, Scott and Daisuke Wakabayashi. 'Google Will Not Renew Pentagon Contract That Upset Employees'. *The New York Times*. June 1st, 2018. Accessed June 19th, 2023. Available at: https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html.

Singer, Peter W. 'Corporate Warriors: The Rise of the Privatized Military Industry and Its Ramifications for International Security.' *International Security* 26, no. 3 (2001): 186–220.

Sparrow, Robert. 'Robots and Respect: Assessing the Case Against Autonomous Weapon Systems'. *Ethics & International Affairs* 30, no. 1 (2016): 93-116. DOI: 10.1017/S0892679415000647.

Stop Killer Robots. Accessed June 1st, 2023. Available at: https://www.stopkillerrobots.org/about-us/.

Tannenwald, Nina. 'Stigmatizing the Bomb: Origins of the Nuclear Taboo.' *International Security* 29, no. 4 (2005): 5–49.

Taylor, Isaac. 'Who Is Responsible for Killer Robots? Autonomous Weapons, Group Agency, and the Military-Industrial Complex.' *Journal of Applied Philosophy* 38, no. 2 (2021): 320-334. DOI: https://doi.org/10.1111/japp.12469.

Toh, Michelle. '300 million jobs could be affected by latest wave of AI, says Goldman Sachs.' *CNN Business*. March 29th, 2023. Accessed June 20th, 2023. Available at: https://edition.cnn.com/2023/03/29/tech/chatgpt-ai-automation-jobs-impact-intl-hnk/index.html.

Verbruggen, Maaike. 'The Role of Civilian Innovation in the Development of Lethal Autonomous Weapon Systems'. *Global Policy* 10, no. 3 (2019): 338-342. DOI: https://doi.org/10.1111/1758-5899.12663.

Wolfe, Liz. '*The New York Times* Is Wrong About the 'Myth of Big Tech Competence'. Still, Facebook should not have allowed its VIPs to flout the rules it claimed applied to everyone.' *Reason*. September 9th, 2021. Accessed June 20th, 2023. Available at: https://reason.com/2021/09/16/the-new-york-times-is-wrong-about-the-myth-of-big-tech-competence/.

Zhang, Baobao, et al. 'Ethics and governance of artificial intelligence: Evidence from a survey of machine learning researchers'. *Journal of Artificial Intelligence Research 71* (2021): 591-666.