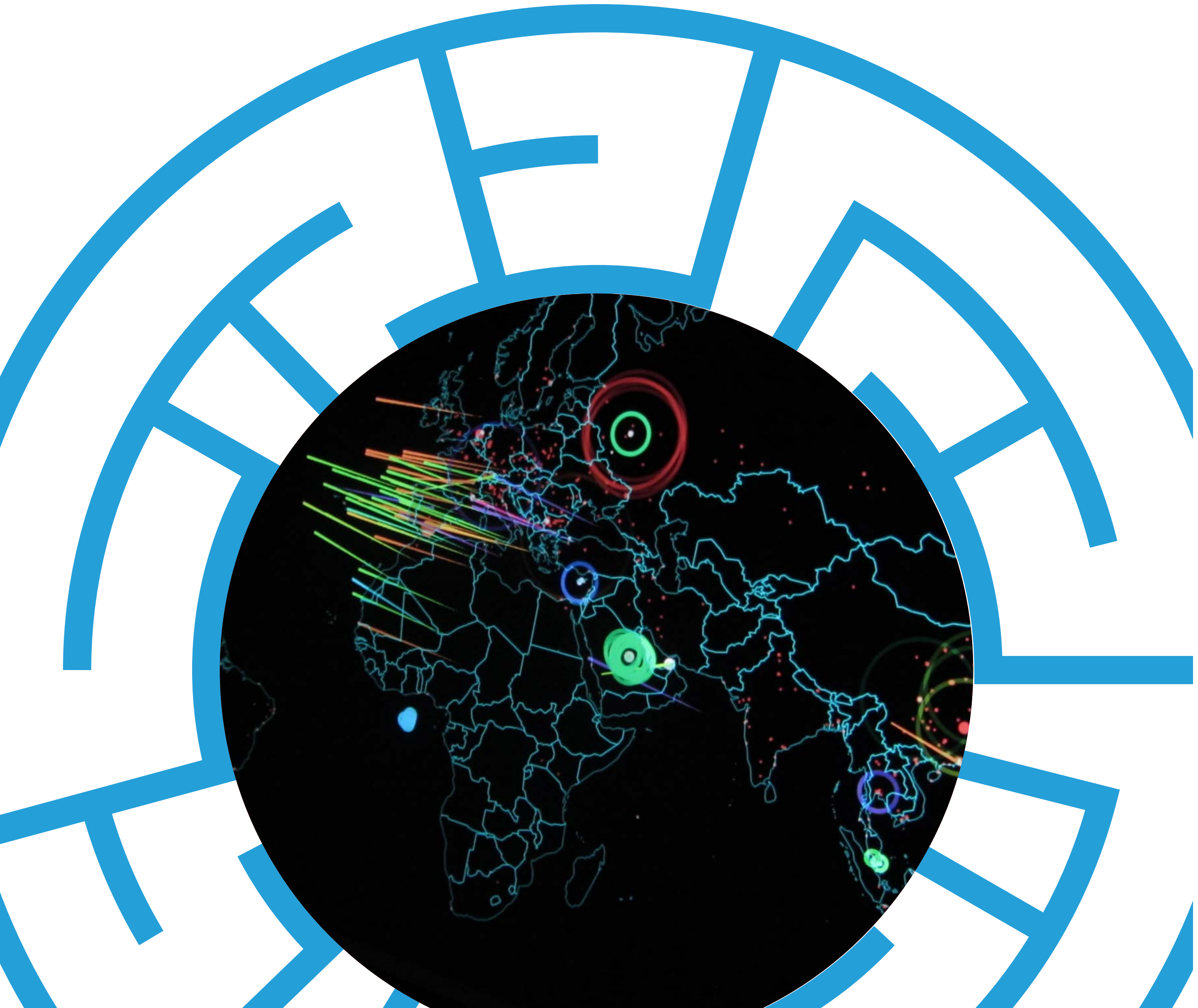
WAR IS FROM MARS, AI IS FROM VENUS: REDISCOVERING THE INSTITUTIONAL CONTEXT OF MILITARY AUTOMATION

Jon R. Lindsay



For nearly a century, the artificial intelligence (AI) revolution has been just over the horizon, and yet that horizon is always receding. Dramatic advances in commercial AI once again inspire great hopes and fears for military AI. Perhaps this time will be different. Yet, successful commercial AI systems benefit from conducive institutional circumstances that may not be present in the anarchic realm of war. As AI critics have recognized since the Cold War, the complexity and uncertainty of security competition tend to frustrate ambitious applications of military automation. The institutional context that makes AI viable, moreover, is associated with important changes in patterns of political violence. The same liberal order that encourages AI innovation also enables more subversive forms of conflict. Military organizations that adopt AI, therefore, are likely to adopt more institutionalized processes to enable automated decision systems, while military AI systems are more likely be used in more institutionalized environments. Unintended consequences of institutionalized automation include unmanageable administrative complexity and unappreciated human suffering in chronic limited conflicts.

AI is once again a hot topic in national security. Hopes and fears about autonomous weapons have been a staple of military futurism for over 50 years.[1] But "AI hype" has often led to an "AI winter" — a dormant time for AI research and development. Throughout this same period, military organizations have become more dependent on information systems, more fraught with coordination problems, and more frustrated in protracted conflicts.[2] Like the demigod Tantalus, condemned to spend eternity longing for fruits just out of reach, technologists keep seeing the revolutionary promise of military AI on an ever-receding horizon. War "at machine speed" is just 10 years away, and it always will be.

But we've come a long way since Clippy, the Microsoft office assistant from the turn of the millennium. By the mid-2010s, remarkable progress in the development and application of machine-learning techniques began to transform many industries, from advertising to transportation and cybersecurity. This trend has culminated spectacularly in a recent smorgasbord of AI applications available to the public, such as ChatGPT and DALL-E from OpenAI. All of a sudden, AI seems to be mastering consummately human pursuits such as creative writing, software design, and the graphic arts. It looks like Tantalus finally got his apple. The global economy has barely begun to reckon with the potential for disruption and dislocation as industries adapt to harness the power of AI.

The military implications literally write themselves. According to ChatGPT, "AI can enable the development of autonomous weapons systems, such as drones, ground vehicles, and ships. These systems can operate without direct human control, making them faster, more efficient, and potentially capable of executing complex missions with reduced human risk." The bot also describes applications for "En-

[1] Paul Dickson, *The Electronic Battlefield* (Bloomington: Indiana University Press, 1976); Daniel Deudney, *Whole Earth Security: A Geopolitics of Peace*, Worldwatch Paper 55 (Washington, DC: Worldwatch Institute, 1983); Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Boston: Little, Brown & Co, 1993); James Adams, *The Next World War: Computers Are the Weapons and the Front Line Is Everywhere* (New York: Simon & Schuster, 2001); Peter W. Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century* (New York: Penguin Press, 2009); Ben Buchanan and Andrew Imbrie, *The New Fire: War, Peace, and Democracy in the Age of AI* (Cambridge, MA: MIT Press, 2022).

[2] C. Kenneth Allard, *Command, Control, and the Common Defense* (New Haven, CT: Yale University Press, 1990); Paul N. Edwards, *The Closed World: Computers and the Politics of Discourse in Cold War America* (Cambridge, MA: MIT Press, 1997); Daniel R. Lake, *The Pursuit of Technological Superiority and the Shrinking American Military* (New York: Palgrave Macmillan, 2019); Jon R. Lindsay, *Information Technology and Military Power* (Ithaca, NY: Cornell University Press, 2020).

hanced Situational Awareness … Decision-Making and Command Systems … Cybersecurity and Information Warfare … Logistics and Supply Chain Management … [and] Predictive Maintenance.”[3] ChatGPT reflects back to us a large speculative literature on the transformative strategic implications of AI, both utopic and dystopic. The United States and China, among others, have commissioned numerous studies and developed working prototypes in a quest to realize the dramatic opportunities — and counter the looming threats — of military AI.[4] The warfighting advantages of AI, furthermore, seem poised to alter the balance of power and trigger arms races as democracies and autocracies alike attempt to substitute autonomous systems for human warriors.[5]

These developments, in turn, have prompted understandable concern about the ethics of AI in peace and war.[6] Many drones and other weapons systems already provide fully automated engagement modes, raising urgent questions about meaningful human control and the potential for inadvertent escalation.[7] An even more dire scenario is one in which the rise of AI-enabled systems transcends human control altogether, leading to worries about the existential implications of so-called artificial general intelligence.[8] Industry leaders like Elon Musk have begun calling for more deliberate ethical reflection as well as outright guidelines and regulations for the development of AI before it is too late. Even ChatGPT hastens to reassure us: “While AI has the potential to enhance military capabilities, decisions regarding its use in warfare should be guided by international laws, regulations, and ethical considerations to ensure the protection of civilian lives, compliance with human rights, and prevention of unnecessary suffering.”[9]

Much of the ethical and strategic conversation about military AI tends to hold the nature of war constant and to consider issues having to do with the adoption of automated weapons on the battlefield. Futurists worry, in effect, about the weapons of tomorrow in the wars of today. This leads to important discussions about accurate targeting, unintended civilian casualties, and meaningful human control. These are serious problems, to be sure, and it is vital for policymakers and commanders to consider them. Yet, it is further possible that the political context of war itself might change in interesting ways, either because of the introduction of AI or because of some hidden factor affecting both the development of AI *and* the evolution of war. The changing organizational or strategic context of war might lead to rather different concerns. These concerns would be less about the ways in which autonomous machines will behave in familiar wars and more about the ways in which human societies will behave in unfamiliar futures.

There is at least one important topic that ChatGPT fails to consider in its hallucination — a technical term for the generation of false or misleading information[10] — about future war. This is whether and how the very economic context that has created ChatGPT may affect or alter the viability of military AI. It is an obvious but underappreciated fact that most of the impressive applications of AI to date have emerged in the commercial world. War, however, is a very different sort of “business.” The conditions that make AI economically viable today may not hold in the chaotic and controversial realm of war, or at least not to the same extent.[11] For instance, AI depends on the availability of data, but war is full of fog and friction. AI depends on having many opportunities for training, but war is a rare and unpredictable event. AI companies submit to the rule of law, while war is famously anarchic. The success of AI systems in the world of peaceful commerce, therefore, may be a poor guide to the performance of AI in the world of wartime combat.

Even more fundamentally, the economic conditions that support AI performance may be associated with important changes in patterns of political conflict. Traditional interstate war, according to classic international relations theory, is a struggle for dominance in an ungoverned world. And yet the modern international system is more globalized, interconnected, interdependent, and institutionalized than ever before. The so-called liberal order is hardly peaceful, however, as we see in the proliferation of espionage and subversion,[12] “hybrid” or “gray zone” conflict,[13] and various forms of “weaponized interdependence.”[14] These limited forms of conflict have a different logic. If traditional war is a clash between feuding organizations in anarchy, then subversive conflict works by infiltrating and manipulating societies from within.[15] It is no coincidence that intelligence contests and irregular violence have become prominent in the hyper-globalized 21st century. With more institutions, and more complex institutions, there are more opportunities to subvert them. Yet, this means that shared institutions are a condition for the possibility of subversion and espionage, as well as their modern manifestations in cybersecurity. How, therefore, should we expect people to use AI for conflict *within* social institutions, rather than *between* them? Note further that the outcomes of subversive conflicts and intelligence contests within the global liberal order tend to be protracted and ambiguous, but this is precisely the opposite of the fast and decisive victories envisioned for AI. Should we expect AI to somehow make these more limited forms of conflict more effective, finally, or just more complicated?

This article examines the institutional context of AI to sketch out an alternative interpretation of its strategic implications. I proceed in six parts. First, I discuss popular worries about the substitution of AI for human activity. Second, I highlight enduring concerns about the automation of strategic systems that appeared in the 1980s and still resonate today. Third, I briefly summarize the economics of AI, highlighting the key institutional conditions that shape AI performance. Fourth, I argue that the political logic of war tends to undermine these institutional conditions. Fifth, I explore the implications of the tension between the institutional conditions for AI and the political context of war. Unintended consequences include unmanageable military complexity and degraded human security in more limited forms of conflict within the liberal order. Finally, I conclude that the future of military AI will resemble its past in many ways.

The Myth of AI Substitution

While we seem to be at a watershed moment in the development of AI, we should bear in mind that this is not a new conversation. Indeed, the history of AI and the history of computer science are largely one and the same. Alan Turing imagined his famous universal computing machine as an automated clerk, and Charles Babbage before him imagined the difference engine as an automated parliament.[16] Turing’s 1950 essay on automating intelligence still provides thoughtful counterarguments to AI skepticism.[17] The Macy Conferences on cybernetics, which brought together founding fathers of AI like Claude Shannon and John von Neumann, were explicitly dedicated to creating a general science of information and control to build a mechanical brain.[18] Indeed, the nascent field of computer science aimed to create a new kind of agent, if not a new kind of lifeform.

[3] Author query of https://chat.openai.com/, June 9, 2023.

[4] Elsa B. Kania, "Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power", Center for a New American Security, November 28, 2017, https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power; "Final Report," National Security Commission on Artificial Intelligence, March 2021, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

[5] Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York: W. W. Norton & Company, 2018); Michael C. Horowitz, "Artificial Intelligence, International Competition, and the Balance of Power," *Texas National Security Review* 1, no. 3 (May 2018): 37–57, https://doi.org/10.15781/T2639KP49; Michael Raska, "The Sixth RMA Wave: Disruption in Military Affairs?" *Journal of Strategic Studies* 44, no. 4 (2021): 456–79, https://doi.org/10.1080/01402390.2020.1848818; Jeffrey Ding and Allan Dafoe, "The Logic of Strategic Assets: From Oil to AI," *Security Studies* 30, no. 2 (2021): 182–212, https://doi.org/10.1080/09636412.2021.1915583; Buchanan and Imbrie, *The New Fire*.

[6] Heather M. Roff, "The Strategic Robot Problem: Lethal Autonomous Weapons in War," *Journal of Military Ethics* 13, no. 3 (2014): 211–27, https://doi.org/10.1080/15027570.2014.975010; Matthew Le Bui and Safiya Umoja Noble, "We're Missing a Moral Framework of Justice in Artificial Intelligence," in *The Oxford Handbook of Ethics of AI*, ed. Markus Dirk Dubber, Frank Pasquale, and Sunit Das (Oxford: Oxford University Press, 2020), 163–80.

[7] Michael C. Horowitz, "When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence and Stability," *Journal of Strategic Studies* 42, no. 6 (2019): 764–88, https://doi.org/10.1080/01402390.2019.1621174; James Johnson, "Delegating Strategic Decision-Making to Machines: Dr. Strangelove Redux?" *Journal of Strategic Studies* 45, no. 3 (2020): 439-477, https://www.tandfonline.com/doi/abs/10.1080/01402390.2020.1759038; Kenneth Payne, *I, Warbot: The Dawn of Artificially Intelligent Conflict* (New York: Oxford University Press, 2021)

[8] Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies* (New York: Oxford University Press, 2014); Nathan Alexander Sears, "International Politics in the Age of Existential Threats," *Journal of Global Security Studies* 6, no. 3 (September 2021), https://doi.org/10.1093/jogss/ogaa027.

[9] Author query of https://chat.openai.com/, June 9, 2023.

[10] Karen Weise and Cade Metz, "When A.I. Chatbots Hallucinate," *New York Times*, May 1, 2023, https://www.nytimes.com/2023/05/01/business/ai-chatbots-hallucination.html.

[11] Avi Goldfarb and Jon R. Lindsay, "Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War," *International Security* 46, no. 3 (2022): 7–50, https://doi.org/10.1162/isec_a_00425.

[12] David V. Gioe, Michael S. Goodman, and Tim Stevens, "Intelligence in the Cyber Era: Evolution or Revolution?" *Political Science Quarterly* 135, no. 2 (2020): 191–224, https://doi.org/10.1002/polq.13031; Thomas Rid, "A Revolution in Intelligence," in *The New Makers of Modern Strategy: From the Ancient World to the Digital Age*, ed. Hal Brands (Princeton, NJ: Princeton University Press, 2023), 1092–1118.

[13] Joseph L. Votel et al., "Unconventional Warfare in the Gray Zone," *Joint Force Quarterly*, no. 80 (January 2016), https://ndupress.ndu.edu/portals/68/documents/jfq/jfq-80/jfq-80.pdf; Alexander Lanoszka, "Russian hybrid warfare and extended deterrence in eastern Europe," *International Affairs* 92, no. 1 (2016): 175–95, https://www.jstor.org/stable/24757841; J. Andrés Gannon et al., "The Shadow of Deterrence: Why Capable Actors Engage in Contests Short of War," *Journal of Conflict Resolution* (2023), https://doi.org/10.1177/00220027231166345.

[14] Daniel W. Drezner, Henry Farrell, and Abraham L. Newman, eds., *The Uses and Abuses of Weaponized Interdependence* (Washington, DC: Brookings Institution Press, 2021), https://www.brookings.edu/book/the-uses-and-abuses-of-weaponized-interdependence/; Henry Farrell and Abraham Newman, *Underground Empire: How America Weaponized the World Economy* (New York: Henry Holt and Co., 2023).

[15] Jon R. Lindsay, "Restrained by Design: The Political Economy of Cybersecurity," *Digital Policy, Regulation and Governance* 19, no. 6 (2017): 493–514, https://doi.org/10.1108/DPRG-05-2017-0023; Lindsey A. O'Rourke, *Covert Regime Change: America's Secret Cold War* (Ithaca, NY: Cornell University Press, 2018); Melissa M. Lee, *Crippling Leviathan: How Foreign Subversion Weakens the State* (Ithaca, NY: Cornell University Press, 2020); Lennart Maschmeyer, "Subversion, Cyber Operations and Reverse Structural Power in World Politics," *European Journal of International Relations* 29, no. 1 (2022), https://doi.org/10.1177/13540661221117051.

[16] Jon Agar, *The Government Machine: A Revolutionary History of the Computer* (Cambridge, MA: MIT Press, 2003).

[17] A. M. Turing, "I.—COMPUTING MACHINERY AND INTELLIGENCE," *Mind* LIX, no. 236 (October 1950): 433–60, https://doi.org/10.1093/mind/LIX.236.433.

[18] Jean Pierre Dupuy, *The Mechanization of the Mind: On the Origins of Cognitive Science* (Princeton, NJ:: Princeton University Press, 2000); Ronald R. Kline, *The Cybernetics Moment: Or Why We Call Our Age the Information Age* (Baltimore: Johns Hopkins University Press, 2015).

But the mechanization of human intelligence proved elusive. Various technical methods such as formal theorem-proving, expert systems, and other symbol-processing approaches struggled to deliver on their early promises. These symbolic approaches are sometimes described collectively as "good old-fashioned AI" to distinguish them from modern connectionist approaches.[19] Symbolic AI was great at doing some things that seemed hard for humans (like calculating formulae) but quite stupid at other things that were easy (like recognizing images). A common refrain among AI skeptics was that AI lacked common sense and could not appreciate why any given computation might be meaningful or useful to human beings.[20] In attempting to automate a very narrow conception of human reasoning, early AI systems ignored the rich pragmatic context of human perception and decision-making.

We might pause to consider whether Cold War science fiction scenarios from the era of symbolic AI are still the best guide to strategic dilemmas in an era of machine learning and surveillance capitalism.

The field of computer science continued to grow, of course, but not because computers simply replaced human cognition. Rather, the emergence of better information technology created more things for human beings to do. If computers were to be practically useful for anything at all, people had to design applications, develop interfaces, build infrastructure, repair glitches, educate scientists and technicians, implement telecommunications regulations, and so on. This gave rise to an incredible array of new jobs and lucrative economic sectors in the second half of the 20th century. Human interaction thus became even more complex as the reliable functioning of software infrastructure became even more dependent on complementary economic and technical activity.

We are now riding the latest wave of AI enthusiasm. Unlike classic symbol-processing approaches to AI, modern connectionist approaches are inspired by the human brain, to include neural networks, deep learning, and machine learning. The first connectionist models emerged in the early days of cybernetics (the McColloch-Pitts perceptron), but they were not feasible at scale given the limited computing power available at the time. But dramatic advances in memory and computing power in recent decades have made this alternative approach to AI more feasible. Moreover, a host of complementary economic innovations in "big data" or "surveillance capitalism" has supercharged AI innovation by creating markets for AI models and products.[21] The current excitement stems from the impressive performance of machine learning in areas where symbolic AI stumbled (e.g., text translation, image recognition, spatial navigation, etc.). Nevertheless, classic concerns remain that machine learning has no understanding of why its pattern recognition outputs might be meaningful, confusing, misleading, or absurd for human beings.[22] Even worse, biased training data may reinforce structural racism and other social ills.[23] The new technology of AI is encouraging familiar skepticism.

The discourse on military AI goes back to the future as well. The public's conception of military AI is largely the product of science fiction movies from the Cold War. In films like *Doctor Strangelove*, *WarGames*, and *The Terminator*, an AI system is given the authority to start a nuclear war. Humans delegate authority to this AI because they want to improve deterrence, but the AI ends up triggering, or almost triggering, World War III because of, respectively, a tragic misunderstanding, a careless hacker, or a malicious AI. In *Tron*, anticipating themes from *The Matrix*, humans become imprisoned in a simulation run by a dictatorial AI, and they must draw on their unique humanity to escape. In *2001: A Space Odyssey* and *Robocop*, we watch AI systems turn on their masters because encoded directives are misaligned with human goals. In *Blade Runner* and *D.A.R.Y.L.*, law enforcement officers hunt down robots that have come up with their own goals, and that seem to be too dangerous for governments to tolerate. And last but not least, *Star Wars* gave us adorable droids with desires, emotions, senses of humor, and, occasionally, formidable lethality.

Most modern discussions about the ethics of military AI are implicitly focused on scenarios like these. The AI technology that we worry about today may be more realistic or grounded in contemporary prototypes, but the basic concerns dramatized in Cold War science fiction still resonate. We fear that lethal machines will make their own decisions to harm humans without appropriate human control or consent. An important theme that runs through such scenarios is *substitution*. The key assumption is that robots will replace some human functions, perform some human tasks, and become autonomous characters, which leads to either good robots (*Star Trek*) or bad robots (*The Terminator*). These robotic substitutes may add something extra (strength, speed, calculating ability) or miss something important (compassion, insight, understanding, creativity). They may be improved or deficient agents, but they are fully autonomous. The modified capabilities of these human substitutes end up creating dangerous or unintended consequences, which makes it necessary to control, regulate, banish, or battle them.

We might pause to consider whether Cold War science fiction scenarios from the era of symbolic AI are still the best guide to strategic dilemmas in an era of machine learning and surveillance capitalism. Great entertainment might not necessarily be the best guide to the future. One important reason is that technological innovation is guided by two very different economic logics — not only substitution but also *complementarity*. Substitutes replace jobs and functions with a cheaper or better improvement, while complements affect a larger network of jobs and functions throughout society.

Often, the advent of technological substitutes will make social complements more economically and politically valuable. If people find a baker who sells cheaper bread, then the market for butter and jam will increase, which means that new shops will open next to the bakery. Thus, the replacement of the horse-drawn carriage with the automobile required a lot of complementary innovation and infrastructure in terms of roads, repair shops, gasoline stations, car dealerships, assembly lines, and so on. One cannot just swap a horse for a car without considering the profound social changes that make this swapping possible.

Likewise for military AI, we need to ask whether the complementary innovations that are unlocking productivity in the AI economy might also be correlated with important changes in the nature or conduct of war. It may be true that an AI drone swarm would be able to defeat a modern company of soldiers in short order, but what are the chances of that company not evolving as well? A machine gun, similarly, would be invaluable when facing an ancient army of hoplite soldiers, but what are the chances that anyone would still fight with spears and swords in the same economic milieu that could produce machine guns? The chances are not strictly zero, as historically lopsided contests between Hernán Cortés and Mesoamericans or the Battle of Omdurman might suggest. But these events are exceptional outliers in military history, and militaries have strong incentives not to repeat them. As military weapons change, the context of war usually changes as well. Either new offensive potentials are countered by defensive innovation with similar technologies or, more radically, political actors start fighting over different things or for different reasons as the economic context changes.

Enduring Software Aspects of Strategic Defense Systems

Instead of taking our inspiration from Cold War science fiction like *Star Wars*, we might do well to study military automation in the real-world "Star Wars." The Reagan administration's Strategic Defense Initiative was an ambitious project to build an automated system that could shoot down enemy ballistic missiles. It featured space-based weapons systems and many computerized components. Automation was justified by the speed at which a missile defense system would have to make decisions in order to intercept incoming targets. Yet, the complementary context of strategic automation proved frustrating.

The Strategic Defense Initiative was a research initiative rather than an operational system. Yet, it raised serious concerns in the arms control community about automated escalation. As one contemporary analyst wrote, "destruction-entrusted automatic devices (DEAD)" for missile defense and nuclear response were "emerging in response to the strategic imperatives of the transparency [information] revolution."[24] This same concern about automated escalation is recognizable in modern worries about lethal autonomous systems. There are a host of extremely important strategic problems to be considered here, ranging from image classification and targeting errors to an excessive speed of decision-making leading to catastrophic escalation.[25]

[19] John Haugeland, *Artificial Intelligence: The Very Idea* (Cambridge, MA: MIT Press, 1985).

[20] Harry Collins, *Artificial Experts: Social Knowledge and Intelligent Machines* (Cambridge, MA: MIT Press, 1990); Hubert L. Dreyfus, *What Computers Still Can't Do: A Critique of Artificial Reason*, Rev. (Cambridge, MA: MIT Press, 1992); Gene I. Rochlin, *Trapped in the Net: The Unanticipated Consequences of Computerization* (Princeton, NJ: Princeton University Press, 1997).

[21] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (New York: PublicAffairs, 2019).

[22] Meredith Broussard, *Artificial Unintelligence: How Computers Misunderstand the World* (Cambridge, MA: MIT Press, 2018); Brian Cantwell Smith, *The Promise of Artificial Intelligence: Reckoning and Judgment* (Cambridge, MA: MIT Press, 2019)

[23] Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: New York University Press, 2018); Ruha Benjamin, "Race After Technology," in *Social Theory Re-Wired*, ed. Wesley Longhofer and Daniel Winchester, 3rd ed. (Oxford: Routledge, 2023), 405–16.

[24] Deudney, *Whole Earth Security*, 37.

[25] Roff, "The Strategic Robot Problem"; Horowitz, "When Speed Kills"; Johnson, "Delegating Strategic Decision-Making to Machines."

These are important concerns that force us to clarify goals and objectives, something that is famously difficult to achieve in politics.

It is important to recognize that these concerns are founded on an assumption that we will be able to build such systems in the first place. What if we will not be able to create strict substitutes for strategic decision-making? What if the concurrent development of the software ecosystem becomes too complex to manage? What if the resulting complexity of hybrid human-machine decision-making in war overwhelms the engineering process? What if the institutional complements to automation make substitution infeasible in realistic wartime scenarios?

Questions like these led the well-known computer scientist David L. Parnas to resign from the Strategic Defense Initiative Panel on Computing in Support of Battle Management. He openly published a series of technical objections in a paper entitled "Software Aspects of Strategic Defense Systems."[26] These objections deserve revisiting in this new era of excitement about military automation.

Parnas argued that it would be impossible for human designers to understand what the Strategic Defense Initiative software systems were doing or to provide training conditions that accurately replicated the fog and friction of a real war in an actual political crisis. And thus, it would also be impossible to draft precise requirements or optimal system designs for circumstances that were guaranteed to change. The net result was that "[t]he military software that we depend on every day is not likely to be correct. The methods that are in use in the industry today are not adequate for building large real-time software systems that must be reliable when first used."[27]

Parnas wrote that "the human mind is not able to fully comprehend the many conditions that can arise because of the interaction of these components" in software systems.[28] Because unanticipated failures could not be ruled out, and "the most competent programmers in the world cannot avoid such problems."[29] The brittleness of logical rules was coupled with a military problem of staggering complexity: "The system will be required to identify, track, and direct weapons toward targets whose ballistic characteristics cannot be known with certainty before the moment of battle. It must distinguish these targets from decoys whose characteristics are also unknown," and, even worse, "It will be impossible to test the system under realistic conditions prior to its actual use."[30] Strategic Defense Initiative designers were thus forced to make assumptions about the strategic context of system operations that were almost sure to be inaccurate in practice:

> *Fire-control software cannot be written without making assumptions about the characteristics of enemy weapons and targets. This information is used in determining the recognition algorithms, the sampling periods, and the noise-filtering techniques. If the system is developed without the knowledge of these characteristics, or with the knowledge that the enemy can change some of them on the day of battle, there are likely to be subtle but fatal errors in the software.*[31]

Design oversights in military technologies are typically mitigated through human intervention and adaptation, or social complements.[32] As Parnas observed, "It is not unusual for software modifications to be made in the field. Programmers are transported by helicopter to Navy ships: debugging notes can be found on the walls of trucks carrying computers that were used in Vietnam. It is only through such modifications that software becomes reliable."[33] Bottom-up adaptation and repair remains a fundamental feature of military information practice today.[34] Yet, full substitution precludes this vital complement: "Such opportunities will not be available in the 30-90 minute war to be fought by a strategic defense battle-management system."[35]

Parnas evaluated several cutting-edge computational techniques of the early 1980s and found them all wanting. Even with unlimited resources, Parnas thought the problem that the Strategic Defense Initiative was trying to solve was intractable: "I don't expect the next 20 years of research to change that fact."[36] If today's challenges in ballistic missile defense are any indication, Parnas' estimate of 20 years was far too conservative. Parnas' skepticism about Strategic Defense Initiative software reliability provides a cautionary tale for any ethicists who hope to encode reliable standards of operation into AI systems for any combat scenario: "It is inconceivable to me that one could provide a convincing proof of correctness of even a small portion of the SDI [Strategic Defense Initiative] software. Given our inability to specify the requirements of the software, I do not know what such a proof would mean if I had it."[37]

Parnas was especially pessimistic about AI: "[I]t is natural to believe that one should use this technology for a problem as difficult as SDI [Strategic Defense Initiative] battle management." But this belief was based on magical thinking, he suggested. "Artificial intelligence has the same relation to intelligence as artificial flowers have to flowers. From a distance they may appear much alike, but when closely examined they are quite different. I don't think we can learn much about one by studying the other. AI offers no magic technology to solve our problem."[38]

Software engineering is always hard, but it is even harder when software systems are expected to perform in situations that are infrequent, complex, and unpredictable. Sadly, the uncommon is common in combat.

Parnas was obviously talking about a previous AI technology (i.e., formal theorem-proving, symbolic logic, or expert system databases). Today's machine-learning techniques seem more impressive and less brittle. Indeed, these are boom times for AI in the commercial economy. We are seeing AI perform tasks that once seemed to belong exclusively to the human domain. AI systems are composing orchestral music, writing interesting screenplays, debugging software code, and generating compelling visual art. AI systems are automating factories, supercharging advertising, and making commercial travel more convenient. AI systems are also excelling in video games and competitive strategy games. It is a reasonable assumption that the automation of war is right around the corner. Why shouldn't war also become more efficient and precise, and why shouldn't robotic combatants become even faster and more creative?

Deep-learning technology is different, to be sure, but warfighting problems and warfighting organizations are as complex as ever. Software engineering is always hard, but it is even harder when software systems are expected to perform in situations that are infrequent, complex, and unpredictable. Sadly, the uncommon is common in combat.

Parnas focused mainly on technical points, but he directed his final criticism toward the Strategic Defense Initiative Organization that managed the program. He was troubled by "people telling me they knew the SDIO [Strategic Defense Initiative Organization] software could not be built but felt the project should continue because it might fund some good research."[39] These concerns are familiar to anyone who has studied the U.S. defense industry.[40] Parnas wrote that he was "astounded at the amount of money that has been wasted in ineffective research projects." He concluded that "[t]he SDIO [Strategic Defense Initiative Organization] is a typical organization of technocrats. It is so involved in the advocacy of the program that it cannot judge the quality of the research involved."[41] This concern is still relevant for modern AI research and procurement. Large-scale AI projects are still likely to be shaped by organizational imperatives for autonomy, resources, control, and identity, not simply pure strategic imperatives. Military services and defense contractors alike have political and economic incentives to oversell the potential of AI and undervalue the human work on which it depends.

In some ways, AI procurement pathologies may be even more acute today. The explosion of hype around commercial applications like ChatGPT creates a sense

[26] David Lorge Parnas, "Software Aspects of Strategic Defense Systems," *Communications of the ACM* 28, no. 12 (December 1985): 1326–35, https://doi.org/10.1145/214956.214961.

[27] Parnas, "Software Aspects of Strategic Defense Systems," 1330.

[28] Parnas, "Software Aspects of Strategic Defense Systems," 1328.

[29] Parnas, "Software Aspects of Strategic Defense Systems," 1327.

[30] Parnas, "Software Aspects of Strategic Defense Systems," 1328.

[31] Parnas, "Software Aspects of Strategic Defense Systems," 1329.

[32] James Jay Carafano, *GI Ingenuity: Improvisation, Technology, and Winning World War II* (Mechanicsburg, PA: Stackpole Books, 2006); Nina A. Kollars, "War's Horizon: Soldier-Led Adaptation in Iraq and Vietnam," *Journal of Strategic Studies* 38, no. 4 (2015): 529–53, https://doi.org/10.1080/01402390.2014.971947

[33] Parnas, "Software Aspects of Strategic Defense Systems," 1329.

[34] Lindsay, *Information Technology and Military Power.*

[35] Parnas, "Software Aspects of Strategic Defense Systems," 1329.

[36] Parnas, "Software Aspects of Strategic Defense Systems," 1332.

[37] Parnas, "Software Aspects of Strategic Defense Systems," 1334.

[38] Parnas, "Software Aspects of Strategic Defense Systems," 1332–33.

[39] Parnas, "Software Aspects of Strategic Defense Systems," 1334.

[40] Peter Dombrowski and Eugene Gholz, *Buying Military Transformation: Technological Innovation and the Defense Industry* (New York: Columbia University Press, 2006).

[41] Parnas, "Software Aspects of Strategic Defense Systems," 1335.

that the AI revolution is nigh. The great expectations for military AI in the Chinese and American defense communities create competitive incentives to invest in AI. And yet, the technical and institutional complexity of AI makes it hard for most policymakers or outside observers to evaluate claims about the military potential for AI. Science fiction tales of robot wars make it easy to "securitize" AI to sell parochial policies and products, just as myths of "cyber war" spurred major investment in cyber security.[42] The benefits of AI investment are concentrated for defense contractors and bureaucratic advocates, while skeptical views about the risks of procurement and operationalization are more diffuse. This is a recipe for the private capture of public resources.

The pessimism of Parnas remains relevant because it is ultimately grounded in political conditions, not just engineering considerations. More accurately, building computational systems is an inherently political activity that is based on strong, but usually tacit, assumptions about conflict and cooperation.[43] Most successful software engineering is predicated on cooperation among developers and users, to some degree, and everyone who maintains the economic ecosystem in which these systems will be employed. And many software systems break when competitors emerge from unforeseen places, subverting the means of cooperation to gain a competitive advantage.[44] Put simply, the political complements of AI dominate the potential for technological substitution.

The Economic Logic of AI

There is a burgeoning body of research on the economics of modern AI.[45] Here, I will simply highlight a few key findings and interpretations. The overarching theme is that AI performance depends on institutional complements. This section will flesh out the institutional conditions that facilitate AI in commercial settings. The next section will examine the challenges of meeting these conditions in military settings. The enduring importance of institutional complements helps to explain why the skeptism of Parnas still resonates for modern AI.

Economic models of decision-making typically highlight four components: data, prediction, decision, and action. In military command-and-control doctrine, these four components are known as the "OODA loop," a cybernetic cycle of observing, orienting, deciding, and acting. Information comes in from the world and is assimilated with stored information to produce models of the world. The system then makes decisions about how to achieve a goal by acting to change the state of the world. Here, "prediction" refers to the second step (orienting in the OODA loop) by inferring missing information from stored information.

All of the forms of AI that are getting so much attention today (i.e., machine learning or "narrow AI") are forms of automated prediction. The notion of artificial general intelligence, which carries the myth of substitution to its logical extreme by assuming superhuman autonomy, is still just science fiction. The statistical notion of prediction applies to actual prediction tasks, such as forecasting weather or planning navigation routes, as well as other forms of filling in missing information, as in classifying images or translating texts. Generative AI applications for producing text copy, software code, and graphical designs also rely on statistical prediction. This means that AI automates only part of the decision-making cycle. Robotics, moreover, may automate aspects of the action component of decision-making, such as running factory machinery or flying drones. And there are, of course, many automated sources of data available through the internet and remote-sensing systems.

Judgment, however, remains a consummately human task. The economic concept of judgment refers to ranking preferences over outcomes and determining the payoffs of choices. An AI weather forecasting system can tell you whether it is going to rain with some given probability, but it cannot decide whether you should bring an umbrella. That depends on whether you mind getting wet or find it a hassle to carry an umbrella whether it is wet or dry. These are value judgments that the AI system cannot make. The concept of judgment can be considered more broadly to encompass all manner of meaning, value, preference, or care.

[42] Myriam Dunn Cavelty, "From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse," *International Studies Review* 15, no. 1 (2013): 105–22, https://doi.org/10.1111/misr.12023.

[43] Geoffrey C. Bowker and Susan Leigh Star, *Sorting Things Out: Classification and Its Consequences* (Cambridge, MA: MIT Press, 2000); John Seely Brown and Paul Duguid, *The Social Life of Information* (Cambridge, MA: Harvard Business Press, 2000); Claudio Ciborra, *The Labyrinths of Information: Challenging the Wisdom of Systems* (New York: Oxford University Press, 2002); Laura DeNardis, *Protocol Politics: The Globalization of Internet Governance* (Cambridge, MA: MIT Press, 2009).

[44] Jon R. Lindsay, "Cyber Conflict vs. Cyber Command: Hidden Dangers in the American Military Solution to a Large-Scale Intelligence Problem," *Intelligence and National Security* 36, no. 2 (2021): 260–78 https://doi.org/10.1080/02684527.2020.1840746; Maschmeyer, "Subversion, Cyber Operations and Reverse Structural Power in World Politics."

[45] Covered extensively in Ajay Agrawal, Joshua Gans, and Avi Goldfarb, *Prediction Machines: The Simple Economics of Artificial Intelligence* (Cambridge, MA: Harvard Business Press, 2018); Ajay Agrawal, Joshua Gans, and Avi Goldfarb, eds., *The Economics of Artificial Intelligence: An Agenda* (Chicago: University of Chicago Press, 2019); Ajay Agrawal, Joshua Gans, and Avi Goldfarb, *Power and Prediction: The Disruptive Economics of Artificial Intelligence* (Boston: Harvard Business Review Press, 2022).

Technical trends in memory, algorithms, and computing power are making AI prediction better and cheaper. But this drop in the price of prediction means that the complements of data and judgment are becoming more valuable. To get AI systems to work, it becomes necessary to have a lot of high-quality, unbiased data. And it is necessary to figure out what to predict and how to act on predictions.

The quality of AI-supported decisions, therefore, will be determined by the quality of the data used to train AI and the quality of the judgments that guide them. Conversely, missing or biased data will lead to suboptimal system behavior. Decisions about appropriate action become challenging when there is political complexity or controversy in decision-making institutions. All the impressive AI achievements are in areas where companies have figured out how to solve the data and judgment problems, typically where decision problems can be very well constrained and lots of representative data can be collected. For other tasks, such as determining the mission and values of an organization, AI is of little use. Companies that figure out how to reorganize themselves to exploit AI complements, which entails investing in data infrastructure and rethinking decision-making processes, may potentially gain a competitive advantage. Substitution alone, however, will not provide a major advantage. AI substitution may even undermine performance if an organization or its environment are unable to accommodate it.

Organizations that want to adopt AI thus must make strategic decisions about organizational design and direction as well as ongoing operational decisions on a case-by-case basis.

A very important decision problem in this respect is understanding the distribution and flow of decision-making in an organization. Disaggregating decisions makes it possible for administrators to identify decision-making tasks that can be fully or partially automated versus those that must be performed by human beings. If a decision can be fully specified in advance — if X then Y — and if lots of data are available to classify situations — X or not X — then fully automated decision-making may be feasible. AI systems that play video games fall into this category: There is a clear goal of winning the game by getting the most points, and there are millions of previous games to learn from. Many successful implementations of AI, likewise, use automation at an abstract level but rely on human beings to make more fine-grained decisions at a local level. Thus, for instance, executives and engineers at a ride-sharing service have created a business model that can automate route-finding and billing in areas where there are standardized geospatial data available and lots of data about previous trips and rider demand patterns. But the human driver's judgment is still required for passenger safety and navigation in crowded, cluttered environments. Organizations that want to adopt AI thus must make strategic decisions about organizational design and direction as well as ongoing operational decisions on a case-by-case basis.

The challenge of business leadership lies in determining how and whether to reorganize decision-making to make the most of automation within a given economic niche. Many uses of AI, such as self-driving mining trucks on well-controlled routes, the replacement of taxi drivers, or quality-control devices in manufacturing, are still focused on substituting for human prediction tasks while providing complementary infrastructure for data and judgment. Platform innovation is akin to simply replacing steam engines with local dynamos, while systemic innovation entails the invention of assembly lines with distributed energy supplies.[46] We are still largely in the platform substitution phase of the commercial AI revolution, but major realignments may follow from the innovation of systemic complements. There are just a handful of industries, most notably in online advertising, that have fundamentally rearranged business processes and the industrial ecosystem to make the most of automated prediction.

In short, automated prediction depends on the economic complements of data and judgment. These complements, in turn, depend on permissive institutional conditions. Institutions are the human-built "rules of the game" that constrain and enable human beings to solve collective action problems.[47] "Sociotechnical" institutions include the "tools of the game." Data depend not only on data collection, processing, and communication infrastructure, but also on shared standards and technical protocols as well as access, quality control,

[46] Agrawal, Gans, and Goldfarb, *Power and Prediction.*

[47] Oliver E. Williamson, *The Economic Institutions of Capitalism: Firms, Markets, Relational Contracting* (New York: Free Press, 1985); Douglass C. North, *Institutions, Institutional Change, and Economic Performance* (New York: Cambridge University Press, 1990); Elinor Ostrom, *Governing the Commons: The Evolution of Institutions for Collective Action* (New York: Cambridge University Press, 1990).

and maintenance agreements. Judgment depends on organizational institutions to solicit opinions, develop ideas, adjudicate disputes, and socialize values. Therefore, AI performance depends on sociotechnical institutions. And the platform innovations of the future that unlock the productive potential of AI will fundamentally depend on complementary innovations in shared sociotechnical institutions.

Indeed, most command decisions depend thoroughly on diverse background knowledge and common sense, exactly the conditions that are not conducive for AI.

An underappreciated reason why we are seeing so much dramatic progress in AI is that national and global economies are more complex and institutionalized than ever before. Institutions create reliable conditions for exchange. They stabilize data collection protocols and processes for managing, sharing, and curating databases. They also create shared expectations about what political and economic actors want and how they will behave. The institutions that enhance shared data and collective judgment, in turn, depend on complex systems of shared norms, epistemic concepts, and political mechanisms for monitoring and enforcing agreements. The concept of a “global liberal order” can be understood as shorthand for this set of shared expectations, norms, and governance mechanisms. This shared institutional order is what makes AI viable commercially. Conversely, institutional distortions and failures should undermine the viability of AI.

The Political Logic of War

The political logic of war could not be more different. War, in the realist tradition of international relations, is associated with political anarchy.[48] In anarchy, there is no overarching government, and so actors must help themselves to survive and thrive. In anarchy, actors will lie, cheat, and steal, and there is no global court or policy to make them behave. War, conquest, and exploitation are always possible in this tragic world. This situation is the exact opposite of the liberal order described above. This means that the conditions that are most conducive for war are least conducive for AI performance.

AI performance depends on the institutional complements of data and judgment, but these same conditions are absent or elusive in war.[49] War is notoriously uncertain, surprising, and chaotic.[50] Combat is not simply risky because we have to assign probabilities to known variables.[51] It is more fundamentally uncertain because we do not always know what variables matter. Modern theories of war stress that uncertainty is a major — if not *the* major — cause of war.[52] Actors bluff about their power and may not keep to agreements, both of which can make fighting more attractive than peace. Still, wars are rare events. But this is another way of saying that the outbreak of war itself is prime evidence that the political system is unpredictable in some fundamental way. If we observe a war, then at least one actor, and probably more, must be confused about the true balance of power and interests. If this were not the case, they would prefer a deal to avoid the terrible costs and risks of war. War is inherently unpredictable, which does not bode well for prediction machines.

War is also controversial, obviously. Organizations and societies disagree enough to kill and be killed. Contestation includes not only external combat between armed adversaries but also, inevitably, many internal controversies as well. Different components of military organizations will disagree about doctrine or strategy. Different political factions of government will disagree about war aims and the conditions of negotiation. Different interest groups will disagree about what sorts of behavior and targets are legitimate, given the stakes of a conflict. Coordination and consensus are always hard in complex distributed organizations, but these tasks may be well-nigh impossible when the goal is the management of violence for politically consequential stakes. This means that the conditions of clear consensual judgment about strategies, missions, rules, limits, and ethics are especially difficult to achieve. This does not bode well for prediction machines, either.

A more fine-grained look at the conditions that are conducive for AI does little to relieve pessimism. Economist Erik Brynjolfsson and computer scientist Tom Mitchell describe eight general situations that are most amenable to automation with modern machine learning.[53] They provide more nuanced ways of talking about data and judgment. All of them are complicated in a military context:

1. *Learning a function that maps well-defined inputs to well-defined outputs.* This is rarely the case in war. Even in Carl von Clausewitz’s day, war was already a nonlinear combination of hundreds of relevant factors: “Bonaparte was quite right when he said that Newton himself would quail before the algebraic problems [war] could pose.”[54] The complexity of war today is exponentially greater. As Parnas pointed out with the Strategic Defense Initiative, there were challenging problems with “the number of independently modifiable subsystems, and with the number of interfaces that must be defined. Problems worsen when interfaces may change.”[55]
2. *Large (digital) data sets that contain input-output pairs exist or can be created.* Wars tend to have many unique features that resist systematic comparison. As Clausewitz wrote, “Countless minor incidents — the kind you can never really foresee — combine to lower the general level of performance so that one always falls short of the intended goal. … Moreover, every war is rich in unique episodes. Each is an uncharted sea, full of reefs.”[56] While training data for military AI systems can be generated on ranges and in exercises for some tactical scenarios, those systems are likely to encounter many surprises in real combat.
3. *The task provides clear feedback with clearly definable goals and metrics.* War colleges encourage strategists to define clear goals and objective measures of effectiveness. But in practice, goals are ambiguous, contested, and evolving, and military organizations default to measuring their own performance. Clausewitz again: “[W]ar turns into something quite different from what it should be according to theory — turns into something incoherent and incomplete.”[57]
4. *There are no long chains of logic or reasoning that depend on diverse background knowledge or common sense.* War, however, “is dependent on the interplay of possibilities and probabilities, of good and bad luck, conditions in which strictly logical reasoning often plays no part at all and is always apt to be a most unsuitable and awkward intellectual tool.”[58] Indeed, most command decisions depend thoroughly on *diverse background knowledge and common sense*, exactly the conditions that are not conducive for AI. Command judgment often has an intuitive and even creative aspect that can only be developed through experience in war and historical study: “Practice and experience dictate the answer: ‘this is possible, that is not.’”[59]
5. *There is no need for a detailed explanation of how the decision was made.* Commanders often press their subordinates to explain and justify their decisions as part of an “unequal dialogue” about the relationship between strategic ends and tactical means.[60] Staff officers and intelligence officers are expected to provide evidence supporting their assessments. Commanders and soldiers are held accountable for their decisions, and controversial ones may be investigated in courts martial. These norms are a matter of judgment.
6. *There is a tolerance for error and no need for provably correct or optimal solutions.* This condition appears to be easier to meet in war. Militaries make mistakes all the time — bombs miss their targets and civilians become casualties — and most commanders will not only tolerate but accept a degree of error as the price of doing business on the battlefield. Military solutions tend to be pragmatic and “satisficed” rather than optimal. But error tolerances may vary, for example, in conducting nuclear operations or a sensitive hostage rescue mission. This variance is also a matter of judgment, of course.
7. *The phenomenon or function being learned should not change rapidly over time.* This condition is particularly ironic given the popular assumption

[48] Hans J. Morgenthau, *Politics Among Nations: The Struggle for Power and Peace*, 3rd ed. (New York: A. A. Knopf, 1960); Kenneth N. Waltz, *Theory of International Politics* (Reading, MA: Addison-Wesley Pub. Co., 1979).

[49] Goldfarb and Lindsay, "Prediction and Judgment."

[50] Alan Beyerchen, "Clausewitz, Nonlinearity, and the Unpredictability of War," *International Security* 17, no. 3 (1992): 59–90, https://doi.org/10.2307/2539130.

[51] This type of uncertainty is associated with Frank H. Knight, *Risk, Uncertainty, and Profit* (New York: Houghton Mifflin Co., 1921).

[52] James D. Fearon, "Rationalist Explanations for War," *International Organization* 49, no. 3 (1995): 379–414, https://www.jstor.org/stable/2706903; Erik Gartzke, "War Is in the Error Term," *International Organization* 53, no. 3 (1999): 567–87, https://www.jstor.org/stable/2601290; Kristopher W. Ramsay, "Information, Uncertainty, and War," *Annual Review of Political Science* 20, no. 1 (2017): 505-527, https://doi.org/10.1146/annurev-polisci-051215-022729.

[53] Erik Brynjolfsson and Tom Mitchell, "What Can Machine Learning Do? Workforce Implications," *Science* 358, no. 6370 (December 2017): 1530–34, https://doi.org/10.1126/science.aap8062. The italicized sentences in the following numbered list are direct or lightly edited quotes from this article.

[54] Carl von Clausewitz, *On War*, trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), 586.

[55] Parnas, "Software Aspects of Strategic Defense Systems," 1329.

[56] Clausewitz, *On War*, 120.

[57] Clausewitz, *On War*, 580.

[58] Clausewitz, *On War*, 580–81.

[59] Clausewitz, *On War*, 120.

[60] Eliot A. Cohen, *Supreme Command: Soldiers, Statesmen, and Leadership in Wartime* (New York: Free Press, 2002).

that AI will speed up the pace of war. If so, then AI weapons will undermine a condition for their possibility. More generally, any campaign study will reveal that change is a constant part of war. Even the static fronts of World War I witnessed ongoing innovation in weapons and doctrine prior to the breakouts of 1918, but as innovation opposed innovation, the equilibrium was stalemate.

8. *No specialized dexterity, physical skills, or mobility is required.* War remains a physically demanding, even athletic, endeavor for its participants. Even staff officers find themselves engaging in "battlefield circulation" to inspect and correct local problems or enduring long hours and chronic strain in complex social spaces (i.e., headquarters). Systems break down constantly, requiring ongoing human intervention, repair, and adaptation.[61] Modern combined-arms warfare and "multidomain operations," moreover, require extensive maneuver.

The situations most amenable to automation, in sum, are very hard to meet in wartime scenarios. Nevertheless, we see plenty of military AI applications that have already been fielded or are soon to be deployed. We can point to examples of automated sensors, loitering munitions, and armed drones in use on battlefields today. Experimental prototypes of swarming drones, uncrewed submarines, and robotic wingmen further suggest the art of the possible. Even more applications of AI, but far less glamourous ones, can be found in the realms of logistics, administration, and intelligence. How do we explain this?

Military information systems work well when organizations adopt institutionalized solutions to stable problems.[62] Existing AI prototypes, likewise, work when there is adequate institutional scaffolding for problems that are well defined. What makes for a stable information problem? In practice, no war is completely unconstrained. Anarchy is not absolute. Armed conflict, surprisingly enough, often features some degree of mutual, even voluntary, constraint. Combatant behavior and expectations may be mutually constrained by geographical conditions, common infrastructures, shared practices, or normative institutions. Even the world wars featured coordination, and some outright cooperation, between feuding combatants.[63] Mutual constraints become more salient in more limited wars or in conflicts that are more constrained by civil societies. Each combatant organization and society, furthermore, is itself an institution, or set of institutions. Military organizations provide shared cultures and standard operating procedures. Military doctrine breaks down complicated operations into simpler steps, scripts, and templates. All this institutionalization in war is what creates the potential for generating data to enable AI systems to perform in well-defined combat scenarios.

The degree of institutionalization of a task, therefore, is what explains the potential for successful automation. Whenever it is easier to meet the conditions enumerated above, we should thus expect to find more promising candidates for military automation. When quality data are not available to inform prediction or judgments are ambiguous or controversial, by contrast, we are less likely to find attractive problems for automation. The scariest scenarios of fully autonomous robot armies may be simply impossible given the severe problems associated with wartime data and strategic judgment. Conversely, the areas of armed conflict that are most bureaucratized are the best candidates for automation. While lethal drones get all the attention, more promising applications may be found in the realms of logistics, administration, personnel, recruitment, medicine, civil affairs, intelligence analysis, and operations research. These categories of military activity have clear analogs in civilian organizations. They are insulated from battlefield turbulence, for better or worse, by a cocoon of standards, protocols, procedures, rules, and regulations. Even Clausewitz recognized the advantages here: "Routine, apart from its sheer inevitability, also contains one positive advantage. Constant practice leads to *brisk*, *precise*, and *reliable* leadership, reducing natural friction and easing the working of the machine."[64] Institutions that enable reliable, repeatable performance also enable automation.

However, many military applications, even the most routinized tasks, will still be difficult to fully automate. As Clausewitz observes, "War is not like a field of wheat, which, without regard to the individual stalk, may be mown more or less efficiently depending on the quality of the scythe; it is like a stand of mature trees in which the axe has to be used judiciously according to the characteristics and development of each individual trunk."[65] Military administration and staff work, as much as combat tasks, require the constant application of judgment. Therefore, while full automation may be possible in theory for some tasks (i.e., those that are standardized, regulated, doctrinal, bureaucratized), we should expect real automation to fall short of the ideal. War is complicated by ubiquitous friction and contingent historical circumstances.

Indeed, reliance on robots might send exactly the wrong message, precisely because the state literally has no skin in the game.

The most realistic scenarios of military automation involve teams of humans and machines.[66] Human beings take the output of prediction systems and then decide how to act on the prediction (or not). Many people are already using generative AI systems in this way to improve writing, coding, and graphic design. Human beings also must define what to predict in the first place, when to make the prediction, and how to act on it. This design work does not occur only in advance but also on an ongoing basis. Teamwork between people and machines should thus be understood expansively to include all of the support, maintenance, and repair activity required to keep AI infrastructure up and running. The use of AI systems to replace human prediction tasks in existing work processes (substitution) will still require a supporting ecosystem of human work. Human work will be even more salient for the innovation of new military decision-making processes, organizational models, and operational concepts (complements) that can better exploit the power of automated prediction.

The question here is not simply whether military organizations will automate tactical functions that are currently performed by human beings or couple automated classifiers with automated decisions about lethal effects. This is indeed possible and is already happening, to some extent. The extent of automation in any given case depends on the suitability of complementary institutions. To talk intelligently about AI, therefore, we must separate applications into more fine-grained tasks and determine which of them can or cannot be automated. It may not even make sense to talk about "military AI" as a coherent category. We should inquire instead into specific

[61] Meir Finkel, *On Flexibility: Recovery from Technological and Doctrinal Surprise on the Battlefield* (Stanford, CA: Stanford University Press, 2011); Kollars, "War's Horizon."

[62] Lindsay, *Information Technology and Military Power*, chap. 2.

[63] Jeffrey W. Legro, *Cooperation Under Fire: Anglo-German Restraint During World War II* (Ithaca, NY: Cornell University Press, 2013); James D. Morrow, *Order Within Anarchy: The Laws of War as an International Institution* (New York: Cambridge University Press, 2014).

[64] Clausewitz, *On War*, 153.

[65] Clausewitz, *On War*, 153.

[66] "Human-Machine Teaming," Chiefs of Staff Development, Concepts and Doctrine Centre, U.K. Ministry of Defence, Joint Concept Note 1/18, May 2018, https://assets.publishing.service.gov.uk/media/5b02f398e5274a0d7fa9a7c0/20180517-concepts_uk_human_machine_teaming_jcn_1_18.pdf; Scharre, *Army of None*; Goldfarb and Lindsay, "Prediction and Judgment."

task objectives and workflows, interdependencies across tasks and organizations, and data governance processes in order to understand the feasibility and dynamics of automation.

A more pressing question, from a strategic perspective, is how do automated weapons serve the political purposes of war? This question is fraught for AI since answers depend on judgments about whether, when, and to what degree to employ organized violence to settle political disputes.

For tactical prototypes, combat might be modeled as a game that is won by destroying more enemies while preserving more friendlies. Perhaps modern AI can excel in such games. But at the strategic or political level, war is about solving fundamental disputes. The concern here is not *only* that, as Kenneth Payne argues, "Warbots will make incredible combatants, but limited strategists."[67] In addition to AI's fundamental lack of understanding of the political purposes of and tradeoffs in violent conflict, it is further unclear how the ability of robots to win set piece battles would translate into political influence over human societies. War is a costly, and thereby effective, way of measuring the balance of power between actors who care about something enough to kill and die. But robotic systems enable a state to separate killing from dying, i.e., inflicting hurt while avoiding pain. The use of such systems may not be useful for communicating political resolve. Indeed, reliance on robots might send exactly the wrong message, precisely because the state literally has no skin in the game. It is not clear how costless combat can fulfil the political function of war as the final arbiter of disagreement.[68]

Distinguishing the tactical problems of combat from the political functions of war leads to slightly different questions. Do the motivations for war change with the automation of means? How do the political conditions that give rise to the onset, escalation, or duration of war relate to the economic conditions that support AI performance? Should we expect AI-enabled weapons to be most useful in traditional forms of conflict, which is where most of the research and development efforts and public debate seem to be focused? Or should we expect AI applications to be more prevalent in support of ambiguous or protracted contests in the "gray zone" between peace and war?

The Institutional Complexity of Automated Warfare

During the same century in which the commercial foundations of AI have been developing, long-term patterns of political violence have been shifting.[69] The same economic conditions that make modern AI possible are also associated with important changes in the incidence, intensity, and conduct of armed conflict. Classical liberal perspectives stress the pacifying effects of economic interdependence, which lead to lower rates of major interstate war.[70] As states become more invested in trade, and as war becomes more destructive, states become less interested in open conquest.

The classical perspective is incomplete, of course. The same globalizing developments are associated with an increase in other forms of conflict, typically described in terms of irregular war, hybrid war, gray-zone conflict, cyber conflict, covert action, terrorism, and other forms of political secrecy.[71] From a theoretical perspective, these sorts of conflicts take place *within* shared institutions rather than *between* them. Revisionists subvert or usurp societies from the inside, rather than conquering them from the outside. This means that the growth of global liberal order does not categorically reduce conflict. Instead, it alters its manifestation.

Perhaps this is good news, insofar as the risk of total war between nuclear powers becomes less likely. But it is still bad news for human security because civilians tend to bear the brunt of limited conflict and cyber aggression.[72] More robust institutions may enhance the rule of law in democracies, but more robust authoritarian institutions also improve the efficiency of state repression of civil society actors at home and abroad. Even advanced industrial democracies are tempted to expand executive power and enable more intrusive law enforcement. The traditional focus on interstate war tends to overlook intrastate violence. Yet, AI may very well be more consequential for the latter than the former.

It is an unappreciated paradox that the same historical trends that have produced viable commercial AI at scale are also associated with the increasing salience of gray-zone conflict, cyber insecurity, terrorism, subversion, sabotage, and counterintelligence. The current Russo-Ukrainian war, the largest episode of land warfare in Europe since World War II, may be an exception that proves the rule. And yet, Russia escalated because its prospects for winning in the gray zone were declining, and cyber conflict and information operations remain prevalent at the margins of the war.[73] A reasonable question, then, is whether there is some relationship between these two trends. Is there a common cause for the "graying" of conflict and the rise of AI? If so, what does the concurrent change in the nature or conduct of war mean for widespread worries about using certain weapons in war? This raises subtly different questions than those predicated on traditional models of combat.

The emergence of viable AI at scale is a product of global liberal order, which is an amorphous concept that describes a complex constellation of institutions for monetary policy, technical protocols and standards, the rule of law, and so on. The realist tradition of international relations, however, emphasizes that war tends to emerge where institutions are weak or irrelevant, i.e., in a state of political anarchy. So, what does it mean for us to imagine an AI-enabled war, given that the emergence of AI is best explained by liberalism while war is the consummately realist pursuit? Should we expect AI to work differently in this world, or conversely, should we expect war to take on a different form that is more conducive to AI? I cannot begin to answer these questions here. The dual institutionalization of AI and political conflict is an area ripe for further research. In the pages remaining, I will just speculate on a few possibilities, grounded in what we know about the organizational and strategic context of military technology.

As discussed above, research in economics has established that AI is *not* a simple substitute. AI performance — more precisely, the contribution of machine-learning prediction products to the efficiency of operational tasks — depends on the institutional complements of data and judgment. This will have important implications for military institutions. We should expect that the human support system for institutionalized prediction in military organizations will become ever more complex. This continues a long-term organizational trend toward greater complexity associated with greater reliance on information technology. It is perhaps better to understand AI, cyber security, and network-centric warfare as lesser-included features of a more general informational turn in military practice over the past several decades, rather than as independent revolutions in military affairs. All these informational innovations entail greater sociotechnical complexity.[74]

With more complex, distributed information systems, moreover, comes more potential for disagreement about goals and plans, bureaucratic politics and friction, and interagency and coalition coordination failure, to say nothing of enemy subversion and manipulation. Reliance on AI for almost any military task will require ongoing human intervention, tinkering, and negotiation. These activities are needed to modify system functionality and gain access to relevant data as operational circumstances take unexpected turns. These general tasks become even more difficult in an environment of classified and controlled information, which further exacerbates institutional complexity. AI theorists often emphasize the importance of having a "man in the loop" for any decision. This framing overlooks the fact that any real software system will be a tangled mess of many loops, and loops within loops. This is a longstanding challenge for enterprise software systems.[75] Increasing interdependencies in

[67] Payne, *I, Warbot*, 181.

[68] Erik Gartzke, "Blood and Robots: How Remotely Piloted Vehicles and Related Technologies Affect the Politics of Violence," *Journal of Strategic Studies* 44, no. 7 (2021): 983–1013, https://doi.org/10.1080/01402390.2019.1643329. Gartzke discusses the classic *Star Trek* episode, "A Taste of Armageddon," about warring planets that have agreed to spare themselves the cultural destruction of war by simulating combat instead and executing their own citizens. This scenario is predicated on an institutionalized dispute resolution process that is at odds with the anarchic nature of war. War works as a dispute resolution process precisely because it *works outside the rules.*

[69] John E. Mueller, *The Remnants of War* (Ithaca, NY: Cornell University Press, 2004); Steven Pinker, *The Better Angels of Our Nature: Why Violence Has Declined* (New York: Penguin, 2011); Azar Gat, "Is War Declining – and Why?" *Journal of Peace Research* 50, no. 2 (2013): 149–57, https://doi.org/10.1177/0022343312461023; Nils Petter Gleditsch et al., "The Forum: The Decline of War," International Studies Review 15, no. 3 (September 2013): 396–419, https://doi.org/10.1111/misr.12031; Bear F. Braumoeller, *Only the Dead: The Persistence of War in the Modern Age* (New York: Oxford University Press, 2019)

[70] John R. Oneal et al., "The Liberal Peace: Interdependence, Democracy, and International Conflict, 1950-85," *Journal of Peace Research* 33, no. 1 (1996): 11–28, https://www.jstor.org/stable/425131; John R. Oneal, Bruce Russett, and Michael L. Berbaum, "Causes of Peace: Democracy, Interdependence, and International Organizations, 1885–1992," *International Studies Quarterly* 47, no. 3 (2003): 371–93, https://www.jstor.org/stable/3693591; Erik Gartzke, "The Capitalist Peace," *American Journal of Political Science* 51, no. 1 (January 2007): 166–91, https://www.jstor.org/stable/4122913; Robert O. Keohane and Joseph S. Nye, Jr., *Power and Interdependence*, 4th ed. (Boston: Pearson, 2011); Erik Gartzke and Oliver Westerwinter, "The Complex Structure of Commercial Peace Contrasting Trade Interdependence, Asymmetry, and Multipolarity," *Journal of Peace Research* 53, no. 3 (2016): 325–43, https://doi.org/10.1177/0022343316637895.

[71] Michael Poznansky, *In the Shadow of International Law: Secrecy and Regime Change in the Postwar World* (New York: Oxford University Press, 2020); Drezner, Farrell, and Newman, *The Uses and Abuses of Weaponized Interdependence*; Allison Carnegie, "Secrecy in International Relations and Foreign Policy," *Annual Review of Political Science* 24, no. 1 (2021): 213–33, https://doi.org/10.1146/annurev-polisci-041719-102430; Farrell and Newman, *Underground Empire*; Nadiya Kostyuk and Erik Gartzke, "Fighting in Cyberspace: Internet Access and the Substitutability of Cyber and Military Operations," *Journal of Conflict Resolution* (March 2023), https://doi.org/10.1177/00220027231160993; Gannon et al., "Shadow of Deterrence."

[72] Lennart Maschmeyer, Ronald J. Deibert, and Jon R. Lindsay, "A Tale of Two Cybers: How Threat Reporting by Cybersecurity Firms Systematically Underrepresents Threats to Civil Society," *Journal of Information Technology & Politics* 18, no. 1 (2021): 1–20, https://doi.org/10.1080/19331681.2020.1776658; Florian J. Egloff and James Shires, "The Better Angels of Our Digital Nature? Offensive Cyber Capabilities and State Violence," *European Journal of International Security* 8, no. 1 (2023): 130–49, https://doi.org/10.1017/eis.2021.20.

[73] Gannon et al., "Shadow of Deterrence."

[74] Allard, *Command, Control, and the Common Defense*; Chris C. Demchak, *Military Organizations, Complex Machines: Modernization in the U.S. Armed Services* (Ithaca, NY: Cornell University Press, 1991); Rochlin, *Trapped in the Net*; Lindsay, *Information Technology and Military Power,* chap. 1.

[75] Frederick P. Brooks, Jr., *The Mythical Man-Month: Essays On Software Engineering*, Anniversary Edition (Reading, MA: Addison-Wesley Longman, Inc., 1995); Ciborra, *The Labyrinths of Information.*

AI systems, data sources, and client organizations, in an environment of fierce interagency competition and coalition negotiation, will make coordination problems more difficult.[76] Greater adoption of AI, therefore, will simply exacerbate a decades-long trend in military organizations of increasing complexity, coordination problems, and dependence on human capital. In short, more reliance on AI for even mundane military tasks will make military organizations *more* reliant on people, not less.[77]

We can carry this analysis up to the political level. The discussion above suggests a simple argument: If AI performance depends fundamentally on quality data and clear judgment, and if military organizations that depend on AI thus depend more on data and judgment, then data and judgment will become critical strategic resources in political conflict, and adversaries will alter their strategies to complicate and contest data and judgment processes. The very institutional complements that make it possible to use AI in war will change the ways in which that same war will be fought.

Future research should explore not only the ways in which AI changes the technology and tactics of war but also how it interacts with concurrent changes in the strategy and politics of war.

What does this mean in practice? It means that cyber security and disinformation, which are already prominent and incredibly challenging features of modern war, will become even more of a problem in conditions of intensive automation. Adversaries have incentives to manipulate or poison the data that feeds AI systems.[78] AI will thus expand the range of counterintelligence risks to worry about. It also means that adversaries have incentives to move conflict in unexpected directions, i.e., where AI systems have not been trained and will likely perform in undesired or suboptimal ways. This creates not only data problems but judgment problems as well. Combatants will have to reconsider what they want in challenging new situations. As intelligent adversaries escalate conflict into new regions, attack new classes of targets, or begin harming civilians in new ways, how should AI targeting guidance change, and when should AI systems be withheld altogether? We should expect adversaries facing AI-enabled forces to shift political conflicts into ever more controversial and ethically fraught dimensions.

Adversaries facing automated armies may elect to avoid direct engagements altogether. After all, it may be impossible for the target of automated weapons to determine whether the enemy is fighting with robots because robots are the most effective means or because the enemy is afraid of losing human lives. War is a test of resolve, but automated weapons provide no information about how much their owners are willing to suffer. Targets of automated weapons may thus try to get this information from somewhere else. They might attempt to measure resolve by instead targeting civilians, expanding the war to other regions where robots are not used, or protracting the war to impose more costs over time. We already see some evidence of this dynamic at work in U.S. drone campaigns.[79] At the end of the day, the politics of violence is not only about the ability to kill — which tactical AI forces can do well — but also about the willingness to die — about which the use of automated forces says less than nothing.

A terrible irony is that the use of AI to fight decisive tactical engagements, at reduced risk to military personnel, is likely to result in more drawn-out political conflicts, with increased suffering for civilians. This is not simply a problem of bad targeting guidance or failing to incorporate ethical precepts in lethal control systems, which are the usual focuses of conversations about the responsible use of military AI. The problem is rather that the strategic incentives for inflicting violence change together with material changes in the tactical conduct of war. The underlying political problem here is that AI is a product of stable institutions, but war is a product of anarchy. The conditions that make AI performance better also make traditional war less likely. Conversely, the conditions that allow war to persist or escalate also make it harder to use AI systems in reliable ways. Many just-so stories about automated robots engaging in decisive set-piece battles (or even "man in the loop" or "centaur" systems) are based on a political fantasy. Armed conflict — the reduction of political uncertainty through physical violence — is more likely to emerge in areas where AI systems cannot be used effectively, if they can be used at all.

So far, I have emphasized the unintended consequences of military AI for international conflict. But this may not even be the most salient growth area for AI-enabled political violence. Indeed, if the institutional factors of data and judgment are necessary complements for AI, we should expect to see the most promising applications of AI where institutional complements are most robust. AI is an institutional innovation that will help to make strong institutions even stronger. Sadly, this is great news for authoritarians and bad news for civil society. A sweet spot for political applications of AI is the combination of censorship and surveillance infrastructure with internal security operations, especially in societies where there are limited privacy protections and consensus within the regime about its imperatives for survival. AI can be expected to supercharge the chronic counterintelligence siege against subversives, real or imagined. AI thus expands the dragnet for political repression. Again, the key factors here are more institutional than merely technical. The imposition of authoritarian control is the ultimate form of conflict within common societal institutions. AI is not only attractive but viable in authoritarian societies (and in democracies with authoritarian tendencies).

Future research should explore not only the ways in which AI changes the technology and tactics of war but also how it interacts with concurrent changes in the strategy and politics of war. This shift of focus may lead to a different set of ethical, operational, and strategic concerns. As military planners and antiwar activists alike focus on applications of AI for high-end conflict, they may be missing some of the most likely and most pernicious applications of AI in political conflict. It would be tragic to succeed in coming to an agreement about the responsible use of *robots* in major combat operations only to fail to consider the ways in which the same technologies encourage *humans* to behave less responsibly in war.

Judgment Day

Rather than worrying about an AI-enabled apocalypse like "Judgment Day" in the *Terminator* movies, we should be more concerned with the day-to-day judgments that enable complex organizations to muddle through complex environments. AI systems will have to perform in the quotidian world of military bureaucracy, which becomes more necessary than ever to provide data and judgement for military AI.

Each generation of AI has encouraged hopes and fears about military automation. AI hype has typically been followed by disappointed expectations, a few practical applications, and greater institutional complexity. Given the dramatic advances in the world of commercial AI today, many are tempted to assume that this time will be different. But I expect that the future of military AI will resemble its past in many ways.

Great expectations of faster, more decisive, automated war will continue to emerge with every new advance in AI technology (and in information technology more broadly). Commercial successes of AI, moreover, will supercharge those expectations, which will encourage paranoia about shifting balances of power, as well as slicker defense marketing and greater defense spending. Meanwhile, the problems of implementing information systems in complex national security organizations will continue to grow ever more wicked. Twenty-first century military organizations will continue to become more reliant on the civilian economy, civilian technology, and civilian skills. But real wars — and proliferating conflicts short of war — will continue to be as full of friction and as politically frustrating as ever. The only difference is that the increasing complexity of sociotechnical implementations of AI systems will generate even more friction, to include even more opportunities for adversaries to cause friction.

We should thus prepare to be disappointed by AI. Preparation for disappointment can be understood in at least two ways. First, military AI systems will fail to live up to the hype, as they have for over 50 years. Second, because AI systems will not perform as well as their designers intend them to perform, organizations using AI should be prepared to respond creatively and proactively in changing circumstances. Military organizations should prepare and empower their personnel to intervene, adapt, and repair the information infrastructure that enables and constrains AI performance. Military practitioners will also have to sustain an ongoing conversation about what to predict and what to do with predictions. While there is real potential to improve the efficiency of some military tasks, doing so will depend on empowering people to make the most of automated prediction. In lowering our expectations for what AI systems can do, therefore, we also must raise our expectations for what human personnel can do.

The most promising military applications of AI, ironically enough, are in the aspects of war that most resemble peace. These are the boring administrative and logistical parts of the military enterprise

[76] Risa Brooks, "Technology and Future War Will Test U.S. Civil-Military Relations," *War on the Rocks*, Nov. 26, 2018, https://warontherocks.com/2018/11/technology-and-future-war-will-test-u-s-civil-military-relations/; Erik Lin-Greenberg, "Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making," *Texas National Security Review* 3, no. 2 (Spring 2020): 56–76, http://dx.doi.org/10.26153/tsw/8866.

[77] Goldfarb and Lindsay, "Prediction and Judgment."

[78] Heather Roff, "AI Deception: When Your Artificial Intelligence Learns to Lie," *IEEE Spectrum*, Feb. 24, 2020, https://spectrum.ieee.org/automaton/artificial-intelligence/embedded-ai/ai-deception-when-your-ai-learns-to-lie.

[79] Erik Gartzke and James Igoe Walsh, "The Drawbacks of Drones: The Effects of UAVs on Militant Violence in Pakistan," *Journal of Peace Research* 59, no. 4 (2022): 463–77, https://doi.org/10.1177/00223433211044673.

rather than the exciting combat tasks. While the latter garners all the attention in strategic and ethical debates about AI, the former is implicated in more significant long-term organizational changes in the conduct of military operations. There is also, perhaps, some potential for AI in conflicts in the "gray zone" between peace and war, where adversaries struggle within shared systems and with shared resources and assumptions, as well as for improving authoritarian repression through censorship and surveillance. What these developments have in common — greater organizational complexity, more strategic controversy, and more intrusive social control — is greater institutionalization. Large-scale military AI will only be viable if military organizations supply a greater degree of institutionalization themselves, or if they fight (or repress fighting) in more institutionalized environments.

AI relies on large-scale data and stable collective judgments. But these same conditions are elusive in war.

There is a fundamental paradox lurking in the hype about military AI. The political circumstances that are most conducive for automated prediction are in tension with the political circumstances that give rise to violent conflict. AI relies on large-scale data and stable collective judgments. But these same conditions are elusive in war. Most examples of commercial or governmental AI success to date are grounded in the pervasive institutionalization of capitalist infrastructure in a global liberal order. Global information infrastructure, collectively produced and maintained, is the product of extensive social cooperation that is unequalled in human history. AI, to put it glibly, is an economic product of peace. But war destroys the conditions that make AI viable. The conditions that are conducive for AI are not conducive for war, and vice versa. This strategic complementarity embodies a contradiction between the political conditions that are conducive for AI performance and the conditions that are conductive for the onset, duration, and escalation of war.

Reliance on the technology of peace for the politics of war is sure to lead to unintended consequences. The silver lining is that the same conditions that are creating so much fantastic progress in AI are also reducing the attractiveness of major-power war. There are gray clouds, of course, which are currently gathered over Ukraine and Gaza, because modern militaries can still go to war with traditional weaponry and ignore AI altogether. Another gray cloud is that globalized institutional interdependence is increasing the opportunities for subverting societies and abusing human security. If AI is the future of war, then the dark side of the liberal order is about to get darker still.

Jon R. Lindsay *is an associate professor at the School of Cybersecurity and Privacy and the Sam Nunn School of International Affairs at the Georgia Institute of Technology. He is the author of* Information Technology and Military Power *(Cornell, 2020) and coauthor of* Elements of Deterrence: Technology, Strategy, and Complexity in Global Politics *(Oxford, 2024). His latest book project is* Age of Deception: Cybersecurity and Secret Statecraft.

Image: *Christiaan Colen* (CC BY-SA *2.0 DEED*)[80]

[80] For the image, see https://flickr.com/photos/christiaancolen/21382575392/. For the license, see https://creativecommons.org/licenses/by-sa/2.0/.