Transcending the fog of war? US military 'AI', vision, and the emergent post-scopic regime

Hendrik Huelss 厄

Department of Political Science and Public Management, University of Southern Denmark, Odense M, Denmark Email: huelss@sam.sdu.dk

(Received 2 March 2023; revised 3 May 2024; accepted 8 May 2024)

Abstract

The integration of 'AI' technologies into weapon systems introduces a complex dimension to international relations and security, championing technological solutions for enduring warfare challenges, notably enhancing 'situational awareness' through advances such as automated 'vision'. However, the discourse, particularly in Western militaries like that of the United States, often overlooks inherent limitations and issues in AI-based warfare. This paper explores 'AI's' implications for military vision by *inter alia* scrutinising the US military's Joint All-Domain Command and Control (JADC2) process. It argues that the US military actively transforms the observation, decision, and action apparatus, progressively substituting human vision and decision-making, leading to a multidimensional de-visualisation. This denotes fundamental changes in human perception, reshaping knowledge, control, and agency dynamics. In conclusion, the paper suggests an imminent era of de-visualisation in the military – a deliberate relinquishment of human control for perceived military efficiency and effectiveness. This marks a transformative shift, urging nuanced consideration of the profound impact of 'AI' technologies on warfare dynamics.

Keywords: AI; military; scopic regime; vision

Introduction

Technological advances in the civilian and military sectors comprising 'AI' (artificial intelligence) are progressing at pace. In political and public discourse, the military transformation associated with automatisation, technological autonomy, and algorithms is framed by a discourse that, for example, argues for an inevitable 'AI' arms race¹ and underlines the superiority of 'AI' made to finally overcome human limitations. As the March 2021 final report of the US National Security Commission on Artificial Intelligence (NSCAI), put it, 'the ability of a machine to perceive, evaluate, and act more quickly and accurately than a human represents a competitive advantage in any field – civilian or military'.² This call to 'AI' arms promoted by segments of the political and think tank community as well as the industry is not only remarkable because it leaves aside a substantial academic-political debate on the limitations and risks of using military AI such as autonomous weapon systems (AWS).³ It also portrays the technological capabilities, referring chiefly to machine

¹Matt Bartlett, 'The AI arms race in 2020' (16 June 2020), Towards Data Science, available at: {https://towardsdatascience. com/the-ai-arms-race-in-2020-e7f049cb69ac}; Edward Moore Geist, 'It's already too late to stop the AI arms race – we must manage it instead', *Bulletin of the Atomic Scientists*, 72:5 (2016), pp. 318–21.

²NSCAI, 'National Security Commission on Artificial Intelligence final report' (2021), p. 7, available at: {https://www.nscai.gov/2021-final-report/}.

³In the definition of the International Committee of the Red Cross (ICRC), 'Autonomous weapon systems select and apply force to targets without human intervention. After initial activation or launch by a person, an autonomous weapon system

© The Author(s), 2024. Published by Cambridge University Press on behalf of The British International Studies Association. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

learning (ML) in combination with different platforms, as unequivocally advanced, reliable, and preferable. What is this supposed to mean in practice?

Since the introduction of the influential OODA loop (Observe, Orient, Decide, Act) by US Air Force Colonel John Boyd in 1986, the US military is sounding out ways to improve its decision-making framework. Perception, the ability to become aware of information based on the senses, is central to the initial observation stage. Over the past 20 years, the technological promise to prevail in the perennial struggle to gain complete 'situational awareness' in military terms is particularly boosted by the proliferation of platforms such as drones and software that are meant to close the gaps between the OODA stages evermore. Ultimately, this development comes with the promise of 'lifting the fog of war'⁴ – historically pointed out by Carl von Clausewitz – in the literal rather than in the metaphorical sense.^{5,6} As two of the main protagonists of the US narrative about the promises of military 'AI' shaped at the interstice of government and industry – Eric Schmidt and Robert O. Work – put it, 'one key change is that militaries will have great difficulty hiding from or surprising one another. Sensors will be ubiquitous ... Machines can also serve as the "eyes and ears" of their human teammates.⁷

The augmentation of the limited human senses of perception by using technology to 'observe' is a century-old undertaking. For that reason, observation in the sense of 'seeing' or 'vision' in the context of security, military, and warfare is an important research field for theoretically motivated studies in International Relations (IR) and security studies.

More specifically, there is a substantial body of literature on vision in the context of drone warfare.⁸ This literature has highlighted the implications of a scopic regime that according to Maurer 'refers in this context to the drone's visual framing, i.e. its ocular operations of capture, its optical perspective on the target, the visual sensing of the drone and its controller, the target's range of vision, as well as the representation of drones in social and aesthetic discourses.⁹ A scopic regime is hence about established forms of seeing, perceiving, and deciding in the context of technological augmentation, but also about establishing 'truth claims', in the words of Allen Feldman.¹⁰ Here, the ocular-centrism of 'the eye turned into a weapon'¹¹ is represented by the repeated evocation of the all-seeing 'eye of God' analogy and amplified by the US military practice of mystifying systems by

⁷Eric Schmid, and Robert O. Work, 'How to stop the next world war', *The Atlantic* (5 December 2022), available at: {https:// www.theatlantic.com/ideas/archive/2022/12/us-china-military-rivalry-great-power-war/672345/}.

⁸Antoine Bousquet, 'Lethal visions: The eye as function of the weapon', *Critical Studies on Security*, 5:1 (2017), pp. 62–80; Kyle Grayson and Jocelyn Mawdsley, 'Scopic regimes and the visual turn in International Relations: Seeing world politics through the drone', *European Journal of International Relations*, 25:2 (2019), pp. 431–57; Derek Gregory, 'From a view to a kill: Drones and late modern war', *Theory, Culture & Society*, 28:7–8 (2011), pp. 188–215; Katharine Hall Kindervater, 'The technological rationality of the drone strike', *Critical Studies on Security*, 5:1 (2017), pp. 28–44; Kathrin Maurer, 'Visual power: The scopic regime of military drone operations', *Media, War & Conflict*, 10:2 (2017), pp. 141–51.

⁹Maurer, 'Visual power', p. 142.

¹⁰'A scopic regime is an ensemble of practices and discourses that establish truth claims, typicality, and credibility of visual acts and objects and politically correct modes of seeing'. Feldman, cited in Grayson and Mawdsley, 'Scopic regimes and the visual turn in International Relations', p. 438.

¹¹Grégoire Chamayou, *Drone Theory* (London: Penguin Books, 2015), p. 11; see Oliver Müller, "An eye turned into a weapon": A philosophical investigation of remote controlled, automated, and autonomous drone warfare, *Philosophy & Technology*, 34 (2021), pp. 875–96.

self-initiates or triggers a strike in response to information from the environment received through sensors and on the basis of a generalized "target profile". This means that the user does not choose, or even know, the specific target(s) and the precise timing and/or location of the resulting application(s) of force? ICRC, 'ICRC position on autonomous weapon systems' (12 May 2021), available at: {https://www.icrc.org/en/document/icrc-position-autonomous-weapon-systems}.

⁴William A. Owens and Edward Offley, *Lifting the Fog of War* (Baltimore, MD: Johns Hopkins University Press, 2001).

⁵See Michael J. Shapiro, 'The fog of war', Security Dialogue, 36:2 (2005), pp. 233–46.

⁶Von Clausewitz's central argument in 'On War' (trans. 1873) is that '[w]ar is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty. A sensitive and discriminating judgment is called for; a skilled intelligence to scent out the truth.'

naming them Gorgon Stare or ARGUS-IS.¹² The argument of the omnipresent 'martial'¹³ gaze, of the 'militarized regime of hypervisibility'¹⁴ as a 'fetishized drone vision'¹⁵ is central to the narrative of an omnivoyant, impenetrable, and infallible military instrument that only becomes more powerful the more sophisticated AI is. As Paul Virilio argued in a literary prelude to the algorithmic warfare of the present, 'it is a war of images and sounds, rather than objects and things, in which winning is simply a matter of not losing sight of the opposition. The will to see all, to know all, at every moment, everywhere, the will to universalised illumination: a scientific permutation on the eye of God which would forever rule out the surprise, the accident, the irruption of the unforeseen.'¹⁶

Virilio also highlighted here a crucial link between seeing and knowing that is also reflected in studies on the military scopic regime in the broad sense. Vision as the most central element of perception is the basis of what Bousquet calls the 'martial gaze that threatens anything that falls under it with obliteration', which presents as 'a convergence of perception and destruction' in the 'struggles over visibility across planetary battlespaces'.¹⁷

At the same time, battlefield 'vision' as the basis of observing and knowing is transforming and losing the character it had for thousands of years. The human–machine teaming that is referred to in the above quote by Schmidt and Work is increasingly about supplementing and partly replacing the human input into all OODA stages – to a different extent – with AI applications. We are therefore also encountering a complex transformation of fundamental elements of military agency. This transformation requires a comprehensive consideration of AI implications for the interrelated stages of the loop.

Here, the paper's basic questions are: how does AI change military 'observation' and what implications does it have for the conceptualisation and role of 'vision' in the context of an action loop?

Analytically-theoretically, the paper addresses how the scopic regime as captured conceptually by international security scholarship is contested by what I call a process of 'de-visualisation'. This process is part of a new, powerful regime where seeing is no longer the ultimate basis of knowing (as well as deciding and acting). De-visualisation thereby denotes, first, the decreasing role of human vision, both as a direct and as an electronically mediated observation. Second, it underlines the selective process of algorithmic non-seeing as well as, third, representing counter-acts of de-visualising or disturbing non-human vision, which changes practices of camouflaging and hiding.¹⁸ Moreover, the current transformation of use of force practices from alleged hypervisibility to the de-visualisation associated with an 'algorithmic fog of war'¹⁹ results in a diminished capacity for human control, where seeing is an equally important but underconceptualised basis for knowing.

De-visualisation not only transcends the seeing-knowing-action nexus but also decisionmaking as a process. Military AI could arguably 'be used to help reduce risks to civilians in military operations, such as by ... automating target identification, tracking, selection, and engagement to

¹²See Chamayou, *Drone Theory*, pp. 37–8; Caren Kaplan, 'Drones and the image complex: The limits of representation in the era of distance warfare', in Armina Pilav, Marc Schoonderbeek, Heidi Sohn, and Aleksander Stanišić (eds), *Mediating the Spatiality of Conflicts: International Conference Proceedings* (Delft: BK Books, 2020), pp. 29–43; Max Liljefors, 'Omnivoyance and blindness', in Max Liljefors, Gregor Noll, and Daniel Steuer (eds), *War and Algorithm* (London: Rowman & Littlefield, 2019), pp. 127–63.

¹³Antoine J. Bousquet, *The Eye of War: Military Perception from the Telescope to the Drone* (Minneapolis: University of Minnesota Press, 2018), p. 2.

¹⁴Gregory, 'From a view to a kill', p. 193; see Maurer, 'Visual power'.

¹⁵Anna Jackman, 'Visualizations of the small military drone: Normalization through "naturalization", *Critical Military Studies*, 8:4 (2022), pp. 339–64.

¹⁶Paul Virilio, *The Vision Machine* (Bloomington: Indiana University Press, 1994), p. 70.

¹⁷Bousquet, *The Eye of War*, pp. 2–3.

¹⁸On hiding, see Bousquet, The Eye of War, pp. 153-89.

¹⁹Will Knight, 'The fog of AI war', MIT Technology Review, 122:6 (2019), pp. 44-7.

improve speed, precision, and accuracy²⁰ But the materialisation of what Virilio calls the '*sight-less vision*²¹ of a 'vision machine' constitutes, in fact, a direct challenge to the omniscient 'gaze' narrative. In contrast to this narrative, the putative superior 'martial gaze' defined as 'the entire range of sensorial capabilities relevant to the conduct of war²² of systems can translate into human *un*awareness in the use of force. This is not only relevant for weapon systems that can potentially apply force without prior human assessment, but also in the context of human–machine teaming that is already an everyday operational reality. Human–AI teaming promises to realise the vision of omniscience by implying 'a massive increase in situational awareness, it allows things to go faster, it helps mitigate the chances of human mistakes,²³ as Pentagon's then director of the US Joint Artifical Intellgigence Center (JAIC) Lt General Jack Shanahan put it.

The empirical background of the paper are the current developments regarding the US Joint All-Domain Command and Control (JADC2) strategy to exemplify the move towards a novel, integrated sensory-action loop. JADC2 is supposed to be an AI-integrative 'coherent approach for shaping future Joint Force C2 [command and control] capabilities and is intended to produce the warfighting capability to sense, make sense, and act at all levels and phases of war, across all domains, and with partners, to deliver information advantage at the speed of relevance'.²⁴ In that, it is also meant as a substantial reformation of the existing OODA cycle by compressing the four stages of observe, orient, decide, and act into three accelerated and interrelated dimensions of sense, make sense, and act, which are based on integrating autonomous AI elements. JADC2 shows that the process of de-visualisation is complex and comprehensive, going beyond the former observation stage.

The paper unfolds as follows: in the first section, the discussion delves into the realm of vision within the context of military AI, elucidating the research problem at hand. Additionally, it provides an overview of the pertinent existing literature. The subsequent section illuminates the JADC2 initiative, serving as a concrete illustration of the AI-induced transformation of the well-established observation, orientation, decision, and action loop within the US military. Moving to the third section, the paper introduces its theoretical contribution by articulating the concept of de-visualisation. The fourth section articulates how the development and utilisation of AI-driven technologies inherently revolutionise the concept of vision with consequences for human control and agency. The fifth section extrapolates the implications of an emerging algorithmic fog of war for the lofty promises of attaining ultimate omniscience. The paper's discussion is rounded off with a conclusion.

Seeing, knowing, and doing in war

Since the early 2000s, research on observation and action in the context of military technology is dominated by studies on drone warfare.²⁵ The expansion of drone warfare that started with the launch of the US-led operation in Afghanistan in 2001 marks the rising importance of remotely

²⁰US Mission to the UN Geneva, 'Agenda item 5(d). Review of potential military applications of related technologies. Statement from the 2020 CCW group of governmental experts on lethal autonomous weapon systems' (2020), available at: {https://reachingcriticalwill.org/images/documents/Disarmament-fora/ccw/2020/gge/statements/24Sept_US.pdf}.

²¹Virilio, The Vision Machine, p. 59.

²²Bousquet, The Eye of War, p. 11.

²³US Department of Defense, 'Lt. Gen. Jack Shanahan media briefing on A.I.-related initiatives within the Department of Defense' (30 August 2019), available at: {https://www.defense.gov/Newsroom/Transcripts/Transcript/Article/1949362/lt-genjack-shanahan-media-briefing-on-ai-related-initiatives-within-the-depart/}.

²⁴US Department of Defense, 'Summary of the Joint All-Domain Command & Control (JADC2) Strategy' (2022), p. 1, available at: {https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.PDF}.

²⁵E.g. John Kaag and Sarah Kreps, *Drone Warfare* (Cambridge: Polity Press, 2014); Chamayou, *Drone Theory*; Max Byrne, 'Consent and the use of force: An examination of "intervention by invitation" as a basis for US drone strikes in Pakistan, Somalia and Yemen', *Journal on the Use of Force and International Law*, 3:1 (2016), pp. 97–125; Hugh Gusterson, *Drone: Remote Control Warfare* (Cambridge, MA: MIT Press, 2016); Gregory, 'From a view to a kill'. conducted warfare as a central pillar of deploying military force in the 21st century. The large-scale usage of drones in Iraq, Ukraine, Syria, and Yemen, among other places, and most recently in the Russia–Ukraine war, has changed the way force is projected, perceived, and thought. Optimising the identification, selection, and attack of targets based on novel modes of visualisation is at the core of these military efforts. Schwarz aptly summarises the dominant, positive outlook in the military associated with these developments: 'drones offer a visual technology that enables the collection of data, facilitates diagnostic analysis and is able to administer a course of action in specific situations of conflict with minimal risk to the operators overseeing the use of the technology'.²⁶ 'Vision' should be understood here in the broadest sense of the term, as drones can work as and interact with multi-sensory systems that take in visual but also electronic or audio data.

Drones as remotely controlled uninhabited aerial vehicles (UAVs) are often understood as an extension or an augmentation of humans in terms of vision and action. Control becomes hybrid – humans are no longer necessarily present in the physical space where the use of force takes place, while their vision and ultimately their agency are embodied and hyper-present in an electronically mediated from. The images delivered in real time by UAVs might be regarded and favoured as 'an enhanced, improved, extended, sober and ostensibly neutral version of human vision²⁷. However, drone vision is both an extension and a contraction of vision as well as of space and time. Detailed view, zoom, surveillance, and landscape modes, and various angles promise to deliver what the human eye cannot gather; the distance between the human operator and the target increases tremendously and is often transcontinental; at the same time, close surveillance over prolonged periods produces an unseen intimacy between operator and target, while drone footage is still often of remarkably low definition.²⁸

Drone vision should hence be understood as simultaneously an enhancement and an exacerbation of human sight and perception. The emergence of (armed) drones has therefore contributed to the, for some, panoptic, for others, promising, prospect of total surveillance. Scholarship on novel forms of (drone) vision in warfare has noted that 'there is the potential to see more than can possibly be seen at any given time by human observers.²⁹

The data amassed by drones is not only vast in scope and quantity but also characterised by a distinct paradigm of perception. The multi-sensory capabilities of drones offer a unique way of seeing, encompassing not just what is observed but also what may be intentionally omitted by sensors. This approach extends beyond a pursuit of absolute knowledge or control, emphasising a nuanced perspective that involves seeing differently, not being seen, and, notably, not seeing.

Current developments aimed at incorporating AI into weapons technologies can be understood as a step towards rectifying the human limitations that are still present with drone vision regarding the quantity of data that slows down decision-making and acting. But the techno-optimism reflected in parts of the military and industry discourse does not sufficiently consider the limitations of vision in the interaction of humans and technologies. This is contrary to the military focus on technologically 'lifting' the Clausewitzian 'fog of war'³⁰ by finding a tech solution for gaining ultimate situational awareness.³¹ Bringing 'light' to the 'darkness' of war is thereby tapping into a long-established narrative about the advantages of technological progress for seeing and knowing

²⁶Elke Schwarz, 'Technology and moral vacuums in just war theorising', *Journal of International Political Theory*, 14:3 (2018), pp. 280–98 (p. 285).

³¹See Lucy Suchman, 'Algorithmic warfare and the reinvention of accuracy', *Critical Studies on Security*, 8:2 (2020), pp. 175–87.

²⁷Schwarz, 'Technology and moral vacuums', p. 288.

²⁸See Alex Adams, 'Death TV: Drone warfare in contemporary popular culture', Drone Wars UK (021), available at: {https://dronewars.net/wp-content/uploads/2021/03/DW-DeathTV-WEB.pdf}.

²⁹Grayson and Mawdsley, 'Scopic regimes and the visual turn in International Relations', p. 443.

³⁰Owens and Offley, *Lifting the Fog of War*; see Merel A. C. Ekelhof, 'Lifting the fog of targeting: "Autonomous weapons" and human control through the lens of military targeting, *Naval War College Review*, 71:3 (2018), pp. 61–94; Rune Saugmann, 'Military techno-vision: Technologies between visual ambiguity and the desire for security facts', *European Journal of International Security*, 4:3 (2019), pp. 300–21.

in the military. For example, Canadian troops used helicopters equipped with 'Nightsun' spotlights in Kosovo in the early 2000s. The following quote by Sergeant Robert Wheatley exemplifies this narrative of technology providing divine superiority: 'We did overwatch at night ... They could hear us at night, but they couldn't see us. We'd fly around blacked out. Other times we used Nightsun and it was all overt: it's like a big candle in the sky. The message was, we were like God, who's watching everything.³²

The algorithmic turn in warfare is meant to accelerate and complete this development towards a state of 'omnivoyance',³³ or rather omniscience,³⁴ that novel systems integrating AI technologies are supposed to provide. As a case in point, NSCAI Commissioner Ken Ford reportedly argued that 'AI gives commanders eyeglasses for the mind'.³⁵

We can therefore identify a specific scopic regime of military technovision that promotes the putative options offered by 'AI' as part of a further augmentation or replacement of human perception and importantly decision agency. Research has deconstructed the 'scopic regime of modernity'³⁶ in the context of drone vision. But the transition from the all-seeing system to a 'sight-less vision'³⁷ and to forms of algorithmically informed warfare that feature a new perception–action apparatus remain understudied. The current developments point to a reverse trend of giving away sight and control in warfare in the form of what could be called a post-scopic regime. This does not mean that human vision ceases to play a role. But human–machine interaction is increasingly complex, and human agency increasingly diminished. This concerns particularly developments in computer vision³⁸ and machine learning (ML), especially in deep neural network (DNN) models that deal with unlabelled or unstructured data and are used for anomaly detection.^{39,40}

Research on military AI and the question of vision

In recent years, a substantial and growing body of research addresses the promises and pitfalls of military AI from ethical, legal, and normative perspectives interconnected with critical security studies. Most works consider the (emerging) normative framework that surrounds the implications of integrating AI in terms of autonomous weapon systems (AWS) into the practice of warfare.

³²Cited in Sean M. Maloney and Mike Jackson, *Operation Kinetic: Stabilizing Kosovo* (Lincoln, NE: Potomac Books, 2018), p. 241.

³³Liljefors, 'Omnivoyance and blindness'.

³⁴See Lucy Suchman, 'Imaginaries of omniscience: Automating intelligence in the US Department of Defense', *Social Studies of Science*, 53:5 (2023), pp. 761–86.

³⁵US Department of Defense, 'Honorable Robert O. Work, Vice Chair, National Security Commission on Artificial Intelligence, and Marine Corps Lieutenant General Michael S. Groen, Director, Joint Artificial Intelligence Center hold a press briefing on Artificial Intelligence' (4 September 2021), available at: {https://www.defense.gov/News/Transcripts/ Transcript/Article/2567848/honorable-robert-o-work-vicechair-national-security-commission-on-artificiali/https%3A% 2F%2Fwww.defense.gov%2FNews%2FTranscripts%2FTranscript%2FArticle%2F2567848%2Fhonorable-robert-o-work-vicechair-national-security-commission-on-artificial-i%2F}.

³⁶See Grayson and Mawdsley, 'Scopic regimes and the visual turn in International Relations'; Gregory, 'From a view to a kill'.

³⁷Virilio, *The Vision Machine*.

³⁸Computer vision enables systems to classify visual data such as images or video footage. It often uses the technique of deep learning to generate neural networks that analyse visual data. The military aim is to develop systems that can identify and classify objects in digital imagery and then react to such data based on machine learning.

³⁹Supervised or semi-supervised learning algorithms work with labelled training data based on input variables and desired output variables. They can 'learn' to predict the outputs for inputs even in cases where the input was not part of the training data (semi-supervised). Learning is supervised when the correct output is known. Unsupervised learning algorithms work with data sets that only consist of unlabelled input and 'learn' about underlying patterns in the unstructured input data. The correct output is unknown. See Jason Brownlee, 'Supervised and unsupervised machine learning algorithms', *Machine Learning Mastery* (blog) (15 March 2016), available at: {https://machinelearningmastery.com/supervised-and-unsupervised-machine-learning-algorithms/}.

⁴⁰See Claudia Aradau and Tobias Blanke, 'Governing others: Anomaly and the algorithmic subject of security', *European Journal of International Security*, 3:1 (2018), pp. 1–21.

The political background of this debate are discussions in the United Nations' framework of the Convention on Certain Conventional Weapons (CCW) since 2014 that are critically observed by academia and NGOs. The current formation of the 'Group of Governmental Experts (GGE) on emerging technologies in the area of lethal autonomous weapons systems (LAWS)' is sounding greatly divergent viewpoints on the characteristics as well as regulation or prohibition possibilities of such systems. A more detailed review of research on AWS is beyond the scope of this paper. More importantly, it should be noted that questions of visualisation and de-visualisation are rarely in the research focus. This is noteworthy because there is significant reflection on the question of human control over AI or AWS in this case in the academic and political debate. State parties and NGOs have contributed here by introducing concepts such as 'meaningful human control⁴¹ or 'appropriate levels of human judgment over the use of force'⁴² into the debate, the latter being the standard human control definition of the US government for over a decade. Apart from controversy about important key terms, such as a definition of what autonomy, appropriate, meaningful, control, or judgement could mean, and the resulting lack of universally shared understandings, the question of human control seems to be intricately linked also to vision as a foundation of human agency. Wilke, for example, argues how military agency in terms of targeting and other aspects that are an outcome of observation are traditionally based on 'professional vision'. This is taken up by Suchman, Follis, and Weber, who posit that 'panoptic aspirations to situational awareness are instantiated instead as highly formatted and constrained modes of professional vision⁴³. The transformation of this professional military vision by military AI is not yet well accounted for in the research literature.

In the interaction of humans and AI, agency becomes 'distributed'⁴⁴ and turns into a complex system of human and non-human agentic elements that sense, make sense, and act, to use the terminology of JADC2. We are facing here a new regime of sensing that is very much influenced by a de-visualisation of what has been previously conceptualised as professional vision in the military context. At the same time, de-visualisation goes beyond the 'visual crises'⁴⁵ that are an outcome of bringing together human mindsets and vision technologies, as human vision and agency can be partly replaced altogether.

In the following section, I will take a closer look at JADC2 as an example of the new concept of a distributed agency. Thereafter, I will present the three different stages of visualisation/de-visualisation as outlined in the introduction.

A new perception-action apparatus (JADC2)

The launch of the JADC2 initiative is part of the US military focus on the role and importance of data. As noted by the 2020 Department of Defense (DoD) Data Strategy, 'The DoD now recognizes that data is a strategic asset that must be operationalized in order to provide a lethal and effective Joint Force that, combined with our network of allies and partners, sustains American influence

⁴¹Article 36, 'Killing by machine: Key issues for understanding meaningful human control' (9 April 2015), available at: {http://www.article36.org/autonomous-weapons/killing-by-machine-key-issues-for-understanding-meaningfulhuman-control/; UNIDIR, 'The weaponization of increasingly autonomous technologies: Considering how meaningful human control might move the discussion forward', UNIDIR Resources (2014), available at: {https://unidir.org/publication/ weaponization-increasingly-autonomous-technologies-considering-how-meaningful-human}; Heather M. Roff and Richard Moyes, 'Meaningful human control, Artificial Intelligence and autonomous weapons. Briefing paper prepared for the informal meeting of experts on lethal autonomous weapons systems. UN Convention on Certain Conventional Weapons', Geneva (2016).

⁴²US Department of Defense, 'Directive 3000.09 on autonomy in weapon systems' (2012), p. 2.

⁴³Lucy Suchman, Karolina Follis, and Jutta Weber, 'Tracking and targeting: Sociotechnologies of (in)security', *Science, Technology, & Human Values*, 42:6 (2017), pp. 983–1002 (p. 990).

⁴⁴Werner Rammert, 'Where the action is: Distributed agency between humans, machines, and programs', in Uwe Seifert, Jin Hyun Kim, and Anthony Moore (eds), *Kultur- Und Medientheorie*, 1st ed. (Bielefeld: transcript Verlag, 2008), pp. 62–91.

⁴⁵Christiane Wilke, 'Seeing and unmaking civilians in Afghanistan: Visual technologies and contested professional visions', *Science, Technology, & Human Values,* 42:6 (2017), pp. 1031–60 (p. 1033).

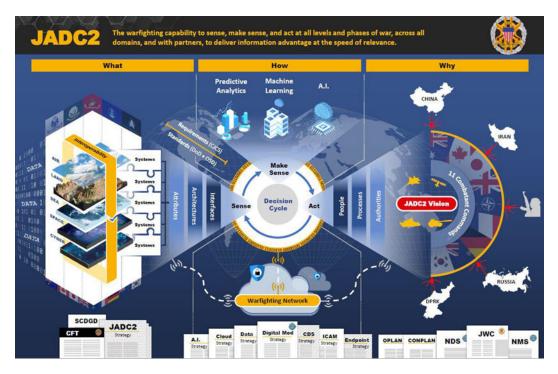


Figure 1. JADC2 overview.^a ^aSource: US Department of Defense, 'Summary of JADC2', p. 3.

and advances shared security and prosperity.⁴⁶ The future vision of the strategy is that the 'DoD is a data-centric organization that uses data at speed and scale for operational advantage and increased efficiency.⁴⁷ JADC2 is an attempt to translate this vision to the operational level by creating a complex network of sensor input, unified data storage and data access, hardware platforms, and actors that allows the informing of real-time decision-making. It was made public in the DoD 'Summary of the Joint All-Domain Command & Control (JADC2) strategy' in March 2022.

Crucially, 'JADC2 provides a coherent approach for shaping future Joint Force C2 capabilities and is intended to produce the warfighting capability to sense, make sense, and act at all levels and phases of war, across all domains, and with partners, to deliver information advantage at the speed of relevance^{'48} The JADC2 vision is depicted in Figure 1 below. It shows the complexity of the system that aims at integrating input from all domains, different platforms, and actors into a new decision cycle that is importantly governed by AI applications such as ML.

The major transformation that JADC2 means for the decision process is the use of AI to achieve 'human on the loop' (supervising algorithmic decision-making) or even 'human out of the loop' (algorithmic decision-making without human supervision) applications in certain parts that contrast with the traditional human in the loop concept of the OODA loop, where human are active decision-makers on different stages.⁴⁹

The information that is yet available on JADC2 is limited. The 2022 strategy paper outlines in general that "Sense and integrate" is the ability to discover, collect, correlate, aggregate, process, and

⁴⁶US Department of Defense, 'DoD data strategy' (2020), p. i, available at: {https://media.defense.gov/2020/Oct/08/ 2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF}.

⁴⁷US Department of Defense, 'DoD data strategy', p. 2.

⁴⁸US Department of Defense, 'Summary of the Joint All-Domain Command & Control (JADC2) strategy', p. 2.

⁴⁹Noel Sharkey, 'Staying in the loop: Human supervisory control of weapons', in Nehal Bhuta, Susanne Beck, Robin Geiβ et al. (eds), *Autonomous Weapons Systems* (Cambridge: Cambridge University Press, 2016), pp. 23–38.

exploit data from all domains and sources (friendly, adversary, and neutral), and share the information as the basis for understanding and decision-making', while "'Make Sense" refers to analyzing information to better understand and predict the operational environment and the actions and intentions of an adversary, as well as the actions of our own and friendly forces'.⁵⁰ Important to note in the 'make sense' category is also the central role AI/ML is supposed to play in the reformation of OODA: 'JADC2 developed capabilities will leverage Artificial Intelligence and Machine Learning to help accelerate the commander's decision cycle. Automatic machine-to-machine transactions will extract, consolidate and process massive amounts of data and information directly from the sensing infrastructure.'⁵¹ There is therefore a clear intention to automate the central elements of sensing and making sense. I understand this development as a move that results in a broad devisualisation. While human vision as 'seeing' that is coupled with 'knowing' based on sensory input plays and will play a role in the future, 'vision' is meant to be largely replaced by AI-driven 'sense' and 'sense making' due to data load and the importance of speed. It is here at the point of data analytics conducted by ML where ocular assessments and human processing are being replaced and lost.

Roberts summarised the JADC2 vision succinctly as follows: 'in simple terms, that JADC2 aims to network everything military (and some non-military stuff too), run it through some AI and ML, and deliver the Joint Force commander a set of recommendations at a speed faster than an adversary can act or react.⁵² In this theoretical example, the commander will still access 'recommendations' based on the visual sense, but this concept of vision is very different from the observation (as well as orientation and decision) of the OODA loop that also summarised military practices of the past centuries.

The JADC2 perspective is the background of the military transformation currently taking place by including AI in imaginations of future warfare. The following section will shed more light on the process and three dimensions of de-visualisation that are arguably an important part of this transformation.

Military vision between visualisation and de-visualisation

The transformation of military vision is part of the US defence AI initiative. The USA as the leading developer of military AI has invested significantly in relevant technology. In recent years, the US military – in acceptance of the seemingly inevitable 'race for AI supremacy'⁵³ vis-à-vis China and Russia – has spent billions on the research and development of algorithmic warfare. The DoD fiscal year 2023 budget proposal submitted to Congress in March 2022 requested more than 130.1 billion USD for research and development and earmarks 1.1 billion USD for 'AI', in addition to 11.2 billion USD funding for 'cybersecurity'.⁵⁴ Bloomberg Government 'found the Pentagon is seeking a combined \$5.2 billion in FY-21 for 319 research and development programs with "some AI/ML component", up from \$4 billion in DOD's FY-20 budget request,⁵⁵ while the Pentagon spent

⁵⁰US Department of Defense, 'Summary of JADC2 strategy', p. 4.

⁵⁵Justin Doubleday, 'New analysis finds Pentagon annual spending on AI contracts has grown to \$1.4B', InsideDefense.com (24 September 2020), available at: {https://insidedefense.com/insider/new-analysis-finds-pentagon-annual-spending-ai-contracts-has-grown-14b}.

⁵¹US Department of Defense, 'Summary of JADC2 strategy', p. 4.

⁵²Peter Roberts, 'JADC2: Better or just faster?', Systematic A/S (20 July 2023), available at: {https://systematic.com/engb/ industries/defence/news-knowledge/blog/jadc2-better-or-just-faster/}.

⁵³NSCAI, 'National Security Commission on Artificial Intelligence final report', p. 7.

⁵⁴US Department of Defense, 'The Department of Defense releases the President's fiscal year 2023 defense budget' (28 March 2022), available at: {https://www.defense.gov/News/Releases/Release/Article/2980014/the-department-of-defense-releases-the-presidents-fiscal-year-2023-defense-budg/https%3A%2F%2Fwww.defense.gov%2FNews%2FReleases%2FRelease%2FArticle%2F2980014%2Fthe-department-of-defense-releases-the-presidents-fiscal-year-2023-defense-budg%2F}.

'an additional \$1.7 billion to \$3.5 billion for unmanned and autonomous systems' in 2020.⁵⁶ The NSCAI's final report to Congress advised to 'increase federal funding for non-defense AI R&D at compounding levels, doubling annually to reach \$32 billion per year by Fiscal Year 2026.⁵⁷

The role of ML in terms of deliberately decreasing human vision can be exemplified by US Department of Defense (DoD) projects such as 'the now-famous'58 image classification project Maven (Algorithmic Warfare Cross-Functional Team). Launched in 2017, Project Maven, repeatedly covered in recent IR research,⁵⁹ is precisely the attempt to develop deep learning models that can perform the 'vision' task on vast quantities of image data. It is a direct response to the limits human cognitive abilities pose to the efficiency of decision-making in military scenarios, predicated on comprehensive situational awareness. In the words of then JAIC director and project leader of Maven Jack Shanahan, Maven is a 'perception project' that is meant to 'automatically detect, classify, track and maybe provide a little bit extra information so that a human doesn't have to stare at a video screen for 11 hours at a time.⁶⁰ But what Maven is supposed to deliver goes beyond the role of a refined telescope. It provides an extensive level of human-machine interaction in form of a perception-action apparatus, where algorithms filter, detect, and highlight data under time constraints: as Shanahan explained, 'this is about, let the machines go through the data as fast as possible, make recommendations or - or options to an analyst, to a commander, to an operator. And it just gets through decision-making processes better and gives humans time back.²⁶¹ The close resemblance to elements of JADC2 are obvious. The argument is that computer vision coupled with suitable ML algorithms can make more accurate and faster detections, but also de facto decisions about the relevance of data.

The Maven technology processes 'traditional' images or video footage gathered by drone sensors, but deploying algorithmic screening marks a de-visualisation that is based on a completely different way of processing image data than human vision. ML is concerned with *statistical* pattern recognition in large data sets – the detection of anomalies.⁶² Even though human seeing and knowing based on vision still play a role when it comes to acting on pre-screened data, the question is to what extent the algorithmic representation produces the image instead of the image producing the algorithmic representation.

Further US projects like Skynet – a National Security Agency (NSA) surveillance programme using ML to analyse communications data in anti-terror operations that made headlines in 2015 – are precisely concerned with developing technical capabilities to use deep neural networks that can detect patterns or anomalies in data autonomously (unsupervised learning) to provide a response to the increasing complexity of data environments on the 'battlefield'.⁶³ These environments consist of a range of mixed and complex data, signals, and electronic emissions. The aim is to gain an advantage in processing such environments.

⁵⁶Jon Harper, 'China matching Pentagon spending on AI' (6 January 2022), available at: {https://www.nationaldefensemag azine.org/articles/2022/1/6/china-matching-pentagon-spending-on-ai}.

⁵⁸William Merrin and Andrew Hoskins, 'Tweet fast and kill things: Digital war', *Digital War*, 1:1 (2020), pp. 184–93 (p. 187). ⁵⁹Ingvild Bode and Hendrik Huelss, 'Autonomous weapons systems and changing norms in international relations', *Review of International Studies*, 44:3 (2018), pp. 393–413; Justin Haner and Denise Garcia, 'The artificial intelligence arms race: Trends and world leaders in autonomous weapons development', *Global Policy*, 10:3 (2019), pp. 331–7; Hendrik Huelss, 'Norms are what machines make of them: Autonomous weapons systems and the normative implications of human–machine interactions', *International Political Sociology*, 14:2 (2020), pp. 111–28; Sarah Kendall, 'Law's ends: On algorithmic warfare and humanitarian violence', in Max Liljefors, Gregor Noll, and Daniel Steuer (eds), *War and Algorithm* (London: Rowman & Littlefield, 2019), pp. 105–25; Schwarz, 'Technology and moral vacuums in just war theorising'; Suchman, 'Algorithmic warfare and the reinvention of accuracy'; Suchman, 'Imaginaries of omniscience'.

⁶⁰US Department of Defense, 'Lt. Gen. Jack Shanahan media briefing on A.I.-related initiatives'.

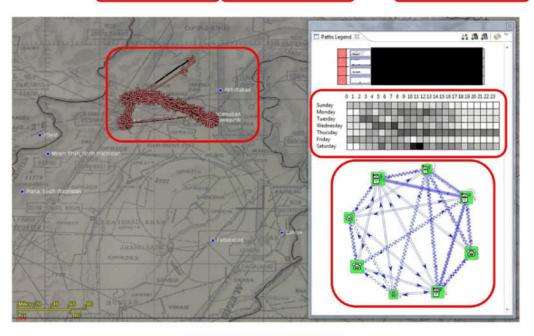
⁶¹US Department of Defense, 'Shanahan media briefing'.

⁶²See Aradau and Blanke, 'Governing others'; Huelss, 'Norms are what machines make of them'.

⁶³See Aradau and Blanke, 'Governing others'; Huelss, 'Norms are what machines make of them'; Jutta Weber, 'Keep adding: On kill lists, drone warfare and the politics of databases', *Environment and Planning D: Society and Space*, 34:1 (2016), pp. 107–25.

⁵⁷NSCAI, 'National Security Commission on Artificial Intelligence final report', p. 188.

From GSM metadata, we can measure aspects of each selector's pattern-of-life, social network, and travel behavior



TOP SECRET//COMINT//REL TO USA, FVEY

Figure 2. Visualisation of metadata by Skynet.^a

^aSource: The Intercept, 'SKYNET: Courier detection via Machine Learning' (2015), available at: {https://theintercept.com/document/2015/ 05/08/skynet-courier/}.

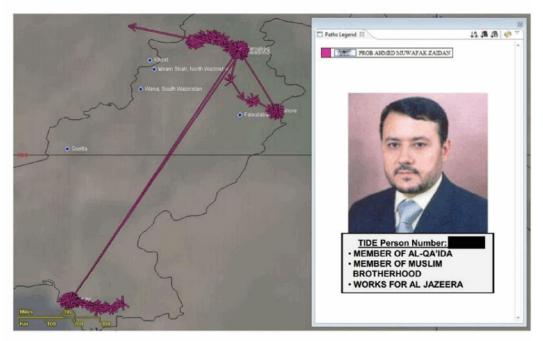
Details about Skynet were leaked by Edward Snowden and published on the website The Intercept. For Skynet, the NSA tested the detection of Al Qaeda couriers based on ML analysis of mobile phone metadata and resulting patterns of usage as well as travel. The visual output of this analysis is shown in Figure 2 below.

The metadata is here translated into a visual display of 'patterns of life' that also provides an interpretation of 'normal' and anomalous, suspicious behaviour. Based on these files, it was reported that the individual with the most suspicious profile was presented as Ahmad Muaffaq Zaidan (see Figure 3), who holds Syrian nationality and has served as the Islamabad bureau chief for Al Jazeera for an extended period. In the files, he was listed as a 'Member of Al-Qa'ida' and the 'Muslim Brotherhood'. But throughout his professional journey, Zaidan has dedicated his reporting to the Taliban and Al Qaeda, conducting numerous notable interviews with senior Al Qaeda figures, including Osama bin Laden.⁶⁴

The use of 'observation' or 'sensing' data that is in this case not based on video footage or photographic images but on data from the electromagnetic spectrum that is invisible to the human eye shows the first step towards a de-visualisation of a military perception-decision-action sequence. The computer output in the leaked examples is optimised to meet human expectations in seeing. It shows a mapped terrain and coloured lines, dots, and arrows that highlight directions of

⁶⁴Cora Currier, Glenn Greenwald, and Andrew Fishman, 'U.S. government designated prominent Al Jazeera journalist as "member of Al Qaeda", The Intercept (8 May 2015), available at: {https://theintercept.com/2015/05/08/u-s-government-designated-prominent-al-jazeera-journalist-al-qaeda-member-put-watch-list/}.

The highest scoring selector that traveled to Peshawar and Lahore is PROB AHMED ZAIDAN



TOP SECRET//COMINT//REL TO USA, FVEY

Figure 3. Visualisation of patterns of movement by Skynet.^a ^aSource: The Intercept, 'SKYNET: Courier detection via Machine Learning'.

travel and agglomerated stays. But the data is in this sense already highly filtered and structured. It provides not only a representation but also interpretation of reality in a visualisation of the nonvisual. The messiness of material and social interactions is sanitised into data points, clear surfaces, unquestionable lines and geometries. It is a representation signalling objectivity and neutrality. The visualisation is here based on making something visual – electromagnetic signals – that are created by humans and have never been directly observable like the image reflections of sunlight.

In the example above, the OODA loop has not necessarily collapsed, as there is no direct execution of 'sense making' into action based on AI. However, the confident presentation of Zaidan as a courier of a terrorist group already questions the extent to which 'meaningful human control' or agency is applied in the human–machine interaction.

The implication of visual representation of non-visual data such as mobile phone signals is related to the proliferation of interfaces in the security and military context but also beyond. In the words of Fedorova, 'in a conventional sense, or in relation to computational technologies, the interface is a place of connection between a human and a digital system that allows them to communicate with one another in order to generate and exchange information^{'65} and is based on visual presentations. In a broader perspective of initiatives such as JADC2, it can be argued that 'interfaces are situated devices designed in relation to political visions and imaginaries of control and power while being interactive, malleable, and adaptable,^{'66} as Maia put it.

⁶⁵Ksenia Fedorova, Tactics of Interfacing: Encoding Affect in Art and Technology (Cambridge, MA: MIT Press, 2020), p. 3.

⁶⁶Pedro Maia, 'The case for interfaces in International Relations', Global Studies Quarterly, 3:3 (2023), pp. 1–10 (p. 2).

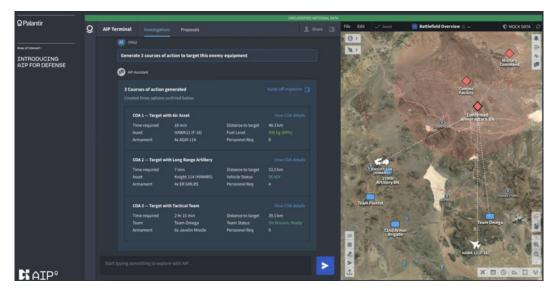


Figure 4. Palantir AIP interface.^a

^aSource: Video screenshot from Palantir, 'Palantir AIP for Defense' (2023), available at: {https://www.palantir.com/aip/defense/}.

Interfaces are a decades-old technology of translating machine data into output information that is understandable and usable by human actors. In the military context, platforms, systems, and weapons all have a type of interface that can be sophisticated or very simple. Regarding the studies on drone warfare referred to above, drone control stations are typical interfaces based on screen output and the real-time processing of different sensory inputs, most importantly video footage. In that, the interface is the technological artifact of the promise of transparency, full situational awareness, control, and agency.⁶⁷ The visual representation is also a truth claim about what is happening in a given situation and moment. At the same time, it stands for a further step in the de-visualisation process, where not only is the role of human vision in terms of 'observing' changing and of decreasing importance, but also ML is de-visualising due to the selective 'seeing' that the algorithm offers to the human operator. The sanitised interface is not fulfilling dreams of omniscience – rather they offer a limited representation of social reality by reducing data to what is processable by humans.

The most recent aim of the industry is to link visual interfaces with the emerging generative AI models (large language models) that are known as ChatGPT and similar applications in the civilian domain. The company Palantir is at the forefront of this development by presenting in April 2023 an Artificial Intelligence Platform (AIP) that runs large language models coupled with an interface. The image below (Figure 4) is a screenshot from a Palantir demo video of AIP. The operator can interact with AIP by asking questions and providing prompts in the way a chat between humans would generally take place. The fundamentally transformative aspect is that AIP also gives recommendations for actions that can be selected by the operator. Again, we see here a neat representation of the 'battlefield' that gives no reason or rather basis to 'doubt'⁶⁸ the algorithmic situational assessment that is cleared from all unnecessary noise of the old 'fog of war'. At the same time, important situational nuances and distinctions such as between combatants and non-combatants that could be much safer made in a slower and deliberative OODA loop seem to be disappearing in the new electronic fog of war.

⁶⁷See Maia, 'Case for interfaces', p. 2.

⁶⁸Louise Amoore, 'Doubt and the algorithm: On the partial accounts of machine learning', *Theory, Culture & Society*, 36:6 (2019), pp. 147–69.

These examples also underline the trend towards a realisation of the JADC2 vision, in which de-visualisation will be completed by removing human operators from immediate and high-speed decision-making. In this regard, it seems that military operators dealing 'with second-order visualisations of these sensor inputs'⁶⁹ based on interfaces are increasingly considered as the weak link in the military ambition to move through JADC2 at machine speed, which becomes an accepted view-point in the miliary discourse promoting AI 'solutionism'.⁷⁰ As the NSCAI's report puts it, 'the best human operator cannot defend against multiple machines making thousands of maneuvers per second potentially moving at hypersonic speeds and orchestrated by AI across domains. Humans cannot be everywhere at once, but software can.⁷¹ In the words of former DoD electronic warfare senior executive William Conley, 'a future battlespace will contain threat signals not previously observed, [so] it will be essential for many platforms to be executing real time decision algorithms.⁷²

The potential use of 'real time decision algorithms' could be seen as at the core of the debate about AWS, the limits of human agency, and whether decision-making takes place within the confines of 'meaningful human control' (MHC).⁷³ While the argument that 'the act of seeing is an act that proceeds action'⁷⁴ is certainly a fundamental epistemological base of past centuries, algorithmic warfare challenges this base because it promises to unify perception, decision, and action as outlined by JADC2: 'it involves new modes of weapons based on the annihilation of time.⁷⁵

This vision is putatively also fulfilled by Anduril Industries, which took over Project Maven after the withdrawal of Google due to internal protest in 2018. Anduril offers the 'Lattice Platform' as a command and control interface device. Here, 'Lattice accelerates complex kill chains by orchestrating machine-to-machine tasks at scales and speeds beyond human capacity'⁷⁶ – without elaborating on the question to what extent 'beyond human capacity' also means beyond human control. Anduril further explains that 'Lattice streamlines the complexity of the decision-making process by presenting decision points – not noise – and using deep learning models to present recommended decision support to operators'.⁷⁷ In that, 'Lattice cuts through the noise and creates a shared realtime understanding of the battlespace. It autonomously parses data from thousands of sensors & data sources into an intelligent common operating picture in a single pane of glass.⁷⁸

Professing trust in AI 'solutions' to long-standing problems of warfare that originate in human limitations deliberately contributes to a de-visualisation in war. The superiority of AI systems in terms of speed and accuracy is valued more than the fundamental role that human vision has played in warfare as a mechanism of knowing followed by decision and acting over centuries. At the same time, the discourse developed by military and industry raises the expectation that human knowledge will be more powerful and more accurate, empowered by superior technologies that enable ultimate 'situational awareness'.⁷⁹ As Luckey puts it, 'I think soldiers are going to be superheroes who have the power of perfect omniscience over their area of operations, where they know where every enemy is, every friend is, every asset is'.⁸⁰ It is part of the older discourse on omnipresence and

⁷⁰See Evgeny Morozov, *To Save Everything, Click Here: Technology, Solutionism and the Urge to Fix Problems That Don't Exist* (London: Penguin Books, 2014).

⁷¹NSCAI, 'National Security Commission on Artificial Intelligence final report', p. 23.

⁷²John R. Hoehn, Jill C. Gllagher, and Kelley M. Sayler, 'Overview of Department of Defense use of the electromagnetic spectrum,' Washington DC: Congressional Research Service (8 October 2020), p. 15.

⁷³Article 36, 'Killing by machine'.

⁷⁴Virilio, *The Vision Machine*, p. 61.

⁷⁵Douglas Kellner, 'Virilio, war and technology: Some critical reflections', *Theory, Culture & Society*, 16:5-6 (1999), pp. 103-25 (p. 110).

⁷⁶Anduril, 'Anduril—Command & Control' (2023_, available at: {https://www.anduril.com/}.

⁷⁷Anduril, 'Anduril—Command & Control'.

⁷⁸Anduril, 'Lattice OS' (2023), available at: {https://www.anduril.com/lattice/}.

⁷⁹See Suchman, 'Algorithmic warfare and the reinvention of accuracy'.

⁸⁰Lee Fang, 'Defense tech startup founded by Trump's most prominent Silicon Valley supporters wins secretive military AI contract', The Intercept (9 March 2019), available at: {https://theintercept.com/2019/03/09/anduril-industries-project-maven-palmer-luckey/}.

⁶⁹Bousquet, 'Lethal visions', p. 74.

omnivoyance mainly boosted by the drones' view from above. But it is vision no longer predicated on humans seeing things.

Acts and counter-acts of de-visualisation

Based on the above, it can be argued that the governmental-military as well as industry discourse has established a strong narrative about the unlimited possibilities of AI for the question of perceiving, knowing, deciding, and acting in recent years. This discourse is partly reproduced by the media that contributed to the mystification of AI also for civilian purposes. The limitations of these AI applications are much less in focus. This is also the case regarding the broad sensing complex, where the same logic of seeing and hiding plays out that has been important for warfare since the beginning of the 20th century in terms of concealing and camouflage.⁸¹ At the same time, the changing mechanism and implications of AI remain an understudied research issue. The aspect I highlight in the following is how de-visualisation appears here as deliberate acts to attack and distort visual sensing technology used in the military.

Bousquet outlines in a detailed study how hiding became part of the military strategy particularly during the First and Second World Wars and how military engineering went to great lengths to improve camouflage to conceal from human vision.⁸² The changes in military sensing after the Second World War, which moved away from the ocular-centric approach to including electromagnetic signals (radar in particular), also required a different approach to hiding. While camouflage remained of importance for items such as uniforms and the painting of military assets, technology such as stealth offered a new response to the challenge of indirect visual detection – indirect in the sense of radar screen and other sensor interfaces. As Bousquet puts it in this context, 'camouflage has become increasingly understood as an exercise in signature management, whereby a given target's signature corresponds to its characteristic aggregate of distinctive signal features across the array of relevant sensorial fields.⁸³

In that, the central logic of hiding is to make objects less easily visible and detectable – whether by the 'naked' human eye or by technologically augmented human vision ranging from the telescope to the drone vision of the past two decades, or by other sensors collecting sound and electromagnetic signal reflections. This central logic still plays a role with the automatisation of vision and applications such as image recognition, where the correct classification of images can be physically perturbed. At the same time, digital attacks add a new dimension to the visual/devisual dimension. Here, it is no longer that the object is being camouflaged, but that the process of image recognition is being disturbed before ML processes a specific image. In other words, it is not the sensing that is directly disturbed but the 'make sense' component.

Vision under attack: Adversarial examples

In the last decade, research in 'adversarial attacks' on deep neural network's perceptual architecture for computer vision has intensified.⁸⁴ What are adversarial attacks or examples (AE) in the context of adversarial machine learning (AML)? In the visual domain, AE can be either digital or physical.⁸⁵ Digitally, examples are imperceptible perturbations to images that consist in adding 'noise' to the pixel of an image, thereby provoking, for example, a misclassification or a misdetection of objects in the image. Noise is digital information that is not perceived by the human eye. In a research example, a layer of digital 'noise' was added to an initial set of images. These images were

⁸¹See Bousquet, *The Eye of War*, pp. 153–89.

⁸²Bousquet, The Eye of War, pp. 153-89.

⁸³Bousquet, *The Eye of War*, pp. 173.

⁸⁴See Battista Biggio and Fabio Rolia, 'Wild patterns: Ten years after the rise of adversarial machine learning—ScienceDirect', *Pattern Recognition*, 84 (2018), pp. 3147–331.

⁸⁵See Shasha Li, Shitong Zhu, Sudipta Paul et al., 'Connecting the dots: Detecting adversarial perturbations ssing Context inconsistency', arXiv:2007.09763 [Cs] (2020), p. 1, available at: {http://arxiv.org/abs/2007.09763}.

beforehand correctly classified as 'dog' by the ML model. After adding the noise, the deep convolutional neural network 'ImageNet' used by Szegedy et al. classifies all images as 'ostrich' with high confidence.

The main challenge for launching such digital, non-physical attacks is to get access to the inner structure and function of a DNN. While access during the development and training phase can potentially enable the infiltration by AE, AML requires a higher level of sophistication. However, there are various other AEs that exploit the vulnerability of deep learning systems that lead to similar outcomes. It is noteworthy that one of the initial findings of Szegedy et al. on emerging adversarial attacks was that 'the specific nature of these perturbations is not a random artifact of learning: the same perturbation can cause a different network, that was trained on a different subset of the dataset, to misclassify the same input.⁸⁶ In other words, they are robust. These attacks are also considered as 'black box adversarial examples' that can create 'a target model without access to the model's architecture or parameters;⁸⁷ which makes the attack especially powerful. In contrast, in white-box settings, full access to the model's parameters is obtained. This refers mainly to full knowledge of a ML algorithm, architecture, and model. Research has repeatedly confirmed the transferability of black-box attacks.⁸⁸ It should also be mentioned that research discusses a 'greybox attack where the adversary may have partial information. This could be access to open-source data used to train the target network, or the ability to probe the target network by analysing the outputs resulting from a given input.⁸⁹

The difference from the practice of camouflage here is that the deliberate de-visualisation of such attacks leads to the putative sensing of objects that are non-existent. It is not about hiding a material object from surveillance view, but about creating the illusion of the existence of a materially non-existent object in the virtual world. Deliberate attacks can aim at the integrity of machine learning models in a subtle and hardly detectable way before it is used in practice. Such attacks could, for example, be aimed at 'data poisoning' in the training phase, and the US military is aware of these risks and the necessity to act upon them. As former Deputy Secretary of Defense Work argued, 'we're moving into an era of AI competition, and poisoning data is a way to gain an advantage. We have to be able to guard against that?⁹⁰ However, the more central question for this paper is how *physical* adversarial examples challenge the promise of computer vision or rather of a decision-making machine.

AEs in the physical dimension work according to the same logic used in the digital domain but alter the physical space within the vision field that forms the sensor input of a computer vision system. In other words, perturbations are physically added to the objects a computer vision system aims to classify. For example, Brown et al. created an attack based on generating an imageindependent patch.⁹¹ This means that the authors 'construct an attack that does not attempt to subtly transform an existing item into another ... This patch can then be placed anywhere within the field of view of the classifier, and causes the classifier to output a targeted class. Because this patch

⁸⁸Nicolas Papernot, Patrick McDaniel, and Ian Goodfellow, 'Transferability in machine learning: From phenomena to blackbox attacks using adversarial samples', arXiv:1605.07277 [Cs] (2016), available at: {http://arxiv.org/abs/1605.07277}.

⁸⁹Christopher Ratto, Michael Pekala, Neil Fendley et al., 'Adversarial machine learning and the future hybrid battlespace' (2021), pp. 4–5, available at: {https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-190/MP-IST-190-28.pdf}.

⁹⁰US Department of Defense, 'Honorable Robert O. Work, Vice Chair, National Security Commission on Artificial Intelligence, and Marine Corps Lieutenant General Michael S. Groen, Director, Joint Artificial Intelligence Center hold a press briefing on Artificial Intelligence.

⁹¹Tom B. Brown, Dandelion Mané, Aurko Roy et al., 'Adversarial patch', arXiv:1712.09665 [Cs] (16 May 2018), available at: {http://arxiv.org/abs/1712.09665}.

⁸⁶Christian Szegedy, Wojciech Zaremba, Ilya Sutskever et al., 'Intriguing properties of neural networks', arXiv:1312.6199 [Cs] (2014), available at: {http://arxiv.org/abs/1312.6199}.

⁸⁷Gamaleldin F. Elsayed, Shreya Shankar, Brian Cheung et al., 'Adversarial examples that fool both computer vision and time-limited humans', arXiv:1802.08195 [Cs, q-Bio, Stat] (21 May 2018), p. 2, available at: {http://arxiv.org/abs/1802.08195}.



Figure 5. Graffiti and physical perturbation to a 'Stop' sign.^a ^aSource: Eykholt et al., 'Robust physical-world attacks on deep learning models', 2.

is scene-independent, it allows attackers to create a physical-world attack without prior knowledge of the lighting conditions, camera angle, type of classifier being attacked, or even the other items within the scene.⁹² In this example, the classifier rated a banana with very high confidence as a 'banana'. After adding the patch, the classifier instead rated the same object with very high confidence as a 'toaster'.

This AE is a variation on a range of experiments undertaken in the context of autonomous driving and machine learning. Crashes involving the autonomous driving systems of Tesla and Uber have gained considerable public attention in recent years and showed the limitation of current computational perception. The creation of general attack algorithms, also known as Robust Physical Perturbations (RP2),⁹³ has proven to be robust in changing, unstable environments and with varying distances and camera angles. Here, an often-considered AE is the alteration of road signs by adding small objects such as patches. Figure 5 shows a 'Stop' sign that is altered by random graffiti (left), which is a general occurrence. The Stop sign on the right shows patterns that are AE. Both alterations are detectable by human vision and do not distort a human's understanding of the sign's meaning. While a human would therefore most likely consider both examples as random acts of vandalism, the deliberate adversarial examples can lead to misclassifications and to incorrect driving decisions by computer vision systems. As in other cases, physical AEs are often easily identifiable by human vision and would not lead to altered action. The decisive point is, however, that the deliberate de-visualisation of what situational awareness or perception means leads to a new set of post-scopic challenges at the interstice of physical imagery and electronic data processing.

The ability to create stable attacks for a noisy environment suggests that this could also influence the reliability of autonomous systems in the military and security domains. One of the key areas

⁹²Brown et al., 'Adversarial patch', p. 1.

⁹³See Kevin Eykholt, Ivan Evtimov, Earlence Fernandes et al., 'Robust physical-world attacks on deep learning models', arXiv:1707.08945 [Cs] (2018), available at: {http://arxiv.org/abs/1707.08945}; Jinghan Yang, Adith Boloor, Ayan Chakrabarti et al., 'Finding physical adversarial examples for autonomous driving with fast and differentiable image compositing', *arXiv:2010.08844* [Cs] (17 October 2020), available at: {http://arxiv.org/abs/2010.08844}.

of research for different militaries are autonomous air, land, and sea vehicles. While the development of land vehicles is particularly challenging due to the complexity of the environment, physical attacks on their vision systems based on RP2 are a possibility. Attacks on autonomous civilian driving systems are even easier to imagine, given the importance of road signs in such environments.

It is noted that physical adversarial attacks on imaging systems are constrained by real-world physical conditions and that the robustness of AEs depends on extensive research and training.⁹⁴ At the same time, Chen concludes that 'ultimately, we found that when AI technology is really widely used in the military field, adversarial examples will have a subversive impact on several activities in several steps in the kill chain, which will directly lead to the interruption of the entire kill chain.⁹⁵

While algorithmic 'seeing' opens new ways of sensing, it is not a step path towards omniscience. Counter-measures against the all-seeing algorithmic eye also take productive forms, moving from concealing to producing classifications. 3D-printed adversarial objects proved to be robust in fooling neural network classifiers in the physical world over varying viewpoints and natural noise.⁹⁶ The authors of an experiment from MIT's Computer Science and Artificial Intelligence Laboratory fooling Google image recognition also showed that they were able to choose what the image recognition algorithm was perceiving. In the words of Anish Athalye, 'It's actually not just that they're [adversarial examples] avoiding correct categorization – they're classified as a chosen adversarial class, so we could have turned them into anything else if we had wanted to ... The algorithm takes in any textured 3D model, such as a turtle, and finds a way to subtly change the texture such that it confuses a given neural network into thinking the turtle is any chosen target class.⁹⁷

Considered in the military context, these insights question the overly optimistic view on AI becoming the ultimate solution for awareness and precision issues. For example, it was suggested that AI could make war 'more ethical'⁹⁸ if 'drones could be taught not to shoot at "protected symbols" such as the red cross sign, or not to shoot at children, by being trained not to target people below a certain height'.⁹⁹ Quite apart from the technological feasibility of using AI reliably in combat, such understandings do not accommodate the established research on AI vulnerability. Based on the insights from this section, 'protected symbols' or 'physical features' could be easily perturbed but also deliberately exploited to cause misclassifications in a way that might be imperceptible by the human eye even if a human operator was in/on the loop.

The algorithmic fog of war

The military-industrial, but also some of the academic, exploration of military vision technology mainly operates in the context of the 'prosthetic' augmentation concept, where vision, knowledge, and decision as well as the human and material are distributed elements of a system. Here, technologically enhanced vision is a tool – a tool that might not always deliver what it promises, but whose failures are usually seen as the outcome of flawed human-machine interaction that could, in principle, be fixed. The idea of JADC2 moves the expectations, however, increasingly outside of this apparatus of distributed agency. ML promises the emergence of a machine that does not

⁹⁴Ratto et al., 'Adversarial machine learning and the future hybrid battlespace' p. 6.

⁹⁵Yuwei Chen, 'The risk and opportunity of adversarial example in military field' (2022), pp. 100–7, available at: {https://openaccess.thecvf.com/content/CVPR2022W/ArtOfRobust/html/Chen_The_Risk_and_Opportunity_of_Adversarial_ Example_in_Military_Field_CVPRW_2022_paper.html}.

⁹⁶Anish Athalye, Logan Engstrom, Andrew Ilyas et al., 'Synthesizing robust adversarial examples', arXiv:1707.07397 [Cs] (2018), available at: {http://arxiv.org/abs/1707.07397}.

⁹⁷Luke Dormehl, 'That turtle is a fun! Scientists highlight major flaw in image recognition', Digital Trends (2 November 2017), available at: {https://www.digitaltrends.com/cool-tech/image-recognition-turtle-rifle/}.

⁹⁸Steven Umbrello, Phil Torres, and Angelo F. De Bellis, 'The future of war: Could lethal autonomous weapons make conflict more ethical?', *AI & SOCIETY*, 35:1 (2020), pp. 273–82.

⁹⁹Jake Evans, 'Australian defence force invests \$5 million in "killer robots" research', ABC News (28 February 2019), available at: {https://www.abc.net.au/news/2019-03-01/defence-force-invests-in-killer-artificial-intelligence/10859398}.

only correct or overcome human limitations but also overcomes the very necessity of distributing tasks between machines and humans. This new unified 'machine' agent is capable of detecting, classifying, deciding, and acting in seconds – it runs through the whole former OODA loop independently in its end-point version. However, this central promise of the imagined algorithmic turn for the military that is strongly connected to the condition of speed makes a consideration of the vulnerability of AI-empowered systems crucial.

While the aforementioned concept of meaningful human control introduced to the debate about LAWS at the United Nations' CCW lacks a systematic and comprehensive operationalisation,¹⁰⁰ the baseline is that control can only be 'meaningful' when 'sense making' and 'deciding' are acts involving human deliberation. However, the comprehensive de-visualisation taking place by automating and de-linking conventional human vision from knowing results in a reliance on data output that gives human operators only an abstract option to control actions.

In that, we are moving towards a twofold contestation of human control and decision-making capacity. First, vision is affected by the translation of live images and by the increasing use of image recognition technologies that will transgress the initial usage of pattern recognition informing human monitoring. Second, moving beyond the simple mechanics of first- and second-generation armed drones (or of other surveillance technology) to the integration of autonomous technologies in vastly different security and weapons apparatuses sets a clear trajectory for decision machines powered by automated sensory input in terms of computer and electromagnetic signals.

Technical research underlines the vulnerability of machine learning to adversarial input perturbations,¹⁰¹ but these findings, along with a growing awareness and response to this problem, have virtually no platform in governmental-military discourse. It remains almost completely dominated by optimistic narratives praising the opportunities of 'AI' while failing to address the technology's complexity and acknowledging associated challenges and risks.

Perspectives based on 'the scopic regimes of modernity, which have been influential in shaping viewing practices in Western contexts for over 500 years'¹⁰² are yet to take account of this emerging post-scopic condition. Grayson and Mawdsley¹⁰³ as well as Bousquet¹⁰⁴ showed that the view from the drone is deeply embedded in Cartesian perspectivalism and Baconian empiricism. Both concepts influence our understanding of vision; they provide the basis for legitimising truth claims predicated on the drone providing the human observer with a privileged status and revealing the 'true' essence of the observed field. The narrative of augmentation within the existing scopic regime lies at the core of the promise to overcome the limits of vision and knowledge in warfare.

But seeing in the prosthetic sense of augmenting or replacing the human eye's direct visual contact with an object (or target) increasingly moves to the background. The emergence of a regime of non-human perception, data processing, and decision as well as the novel truth claims about algorithmic objectivity, precision, and neutrality therefore implies a reversal of fundamental logics of drone warfare understood as 'a mode of "seeing without being seen" that reproduces the scopic regimes of modernity.¹⁰⁵ This is the ultimate future vision of JADC2.

The new regime also features the dissolution of the omnipotent 'gaze'.¹⁰⁶ What we find now is a change of subject positions, in which the human 'operator gaze'¹⁰⁷ is no longer the default viewing

¹⁰⁰Elke Schwarz, 'Autonomous weapons systems, artificial intelligence, and the problem of meaningful human control', *Philosophical Journal of Conflict and Violence*, 5:1 (2021), pp. 53–72.

¹⁰¹For an overview, see Biggio and Rolia, 'Wild patterns'.

¹⁰²Grayson and Mawdsley, 'Scopic regimes and the visual turn in International Relations', p. 432.

¹⁰³Grayson and Mawdsley, 'Scopic regimes and the visual turn in International Relations'.

¹⁰⁴Bousquet, *The Eye of War*.

¹⁰⁵Grayson and Mawdsley, 'Scopic regimes and the visual turn in International Relations', p. 445.

¹⁰⁶Grayson and Mawdsley, 'Scopic regimes and the visual turn in International Relations'; Gregory, 'From a view to a kill'; Maurer, 'Visual power'; Tyler Wall and Torin Monahan, 'Surveillance and violence from afar: The politics of drones and liminal security-scapes,' *Theoretical Criminology*, 15:3 (2011), pp. 239–54; Alison J. Williams, 'Disrupting air power: Performativity and the unsettling of geopolitical frames through artworks', *Political Geography*, 42 (2014), pp. 12–22.

¹⁰⁷Grayson and Mawdsley, 'Scopic regimes and the visual turn in International Relations', p. 440.

and perceiving subject. Here, the established truth claims based on visual evidence are replaced by a different regime that gains its legitimacy from technological superiority in line with the dominant narrative of 'AI' progress. In other words, the truth or accuracy claims of technology presenting its output to a human, or deciding and acting without human input, are legitimised via the meta-narrative of infallible technology that is beyond human abilities (and understanding).

While there is little public debate about the limits of military 'AI', the US military appears to be aware of challenges emerging in de-visualisation. In 2019, the US DoD released a funding call for the creation of the 'Guaranteeing AI Robustness against Deception (GARD)' programme, running for 48 months.¹⁰⁸ It was stated that GARD 'will initially concentrate on state-of-the-art image-based ML, then progress to video, audio and more complex systems – including multi-sensor and multi-modality variations. It will also seek to address ML capable of predictions, decisions and adapting during its lifetime.¹⁰⁹ As Hava Siegelmann, then programme manager for GARD, noted when talking about adversarial examples in military situations that are impossible to identify by humans, 'it's like we're blind.¹¹⁰ Hence, the emerging post-scopic perception and action apparatus that promises superior outcomes leads to a comprehensive 'blindness' of human operators only performing 'meaning-less control',¹¹¹ if any. The expectations of 'lifting the fog of war' that have underpinned imagining technological innovation since the late 1990s were premature. A new, dense, and incapacitating digital fog emerges and arguably, 'even as people worry about intelligent killer robots, perhaps a bigger near-term risk is an algorithmic fog of war - one that even the smartest machines cannot peer through.¹¹²

Conclusion

Algorithmic warfare is transforming war and security policies. While the discipline of Internationl Relations slowly accommodates the powerful narrative of an algorithmic turn in empirical and theoretical regards, the consequences of this development for re-conceptualising 'vision' in the military context remain under-researched. A significant body of research has focused on drone warfare, particularly in the last decade, and has also addressed the important implications of remotely controlled violent force along the visual dimension. At the same time, the development, testing, and deployment of systems integrating AI technologies in targeting continue. But vision in the human ocular sense is not a feature of autonomy. We may be entering an era of ocular regression in which a central human sense – arguably the most central sense in combat – is further and further debilitated. The great visual extension and transformation of the drone age seems to be of limited future relevance in the new vision of JADC2 and similar initiatives that ultimately aim to replace human agency in the novel 'sense', 'make sense', and 'decide' loop. In its most extreme version, this loop will be compressed in a single action.

What is known as 'vision', and now labelled 'sensing', turns into a multisensory data input operation, and conditions of speed decrease options for meaningful human control. The dominant narrative about the potential of 'AI' in terms of providing superior technological omnivoyance and omniscience contributes to a process of de-visualisations that culminates in a deliberate human 'blindness', or rather incapacitation, in the digital fog of war.

In this context, human-machine interactions in terms of interfaces and adversarial ML attacks that are so far able to fool, disturb, and disable image classification significantly are rarely examined.

¹¹¹Ingvild Bode and Tom Watts, 'Meaning-less human control: Lessons from air defence systems for lethal autonomous weapons', Drone Wars UK (2021), available at: {https://dronewars.net/wp-content/uploads/2021/02/DW-Control-WEB.pdf}.

¹⁰⁸DARPA, 'Broad agency announcement guaranteeing AI robustness against deception (GARD) HR001119S0026' (2019), p. 6, available at: {https://www.federalgrants.com/Guaranteeing-AI-Robustness-against-Deception-GARD-75147.html}.

¹⁰⁹DARPA, 'Defending against adversarial Artificial Intelligence' (2019), available at: {https://www.darpa.mil/news-events/2019-02-06}.

¹¹⁰Cited in Knight, 'The fog of AI war', p. 4.

¹¹²Knight, 'The Fog of AI war', p. 47.

Relying on electronically mediated and translated imagery in various forms creates specific problems for humans interacting with machine output in the new, complex decision-action apparatus. Like the existing challenges to perception – to what we see, how we see it, and what we know – that are studied in the context of drone warfare, novel military innovations such as the use of generative AI in interfaces presenting clean visualisations of a messy reality introduce technology that becomes an increasing part of human decision-making. Under conditions of time pressure, speed, and information overload that are characteristic of modern warfare, trust in the objectivity and rationality of what is displayed and filtered becomes a central requirement. Truth claims are, however, increasingly less based on the outlined scopic regime of modernity and the established knowledge about vision. Algorithms that no longer require human intervention or supervision appeal to a different truth that is at the heart of a socio-technical narrative of machine superiority.

As argued, technological developments and political statements in recent years point clearly into the direction of a wide-ranging integration of autonomous or 'AI' technologies into military decision-making and targeting. The perceived advantages of systems that process, filter, and assess information on the spot are tempting for actors in military and security settings. The discourse of powerful 'AI' is, however, contested when we explore the limitations of algorithmic processing. In other words, the systems that have currently been developed and aim at fulfilling the JADC2 vision are much less reliable and more vulnerable than the dominant narrative suggests. However, this does not make the question of autonomy less important or this development less problematic. The socio-technical imagination of a revolution in warfare has paved the way to accepting AI in the broad sense as a solution to long-standing problems such as speed, distance, situational awareness, or precision. This acceptance is linked to an expectation that such systems are now emerging and being developed by perceived adversaries and that there is an immediate necessity to win the race about AI arms.¹¹³

While logics of seeing, perceiving, and knowing have remained stable for centuries, we might now enter an era of a post-scopic regime in which the visual field becomes ever more fragmented in the interplay of electronic and non-electronic data. As Bousquet argued in the context of drone studies, 'it is less the weapon that has come to serve as a prosthetic extension of the eye than perception itself which has been caught up in an unrelenting process of becoming weapon'.¹¹⁴ However, in the process of reversing the dream of human hypervisibility as form of hypervisualisation in favour of algorithmic de-visualisation, the weapon is now in an unrelenting process of becoming perception – it starts to replace human senses and importantly also collapses how the act of seeing precedes action. Rather than distributing tasks in the use of force, this is the development of a unified technological agency that perceives and decides.

Acknowledgements. The author wishes to thank the editors of EJIS as well as two different sets of anonymous reviewers in two review processes as well as Ingvild Bode, Anna Nadibaidze, Guangyu Qio-Franco, and Tom Watts for their helpful feedback on this article.

Hendrik Huelss is Assistant Professor of International Relations at the Center for War Studies, University of Southern Denmark. He is affiliated Senior Researcher in the AutoNorms project at SUD, funded by the European Research Council (2020–5). Hendrik's work is located at the intersection of international political sociology and studies of AI and technologies. His primary research interest and publication activities aim at producing critical thinking on the role of AI in the context of security and military practices. This is often combined with Hendrik's second major research interest, the new conceptualisation of the role of norms in International Relations.

¹¹³For a critical view on the AI arms race, see Arthur Holland Michel, 'Recalibrating assumptions on AI', Chatham House – International Affairs Think Tank (12 April 2023), available at: {https://www.chathamhouse.org/2023/04/recalibrating-assumptions-ai}.

¹¹⁴Bousquet, 'Lethal visions', p. 63.

Cite this article: Hendrik Huelss, 'Transcending the fog of war? US military 'AI', vision, and the emergent post-scopic regime', *European Journal of International Security* (2024), pp. 1–21. https://doi.org/10.1017/eis.2024.21