CONTENTS

Preface vii
Acknowledgements xi

- 1 Robot Wars 1
- **2** What AI Can Do 23
- **3** AI Strategy 43
- 4 A Military-Tech Complex 60
- 5 The Special Relationship 82
- **6** AI and Planning 99
- **7** AI and Targeting 115
- 8 AI and Cyber Operations 131
- **9** The Human-Machine Team 149
- **10** War at the Speed of Light 166

Notes 185 Bibliography 205 Index 219

1

Robot Wars

The New Prometheus

Are we witnessing the birth of a new Prometheus? In 2005, computer scientist and futurist Ray Kurzweil declared that 'the singularity was near'.¹ He believed that computer superintelligence would appear within three decades and, therefore, that machines were about to transform civilization in ways we could only begin to imagine. In 2024, he remained convinced of the epochal powers of artificial intelligence (AI). The 'singularity' was, for him, even nearer.² He predicted that with the help of AI, 'We are going to extend our minds many millions-fold by 2045'.³

There is little doubt that in the last two decades AI has developed startling—near miraculous—powers. Kurzweil is not alone in his belief that AI will transport humans to a new era. James Lovelock, the celebrated originator of the Gaia Theory, believes that the Anthropocene, the age of humans, is over: we are at the dawn of the Novacene, an age in which AI will control and manage humans' lives. AI could soon function a million times more quickly than the human brain. Eventually, according to Lovelock, the Novacene will regulate the 'chemical and physical conditions to keep the Earth habitable for cyborgs'. In his recent bestseller, *The Coming Wave*, Mustafa Suleyman, an AI pioneer and one of the founders of DeepMind, professed a similar view of AI: 'And now we stand at the brink of another such moment as we face the rise of a coming wave of technology that includes both advanced AI and biotechnology. Never before have we witnessed technologies with such transformative potential, promising to reshape our world in ways that are both awe-inspiring and daunting'.

Suleyman is well-placed to know whether we are, indeed, on the edge of an AI revolution. The London-born son of a Syrian taxi driver and an English

2 CHAPTER 1

nurse, he was abandoned at sixteen. He then gained a place at Oxford University to study philosophy but dropped out before beginning to work on AI, a field in which he became a major figure. Indeed, he was integral to an event which is widely regarded as one of the seminal moments in the advance of AI in the last decade: he helped to develop AlphaGo, the AI program which defeated the world Go champion in 2016. AlphaGo was a remarkable achievement. Even after IBM's Deep Blue defeated Garry Kasparov, the world chess champion, in 1997, experts claimed that 'it may be a hundred years before a computer game beats humans at Go—maybe longer',6 because Go is a far more complex game than chess. Go is played on a board of 324 squares. Players place black and white stones on any of the interconnections between the squares, with a view to surrounding each other's pieces. The player who surrounds more of the other player's pieces wins. Go, therefore, has a vastly greater number of potential moves than chess does. After three pairs of moves in a game of chess, there are about 121 million possible configurations; after three moves in a game of Go, there are on the order of 200 quadrillion (2×10^{17}) possible configurations. Experts' scepticism was not wholly misplaced.

Yet the experts were wrong. In 2010, Demis Hassabis, Mustafa Suleyman, and Shane Legg set up a small tech company called DeepMind. They were interested in exploring the possibility of developing artificial general intelligence; as Suleyman put it, 'We wanted to build truly general learning agents that could exceed human performance at most cognitive tasks'.8 It was a hugely ambitious undertaking. In 2013, DeepMind developed an algorithm, Deep Q-Network, which could play Atari computer games. The success of Deep Q-Network attracted the attention of major companies in Silicon Valley, and in 2014 Google bought DeepMind. In 2015, the DeepMind team began to work on AlphaGo, training the program by having it watch 150,000 games of Go. Initially, the computer failed badly in its attempts to play the game. Gradually it learnt on massive datasets, teaching itself a system purely on the basis of trial and error. Because it was a computer program, it could run through games almost infinitely. Eventually, on 15 March 2016, AlphaGo beat world champion Lee Sedol in a five-game series, 4-1. Famously, in move 37 of game 3, AlphaGo made an extraordinary play, positioning a stone on its own on the edge of the board. Amazed observers declared, 'It's not a human move'. 10 Sedol was plainly disturbed by the unexpected move, and AlphaGo went on to win the game. What was most striking was not just that a computer program had learnt to play Go but that it seemed to have developed a creativity that exceeded the imagination of even the best human player.

AlphaGo was designed purely to play a game. The program was thus, in a certain sense, trivial. Yet the evidence for an AI revolution is becoming incontrovertible. AI has already made major contributions to scientific and medical research, fields in which it has affected the lives of perhaps millions and will

soon affect the lives of billions. Since 1972, biologists have been working on the problem of protein structure: 'Determining the crumpled shapes of proteins based on their sequences of constituent amino acids has been a persistent problem for decades in biology. Some of these amino acids are attracted to others, some are repelled by water, and the chains form intricate shapes that are hard to accurately determine'. In 2020, DeepMind announced that AlphaFold, a program created to identify new chemicals, had developed a method of mapping the structure of folded proteins. By the middle of 2021, the program had mapped 98.5 per cent of the proteins in the human body. AlphaFold had solved the problem of protein folding in just eighteen months. In 2021, I

AI programs now routinely read scans for cancer more accurately than doctors do. 13 AI may have even more radical medical uses. One of the pressing needs of modern medicine is to develop new drugs to overcome antibioticresistant bacteria. The Broad Institute at MIT and Harvard, led by Dr Felix Wong, has used AI to make major progress in this area.¹⁴ As Jeremy Hsu has described, Wong's team 'tested the effects of more than 39,000 compounds on Staphylococcus aureus and three types of human cells from the liver, skeletal muscle and lungs. The results became the training data for AI models to learn about the patterns in each compound's chemical atoms and bonds. That allowed the AIs to predict both the antibacterial activity of such compounds and their potential toxicity to human cells. The trained AI models then analysed 12 million compounds through computer simulations to find 3646 compounds with ideal drug-like properties'. Wong explained the significance of AI to the research: 'Our [AI] models tell us not only which compounds have selective antibiotic activity, but also why'. Because AI can process huge quantities of data, plotting thousands of variables, it is able to identify patterns which are quite undetectable to human researchers. Humans simply cannot hold all those variables in their minds. Consequently, AI programs have detected new molecular qualities, identifying relations between a molecule's structure and its antibiotic capacity that humans had neither perceived nor defined. Algorithms have been employed with increasing success in many other fields, including oceanography, in which they have been trained to distinguish between submarines, mines, and sea-life better than humans can.16

AI has also become integral to business and commerce. It has been essential to the competitive advantage of the largest companies.¹⁷ The rise of Amazon is substantially due to data and AI. Amazon's algorithms have automated buying and selling, and, as a result, they have been able to predict consumers' tastes on the basis of the things that other customers, with similar data profiles, have bought.¹⁸ Walmart has also successfully harnessed the predictive power of AI. Walmart's algorithms noted that when a hurricane was announced, consumers in the American South stocked up on Pop-Tarts (likely because Pop-Tarts are easy to prepare and are high in calories). As Linda Dillman, Walmart's chief

4 CHAPTER 1

information officer, observed, 'Strawberry Pop-Tarts increase in sales, like seven times their normal sales rate, ahead of a hurricane'. ¹⁹ Consequently, Walmart shipped more of that product to its stores in the affected states when a hurricane warning was issued.

A similar transformation has been evident in financial markets. Originally, the stock market consisted of human traders physically communicating with each other on the trading floor and exchanging notes documenting the deals they had done in real time, face to face. The process involved famously chaotic scenes in which jacketed traders gesticulated and shouted at one another. In the 1980s, stock markets became predominately computerised; exchanges began to be communicated over email. Electronic trading displaced physical trading. In 2006, entrepreneurs recognised the potential of high-volume electronic trading. High-volume trading involved thousands of small transactions which exploited small price shifts in the market. Traders sold and bought rapidly as prices rose and fell; speed was everything. Since trading had already been digitised—it was electronic—high-volume traders realised that algorithms might be developed to compute and execute trades; software could process financial data far more quickly and accurately than humans could. As a result, from 2006, high-volume traders automated their activities, employing algorithms to sell and buy shares 'at the speed of light'. ²⁰ The stock exchange has been revolutionised by AI; buyers and sellers are connected digitally. Sales are now processed automatically.

AI's progress shows no sign of slowing. On the contrary, it has been exponential and self-reinforcing. On 30 November 2022, OpenAI released Chat-GPT, a large generative language model capable of trawling the entire internet for data and producing useful responses to prompts. Many people see generative AI as the next breakthrough. Indeed, some hope that generative AI will help to alleviate poverty in the developing world, by increasing education and economic productivity: 'AI stands to transform lives in the emerging world, too. As it spreads, the technology could raise productivity and shrink gaps in human capital faster than many before it'.21 In the global south, a lack of teachers, educators, doctors, engineers, and managers is a major obstacle to development; 'AI could ease this shortfall, not by replacing existing workers, but by helping them become more productive'. ²² Locals could draw on AI to help bridge the gaps in expertise. AI might act as a proxy teacher or doctor for locals, accessing the internet for help. For instance, Tonee Ndungu, an entrepreneur in Kenya, has developed two apps to help children learn through engaging with a chatbot.²³ In the West, too, many leaders have advocated AI as a way of transforming the economy and improving the well-being and livelihoods of citizens. For instance, in 2023 the UK prime minister Rishi Sunak, in response to worries about economic stagnation after Brexit, declared that AI represented 'one of the greatest opportunities for the UK': 'Combined with the

computational power of quantum we could be on the precipice of discovering cures for diseases like cancer and dementia or ways to grow crops that could feed the entire world.²⁴

It is difficult to predict how AI will evolve even in the next five years. As a result of advances in AI, humanity is now on the edge of a Fourth Industrial Revolution. The powers of computing, data, and digital communications—all enhanced, enabled, and integrated by AI—are converging to transform every aspect of human existence, just as coal, electricity, and nuclear power successively transformed society in previous eras. A new Prometheus is appearing.

Frankenstein's Monster

Or perhaps, rather than a Prometheus, we are waking a monster. Experts in the field of computing have highlighted the dangers AI may pose. For instance, in an interview with The New York Times in May 2023, Geoffrey Hinton, one of the pioneers of neural networks and a seminal figure in the development of machine learning (ML), confessed his fears that AI was approaching a tipping point, when the interconnection of existing systems might trigger the rise of a new class of intelligence. Computers, he said, by sharing their data automatically with each other, could soon become vastly more intelligent than humans: 'Whenever one [model] learns anything, all the others know it. People can't do that. If I learn a whole lot of stuff about quantum mechanics and I want you to know all that stuff about quantum mechanics, it's a long, painful process of getting you to understand it'. Indeed, Hinton described AI as not just troubling but an 'existential threat'. In the near future, he feared, AI would be harnessed neither to play games, nor to make medical advances, but for war. He urged, 'What we want is some way of making sure that even if they're smarter than us, they're going to do things that are beneficial for us', adding, 'but we need to try and do that in a world where there [are] bad actors who want to build robot soldiers that kill people. And it seems very hard to me'.25 Hinton warned that AI may be used for military purposes. Indeed, AI may automate war, as killer robots, directed by non-human machine intelligence, take over. By February 2024, Hinton's fears had increased. He said: 'If I were advising governments, I would say that there's a 10 per cent chance these things will wipe out humanity in twenty years. I think that would be a reasonable number'.26

Hinton might be considered alarmist. Nevertheless, it is striking that many policymakers and scholars who are experts on strategy and security have also worried about the development of AI and its implications for war. They too fear the automation of war. The former US secretary of state Henry Kissinger has been prominent here. Kissinger, controversial though he is, was probably the most important Western diplomat, strategist, and strategic thinker

6 CHAPTER 1

of the late twentieth century. He was well-placed to make a judgement about the strategic implications of AI for global security. In one of his final acts as a public figure, Kissinger expressed his worries about AI. In 2021, just two years before he died, he published a book with Eric Schmidt and David Huttenlocher about AI and 'our human future'. Kissinger's choice of co-authors was well considered. Schmidt has had a long and illustrious career in Silicon Valley and is profoundly aware of the potential of AI. He served as CEO of Google from 2001 to 2011 and subsequently chaired the Defense Innovation Board and the National Security Commission on Artificial Intelligence (NSCAI) in Washington. Huttenlocher is the dean of computing at MIT, having previously served as the dean of Cornell Tech; both are new centres dedicated to the analysis of digital technology and AI. The book is, then, a statement from a pre-eminent strategist and two tech and AI specialists. It is an important contribution.

In The Age of AI and our Human Future, Kissinger, Schmidt, and Huttenlocher avoid the jeremiads of which Hinton is perhaps guilty. They explore the question of how AI will change strategy and the prosecution of war as a political enterprise. In the near future, might AI replace human strategic judgement? Might computers decide when, where, and how to fight wars? The authors' assessment of the political implications of AI for strategic affairs is sobering: 'Only very rarely have we encountered a technology that challenged our prevailing modes of explaining and ordering the world. But AI promises to transform all human experiences'. 27 It is predicted that 'the introduction of non-human logic to military systems and processes will transform strategy'. If the armed forces accrue an advantage from using AI, then they will surely use it—even if only to defend themselves from those states which do use AI. Yet the perils of AI are clear. The authors are particularly concerned with cyberwarfare, lethal autonomous systems, and nuclear weapons. AI operates at a speed which no human can achieve, offering very real benefits to states and their armed forces. The authors warn that if AI gains control of weapons, including nuclear weapons, the norms of deterrence which have operated since 1945 would collapse. The rationale and motivations of AI might be different to those of humans: 'In contrast to the field of nuclear weapons, no widely shared proscription and no clear concept of deterrence (or of degrees of escalation) attend such uses of AI-assisted weapons [...] Such reliance will introduce unknown or poorly understood risks'.28

Kissinger, Schmidt, and Huttenlocher are therefore disturbed by the prospect of the automation of war, a scenario in which AIs, not humans, develop strategy and prosecute war. In the context of interstate competition, military automation carries many risks. The authors declare that, in order to keep humans in control of lethal weapons, 'We will need to overcome, or at least moderate, the drive to automaticity before catastrophe ensues'. They conclude, 'Defence will have to be automated without conceding the essential elements

of human control'.²⁹ States need to employ AI, but they must also mitigate and control it.

Kissinger, Schmidt, and Huttenlocher are perhaps the most prominent strategic commentators to address the question of AI. Yet they are certainly not alone among strategic experts in their disquiet that AI is about to automate strategy. Many other scholars believe that AI will inform and even automate strategy. In the last decade, the British military scholar Kenneth Payne has been an eloquent voice in these debates. In a series of books and articles exploring the automation of strategy and war, Payne concurs with Kissinger, Schmidt, and Huttenlocher. In the past, human commanders have been inhibited by a range of emotional commitments. They have been scared to put themselves or their troops at risk; fear has emasculated decision-making. In many cases, imagined fears have been crippling. Pity and morality have also constrained decision-making. Commanders have often sought to preserve human life. On other occasions, hatred and vengeance have compelled extreme actions which have no military logic. For Payne, AI potentially cures these strategic inhibitions: 'AI is primarily a decision-making technology. Its effect is on the nature of warfare, insofar as it alters the long-standing human psychology of the decisions made in combat'. That is, AI will not be hampered by the foibles of human psychology. AI will calculate the strategic situation entirely on the basis of a logical analysis of the data, in order to make rational decisions. It will make strategic decisions quickly and accurately to execute those decisions instantaneously. Consequently, 'AI alters the nature of war by introducing non-human decision-making'. 31 War will become an automated competition between computers, not a visceral struggle between peoples.

It is a radical claim, but other scholars have concurred. For instance, the political scientist and arms control expert Denise Garcia echoes Payne exactly: 'The development of artificial intelligence and its uses for lethal purposes in war will fundamentally change the nature of warfare'. ³² In her recent monograph, she claims that 'militarised artificial intelligence' represents an existential threat. She believes that AI will determine how, when, and where wars are fought: 'What is at stake is the potential loss of human control to machines that will kill autonomously in response to an algorithm, with no humans involved'. ³³ For Garcia, the only solution to this future is regulation and human control.

Roberto Gonzalez, a military anthropologist, also decries the military application of AI. Unlike Garcia, he claims that the pursuit of AI is practically misguided; AI is not nearly as effective as military leaders believe. Yet the armed forces are on a 'quest for the automated battlefield'³⁵ and are actively committed to using AI to automate their operations.

In his work on AI and military decision-making, James Johnson has also warned that military automation, and the substitution of human commanders by AI, is imminent. Like Gonzalez, he rejects the claim that AI might perform

8 CHAPTER 1

the functions of human commanders. He insists, 'Machines cannot reliably complement or augment, let alone replace, the role of humans in command decision-making'.36 War is non-linear, unpredictable, and chaotic; AI models are unsuited to the complexity of military decision-making. Nevertheless, Johnson believes that, because of weaknesses in human psychology, AI will begin to assume command responsibilities. In a crisis situation, where there is an overwhelming amount of data, humans are liable to place a false trust in AI. They will become victims of the 'automation bias'; they will defer to AI because they are uncertain what to do themselves. Consequently, 'as deep human-machine symbiosis alters and shapes the psychological mechanisms that make us who we are, thus as they learn and evolve, AI agents will likely become—either inadvertently or more probably by conscious choice—de facto strategic actors in war'.³⁷ Johnson continues: 'The logical end of this trajectory is an AI commander planners, warfighters, and tacticians. The danger is that decision-makers may seek to reconcile the paradox of war by outsourcing our consciences in the use of lethal force to non-human agents who are ill-equipped to fill this ethicalmoral void'. 38 The literature is troubling. Many scholars believe that artificial intelligence is about to assume the role traditionally taken by human commanders and political leaders; AI will make the decisions. AI will arrogate the fatal decision of whether to go to war. AI will assume the role of politician and commander-in-chief. AI will automate strategy. War itself will be directed not by humans but by machines.

Kissinger, Schmidt, and Huttenlocher, and all these other commentators, then, profess an imminent revolution in strategic affairs. It is possible to identify a second theme in the literature on AI and war. Many scholars are not so exercised by the thought of AI automating strategy, but they are deeply concerned that AI will automate *warfare*. They are disturbed by the prospect that AI will automate weaponry. Above all, scholars in this camp fear that AI will necessarily lead to a proliferation of lethal autonomous weapons; drone swarms and robots controlled by AI will dominate.³⁹

The fear that AI will automate weapons has been apparent for about a decade. In 2013, activists concerned about the military threat posed by autonomous weapons created a group called the Campaign to Stop Killer Robots. This group advocates the regulation of the military application of AI. As part of its campaign, at the International Joint Conference on Artificial Intelligence on 28 July 2015, Elon Musk, Stephen Hawking, Demis Hassabis, and many other leading AI experts published an open letter documenting their concerns about the military application of AI; AI could be used to turn weapons against humans. Unlike nuclear weapons, autonomous weapons will be easy and relatively cheap to develop. 'The key question for humanity today is whether to start a global AI arms race or to prevent it from starting. If any major military power pushes ahead with AI weapon development, a global arms

race is virtually inevitable, and the endpoint of this technological trajectory is obvious: autonomous weapons will become the Kalashnikovs of tomorrow'. 40

Stuart Russell, who played an important role in the development of AI from the 1980s, has been a leading opponent of the proliferation of AI-enabled autonomous weapons. He has campaigned vociferously for the regulation of AI for military purposes and was one of the signatories of the Campaign to Stop Killer Robots' 2015 letter. He is scared by the prospect of AI-automated weapons. To highlight his fear, he created a short fictional film called *Slaughterbots*. The film, released in November 2017, dramatized the assassination of a senator by a swarm of killer drones which then attacked a university campus. The implication was that once they have been automated, such swarms will kill without constraint. The

Following *Slaughterbots*, Russell dedicated one of his BBC Reith Lectures in 2020 to the military application of AI. He discussed the issue of automated weapons and killer drone swarms almost exclusively. The lecture reached a climax when Russell described a scenario in which a lethal quadcopter the size of a jar could be armed with an explosive projectile device: A regular shipping container could hold a million lethal weapons [. . .] The inevitable endpoint is that autonomous weapons become cheap, selective weapons of mass destruction. He continued: Anti-personnel autonomous weapons could wipe out all the males in a city between 12 and 60 or all the visibly Jewish citizens in Israel. Unlike nuclear weapons, they leave no radioactive crater. As evidence, he cited the Turkish use of an autonomous Kargu-2 drone in Libya in March 2020. Russell concluded that unless governments acted to regulate the military application of AI, there are eight billion people wondering why you cannot give them protection against being hunted down and killed by robots. He

Eric Schmidt has, apart from in his work with Kissinger, articulated similar concerns about lethal autonomous weapons. He takes an entirely different political and ethical stance to Hinton and Russell, believing that the US must invest in AI in order to retain its supremacy—and to protect democracy and freedom. Yet he, too, sees the cataclysmic military potential of AI:

Eventually, autonomous weaponized drones—not just unmanned aerial vehicles but also ground-based ones—will replace soldiers and manned artillery altogether. Imagine an autonomous submarine that could quickly move supplies into contested waters or an autonomous truck that could find the optimal route to carry small missile launchers across rough terrain. Swarms of drones, networked and coordinated by AI, could overwhelm tank and infantry formations in the field.⁴⁶

Warfare will be automated. Drones and robots, controlled by algorithms, will dominate the battles of the future.

10 CHAPTER 1

The Campaign to Stop Killer Robots, Stuart Russell, and Eric Schmidt might exaggerate the potential of lethal autonomous weapons. It is striking, then, that many prominent security-studies scholars, while eschewing the language of slaughter-bots, have often concurred with their view. They too claim that AI will automate weapons, making war easier and more likely. For instance, in an important article, Jürgen Altmann and Frank Sauer observe: 'Today's unmanned systems have already increased the risk that military force will be used in scenarios where manned systems would previously have presented decision-makers with bigger, caution-inducing hurdles'. The anthropologist Lucy Suchman claims that states will use AI and autonomous weapons to prosecute dehumanised targets anywhere in the world at will: 'These [AI-enabled targeting systems] become ever more dangerous in the contemporary moment, as the figure of the 'imminent threat' is expanded into a horizon of anywhere and of endless war'. Consequently, these and other scholars call for the regulation of autonomous weapons.

In their recent monograph on AI, Ben Buchanan and Andrew Imbrie describe AI as the 'new fire'. For them, AI represents a potentially revolutionary development for the armed forces, and they draw a striking historical parallel:

Humanity has also wielded fire's destructive forces. The Byzantine Empire used it to great military success, first during the siege of Constantinople in 672 AD, and then in the centuries that followed. In battle, Byzantine troops shot a specially formulated compound at their enemies, one that would burn even when it came into contact with water. Once the compound hit the target, the power of fire would kick in, torching enemy equipment and causing soldiers to flee. Since then, the flames of war have become deadlier. Could there ever be another force so productive and perilous, one so essentially defined by the exponential growth of its core components? Welcome to the age of artificial intelligence. ⁵⁰

For Buchanan and Imbrie, AI is the equivalent of ancient Greek fire or the gunpowder weapons of late medieval Europe. AI-automated weapons will magnify the destructive power of weapons. Buchanan and Imbrie have suggested that with the help of AI, 'missiles would fly to an area of concentrated enemy forces and hover. Each missile would release smaller munitions, and each of these would select and attack an enemy target'.⁵¹

In the last two decades, David Hambling has established himself as a leading expert on drones and remotely controlled systems. Like Buchanan and Imbrie, he has claimed that military automation is approaching. Autonomous drone swarms, in particular, will be revolutionary: ⁵² 'A swarm of ten thousand small drones could level a town [...] A small perching drone could deliver multiple incendiaries the size of bats [...] Acting together drones might bring down a bridge or skyscraper, but they could do more than that'. ⁵³

Kenneth Payne's work on the strategic implications of AI was already discussed; Payne sees great potential for AI in weapons development too. In his view, AI will facilitate the rise of automated weapons; 'warbots', as he felicitously calls them in his most recent book. In his analysis of warbots, he discusses the now-famous AlphaDogfight experiment at the US Air Force Research Laboratory in 2016 and 2020, which tested AI in a virtual simulation of aerial combat. AI programs, which had used massive amounts of data to teach themselves the best aerial manoeuvres, flew fighter jets in simulated combat against a human pilot. Heron Systems' Falco program proved successful in the trials in 2020. Displaying 'superhuman precision in its flying and fighting', Falco beat the human pilot 5-0. There were several reasons for Falco's victory; one of these was that 'the AI agent could pull manoeuvres that a human pilot simply could not physically withstand.⁵⁴ Another was that Falco calculated that the most effective way to attack an opponent was frontally: 'The AI agent showed a strong favour for what pilots called forward-quarter gunshots, when the two aircraft are racing toward each other head-to-head'.55 Such an approach is extremely difficult and dangerous; human pilots tended to avoid it. Indeed, one pilot described it as 'a gunshot that is almost impossible'. Many pilots flinch when a plane flies at them. By contrast, Falco, experiencing no emotional response, fired its weapons coolly, no matter how likely the chances of a head-on mid-air collision. These simulated dogfights seemed to demonstrate that AI could automate aerial combat. AI could be quicker, more skilled, and more lethal than even the best human pilots.

On the basis of the AlphaDogfights, many other commentators assume that soon AI will automate combat. In his recent best-seller, Paul Scharre, for instance, fears that military forces are developing autonomous weapons systems which will be able to identify and engage targets independently of human control: 'Militaries around the globe are racing to deploy robots at sea, on the ground, and in the air—more than ninety countries have drones patrolling their skies. These robots are increasingly autonomous and many are armed. They operate under human control for now, but what happens when a Predator drone has as much autonomy as a Google car?'56 James Baker claims that because AI has the ability 'to outperform humans in pattern recognition and anomaly detection', it will soon direct weapons independently of human control.⁵⁷ John Antal confirms the point. He has claimed that the Second Nagorno-Karabakh War was 'the first war won primarily by robotic systems'. The future, for him, is clear: 'When these [autonomous] systems are connected into a network and form a multi-domain strike capability that leverages the synchronization in time, space and effect with artificial intelligence (AI), the ability for anyone or anything to hide in the battlespace will become much harder, if not impossible'. 58 Similarly, Seth Frantzman claims that once drones are AI-enabled, war will start 'to look a lot more like a computer game'. 59

12 CHAPTER 1

In the 1990s, John Arquilla, with David Ronfeldt, made an important intervention into discussions about the evolution of war, claiming that 'cyber war was coming'. Arquilla was impressed by the Revolution in Military Affairs in the 1990s, when the US harnessed the potential of new surveillance systems, digital communications, and precision munitions. These new systems would soon allow US forces to coordinate seamlessly with each other, converging on decisive locations on the battlefield. Arguilla has been similarly impressed by AI and the potential of military automation. For him, AI will accentuate the trends of the Revolution in Military Affairs. Robots and drones will replace humans: 'Future battles between advanced forces will be incredibly fast-paced, replete with weapons empowered by artificial intelligence and coordinated to strike in networked "swarms".60 The ethicist and philosopher Ronald Arkin has developed an unusual position in these debates. He, too, claims that lethal autonomous weapons will proliferate to become extremely important. However, he welcomes the development. He claims that because their judgement is motivated not by fear or hatred but by reason, AI will make decisions more ethically than human combatants would. AI will not kill unnecessarily. 61 Nevertheless, he still believes that autonomous drone swarms will dominate the battlefield of the near future.

A consensus is developing across the study of security, armed conflict, and war. In a field which is typically riven with debate and disagreement, it is surprising that so many scholars and commentators have eventually converged on essentially the same position regarding the military application of AI. Despite the wide divergence in their political and critical viewpoints, Henry Kissinger, Ken Payne, David Hambling, Roberto Gonzalez, Denise Garcia, Jürgen Altmann, Frank Sauer, and many others believe that AI is about to automate war—or significant parts of its prosecution. AI is about to displace humans to make strategic decisions as to when and how to go to war. AI will increasingly direct weapons, killing people independently of human control. It is a troubling vision of the future.

AI Scepticism

The concerns of Kissinger, Hinton, Russell, Payne, and others are not baseless. On the contrary, these authors have good reasons to argue the way they do. It is absolutely true that, today, states are actively seeking to harness the power of AI for military advantage. China, for instance, has announced its intention to become the world leader in AI by 2030. Its 'New General AI Plan' proclaimed that 'AI is a strategic technology that will lead the future'. China is determined to have the world's premier AI-enabled military within a decade. Similarly, the Russian president Vladimir Putin declared, 'Whoever becomes the leader in this sphere [artificial intelligence] will become ruler of the world'. Although Putin has suffered a terrible setback in Ukraine, there

is little doubt that he and his successors will attempt to enhance the Russian armed forces with AI as quickly as they can.

In response to the challenge posed by China and Russia, in 2014 the US committed to a 'Third Offset Strategy'. The US has invested heavily in AI, autonomy, and robotics to sustain its advantage in defence and will continue to do so. Some have declared that the US is in an 'AI arms race'. 64 Indeed, Alex Karp, the CEO of Palantir Technologies, a leading tech defence company, went further: 'The power of advanced algorithmic warfare systems is now so great that it equates to having tactical nuclear weapons against an adversary with only conventional ones'.65 In September 2018, the Defense Advanced Research Projects Agency (DARPA) announced a \$2 billion campaign to develop the next wave of AI.⁶⁶ The US Department of Defense issued its AI strategy in 2019, accompanied by a major increase in AI funding;⁶⁷ in 2024, the Department of Defense budget for AI was \$1.8 billion.⁶⁸ The US has established the Defense Innovation Unit and the Joint Artificial Intelligence Center to germinate, accelerate, and enhance its armed forces' AI capability. Smaller states are equally committed to the military development of AI. The UK and Israel, for instance, are developing their AI capabilities. AI has become an existential security question which no serious military power can ignore any longer. It is becoming as central to defence policy as aircraft carriers, tanks, or atomic bombs were in the twentieth century.

Today, of all the automated and robotic systems being developed for military usage, the drone swarm has attracted by far the most attention and seems to show the most potential. The trajectory of the drone, or the uncrewed aerial system (UAV), over the last two decades is remarkable. The drone first began to be commonly used by the US in 1999, as a surveillance system; by 2024, it was a ubiquitous weapon, used by almost every combatant on a daily basis. There have already been notable developments in autonomous swarming. In October 2016, the US Department of Defense demonstrated a swarm of 103 Perdix micro-drones capable of 'advanced swarm behaviours such as collective decision-making, adaptive formation flying and self-healing'.69 The Chinese have also made significant advances in swarm intelligence. In 2017, a formation of a thousand UAVs flew at Guangzhou Airshow, and China Electronic Technology Group flew a swarm of 119 fixed-wing drones.⁷⁰ The US Army has procured and tested the TSM-800 drone swarm, manufactured by Booz Allen. At Fort Irwin, California, in recent trials in 2023, operators successfully flew a preprogrammed swarm of ninety-seven TSM-800 drones to attack a designated target; one human controller oversaw the attack remotely (with the capability of aborting the mission), but the swarm was essentially autonomous. The swarm was divided into five subgroups of twenty drones, programmed to attack on different vectors, so that it was more difficult to defend against them. 71 The US Navy has tested superswarms which look and fly like flocks of birds in order to deceive enemy radar. The possibility of automated drone swarms controlled entirely by AI is evident.

14 CHAPTER 1

No one should doubt the military utility of AI, then. Yet it is easy to be entranced by AI. AI has, after all, made extraordinary advances in a very short time. No matter how tempting it is to enthuse about AI, though, scepticism is in order. Current predictions about AI are more fragile than they appear. Hinton, Russell, Kissinger, Schmidt, Payne, and other experts project a vision of the future based on their understanding of AI today. Yet they take a relatively narrow view of AI, examining only a few exceptional cases; there is little discussion in their work of the difficulties and shortcomings of AI. In addition, they propose the most extreme future scenarios, on the presumption that further major strides are inevitable and obvious. There are serious epistemological dangers to prognostications of this type, especially in a field as empirically complex as war. Many scholars have been too quick to draw causal conclusions about AI and the inevitable automation of war. They predict an AI military revolution on the basis of thin, narrowly selected evidence which supports only the case for automation while ignoring the limitations of AI and the difficulties of applying it to strategy, to war, and to warfare. Indeed, there is a tendency towards circularity in contemporary work. Because these scholars presume the future of AI, they read the evidence about the performance of AI in the present in only one categoric way, which, they claim, leads to that inevitable, already assumed future. It is a pure case of teleology.

Recently, some scholars have begun to question some of the presumptions which have become so established in the debates around security. Rather than advocating a single AI future, they have highlighted the limitations of AI and the difficulty of applying it to military operations. For instance, in an important recent article, American security-studies scholars Avi Goldfarb and Jon Lindsay have punctured the hyperbole around AI, saying that 'AI, from this perspective, is not a simple substitute for human decision-making'. They fully recognise that AI is capable of better, faster, cheaper statistical prediction than humans are. AI has consequently proved highly successful in the commercial world, allowing companies to predict customer demand and market trends with striking accuracy. There is no doubt AI will be useful to the armed forces. Nevertheless, Goldfarb and Lindsay stress the distinctiveness of military operations: 'the conditions that have made AI successful in the commercial world—quality data and clear judgement—may not be present or present to the same degree for all military tasks'. 73 In the commercial sector, markets are relatively stable; demand is predictable. The data on which companies make their decisions is generally clean, reliable, and adequate. Rival companies are serious competitors, but their actions, too, are broadly predictable, operating from within regulatory parameters. Not so in war: 'In contrast with assumptions about rapid robot wars and decisive shifts in military advantage, we expect AI-enabled conflict to be characterized by environmental uncertainty, organizational friction, and political controversy'. The authors conclude,

'War, by contrast, occurs in a more anarchic environment'.74 In war, data will, therefore, be incomplete, messy, and inaccurate. Moreover, the enemy will actively seek to corrupt and poison data: 'The importance of data and judgment creates incentives for strategic competitors to improve, protect, and interfere with information systems and command institutions'.75 Moreover, the military decision-making process cannot be reduced to statistical prediction; it is not reducible to an algorithm. A command decision is a complex process. Commanders do not just order a weapon to fire at a threat. They have to define a mission, in which all their forces and all their weapons are organised and oriented to a single goal. Commanders, therefore, must consider many different factors before they make a decision. They have to understand the situation; they must comprehend what they have been directed to do by political leaders. Balancing that direction with a variety of military, civil, and political stakeholders, they must work out what is possible, not only militarily but politically. No matter how impressively it processes data, AI does not possess the judgement that underlies decision-making. 76 'AI will alleviate some of the data processing burden', Goldfarb and Lindsay allow, but, in war, human intelligence will remain critical. Indeed, AI, data, and machine learning will make 'human beings even more vital'.77

Goldfarb and Lindsay are not alone in their scepticism about AI. In a closely related article, Benjamin Jensen, Christopher Whyte, and Scott Cuomo also take a sceptical view of AI. They fully recognise the potential of AI for military affairs, as AI can perform and indeed has already performed a variety of useful military functions. They acknowledge that 'deep learning has the potential to create combat-advising software agents that anticipate both the natural and human environment, offering predictions about enemy actions.⁷⁸ AI could prove very useful in military logistics; it could anticipate supply needs, thereby revolutionizing military readiness. It could simulate defence scenarios to improve reactiveness and decision-making. Alternatively, 'AI advances have the potential to perform a wide range of intelligence tasks faster and with higher accuracy than human analysts'.79 There are many military practices to which AI might be usefully applied. However, the authors also highlight the operational limitations of AI. War is a complex, bewildering phenomenon: 'As a nonlinear system, every battle and campaign is contingent and subject to emergent properties'.80 On contemporary battlefields, civilians, friendly and enemy forces are often intermingled and indistinguishable from one another in blasted, ruined urban areas. War is an agonistic enterprise: 'The enemy gets a vote, producing a complexity unique to war. Every change to military capabilities—the hardware—and their battlefield employment through new concepts and organizations—the software—is subject to a corresponding reaction'.81 The smallest bias or gap in the dataset would generate egregious targeting errors. AI would be extremely susceptible to errors of

16 CHAPTER 1

targeting in the confusion of a battlefield: ⁸² 'Consider what would happen if military intelligence professionals entered into a similarly flawed image recognition system hundreds of pictures of adversary fighters assessed to be located in an urban area filled with hundreds of thousands of non-combatants'. ⁸³ The risks are obvious. An AI agent might easily target civilians or friendly fighters; more likely, it might simply stop functioning at all. AI is powerful, but it is also limited. It is very unlikely, according to Jensen, Whyte, and Cuomo, that combat could be completely automated. As a result, the authors dismiss the utopian vision promoted by so many other commentators and scholars. They do not see AI taking over: 'AI does not yet promise to change states' abilities to prevail in major conflict'. ⁸⁴

In an indignant recent article, Cameron Hunter and Bleddyn Bowen have made a similar argument and rebutted the claim that AI could ever supersede human commanders. Because AI has been successful under closed conditions, they explain, AI proponents describe war as a similarly prescribed system: 'Decision-making in war under this implied vision is within a closed, rulebased system [...] Conceiving of war as a kind of game or closed system allows AI optimists to envisage a future in which AI will be able to make or advise on command decisions'. 85 Hunter and Bowen vehemently disagree with that view; war is an open, complex—indeed, chaotic—environment. Strategy, command, and military decision-making, therefore, require more than mere calculation: 'Command in strategy and tactics requires abductive logic—an ability to think and make decisions based on the constant presence of unknowns and unknowable things that may never appear in a historical dataset or past experience'.86 Strategists need a subtle awareness of other actors and the range of factors at play as a state moves to war: 'AI currently cannot make judgements, but rather makes probabilistic inferences. Nor can it make useful decisions in the absence of comprehensive data in a closed system'. It is, therefore, difficult to see how second-generation AI could automate military decision-making—much less war more widely. It will be a good deal more difficult for AI to automate war than many scholars presume.

There is much evidence to support the arguments of sceptical scholars like Goldfarb and Lindsay. For instance, there is a common error in much of the literature about the application of AI to military affairs. Many AI advocates extrapolate from military simulations that make use of AI to presume that the same situation would pertain on the battlefield itself. On this account, the evidence from simulations transposes immediately onto the battlefield; what happens in virtual reality will soon inevitably happen in reality.

The heavily referenced AlphaDogfight trials illustrate the problem of this evidential carelessness rather well. AlphaDogfight has been recurrently cited by AI advocates to prove the superiority of AI over human pilots. In the simulations, the AI pilots won. On this basis, it is presumed—by Kenneth Payne and

by Kissinger, Schmidt, and Huttenlocher-that AI will soon fly real planes in combat more successfully than human pilots can. Yet the conditions in those trials were vastly in the favour of AI: 'The AI agent [Falco] was given perfect situational awareness of the simulated environment, including the location of the opposing fighter'. 87 In addition, the human pilot was constrained in a way which Falco was not. In training, human pilots are not permitted to conduct head-on shots; it is too dangerous to practice them in the air. 88 And human pilots do not like taking head-on shots. However, in actual combat, human pilots might well adopt this kind of tactic. Trained on large amounts of pristine data from previous simulations, Falco performed supremely. Yet the real world is vastly more complex than the world of such simulations. Human pilots have to deal with weather—clouds, rain, wind, unusual lighting conditions, and so on—unexpected enemy action, mechanical failures, human errors, air-defence systems, and more. They have to land and take off; they have to coordinate with their colleagues. Their mission changes. It is sometimes difficult to distinguish friend from foe. To an AI pilot, by contrast, even the smallest change to the environment might be confusing.

US Air Force commanders know all this full well and recognise that, in reality, a completely autonomous aeroplane is improbable. They were certainly still interested by the results of the AlphaDogfight trials, but they saw the experiment as a way of improving the performance of human pilots by augmenting them with AI, rather than replacing them. ⁸⁹ The air force recognised that this trial was only a simulation in a virtual world. For the air force, it is important to distinguish between the virtual and the real. Yet, in many discussions of AI, evidence taken from simulations is assumed to apply immediately in the real world.

A recent furore surrounding the US Air Force demonstrates the fallacy with even more force. In May 2023, Colonel Tucker 'Cinco' Hamilton precipitated a Twitter storm when he seemed to claim that, in a recent exercise, a rogue autonomous drone had attacked its own command post. It was reported that the drone had been unable to find an enemy headquarters and, therefore, logically following its algorithms, attacked a friendly one instead. Many people took this incident as proof that military automation was imminent. They presumed the incident was real. Hamilton later admitted that he had 'misspoken'. The episode had not really happened at all; it had occurred within a simulation. Although the US Air Force is certainly experimenting heavily with AI—with autonomous and quasi-autonomous aircraft—the replacement of piloted combat planes with completely autonomous ones is unlikely. As Bill 'Evil' Gray, a test pilot, observed: 'We are trying to figure out how to integrate artificially trained neural networks, trained in a simulation[, . . .] into the real world'.90 That is not easy. Prophecies about the imminent AI revolution in military affairs are overstated and under-evidenced.

18 CHAPTER 1

Al at War

Is AI about to automate war? This question is the central theme of this book. In order to address this issue, I focus on recent and contemporary military practice, rather than projecting into the future. Specifically, I answer two subordinate questions: first, in the last two decades, how has AI been employed in military operations? Second, how have the armed forces reorganised themselves in order to exploit AI? I eventually address a third issue: how has AI changed the character of war in the last decade, and, consequently, how might it change the character of war in the next ten years? The method is deliberately historical; it looks to the past and present. It looks at how militaries have actually applied AI to their activities and operations in the recent past and how they are planning to use AI in the near future. Their plans cannot be taken as a reality in themselves, though they may be organisationally relevant for the present practices. I try not to speculate about how AI might be used or how it might change war and warfare ten or more years from now. In focusing on the past—and therefore on actual evidence—I adopt a sceptical, empiricist approach to AI. I consciously follow the philosophy of the eminent Scottish philosopher David Hume here.

A great deal of contemporary scholarship on AI presumes the future. This is a problem, because there is no evidence about the future. So, any prediction, however plausible it might seem, can be only speculation in the proper philosophical sense. Hume highlighted the dangers of prediction over two hundred years ago from his position of 'determined scepticism'. In a famous passage in his Treatise of Human Nature, he showed that cause and effect, so often presumed by philosophers and theologians, can never actually be assumed. He considered the example of billiard balls striking each other. Because billiard balls have collided in the same way in the past, observers naturally presume that they will interact in the same way in the future. 91 Although practically—and empirically—it is correct to assume this eventuality, there is no logical necessity that the balls should strike each other as they have before. Philosophically, there is no necessary bridge forward from the present to the future. In any future case, anything might happen; factors of which we were ignorant might suddenly influence events. Cause and effect are not inevitable or obvious. Humans infer necessary cause from seeing events repeat themselves regularly; they presume a certainty to which they are not entitled. Consequently, Hume famously concluded, 'We have no other notion of cause and effect but that of certain objects which have always conjoin'd together and which in all past instances have been found inseparable'. 92 In the future, even the most apparently ineluctable causal links might not operate. The future development of AI and its application to war is far more indeterminate than billiard balls colliding on a flat baize-covered table.

In this book, I try to avoid prediction and prognostication. Instead, I consciously look backwards to what has actually happened. I examine military

developments in the present and the recent past. I look at how the armed forces have sought to adopt AI, to train with it, and to apply it to military operations. Recent wars are plainly a vital part of the evidence base. Since 2001, conflicts have proliferated and intensified in Ukraine, Georgia, the Middle East, Afghanistan, the Sahel, sub-Saharan Africa, and South-East Asia. War has been a constant, and the amount of potentially relevant material is vast. In particular, the Russo-Ukraine War is of prime significance; it continues to generate nearly endless, often surprising, evidence about war in the twentyfirst century, defying many predictions. For instance, as General Mark Milley, the chair of the US Joint Chiefs of Staff, claimed, the Russo-Ukraine War has delivered a unique insight into the potential of AI for war: 'We are witnessing the way wars will be fought, and won, for years'. 93 In a speech to the Royal United Services Institute in November 2022, General Sir Jim Hockenhull, the head of the UK's Strategic Command, discussed the Russo-Ukraine War and AI at length. He used the conflict as a way of illustrating the growing importance of AI, data, and open-source intelligence, declaring, 'The conflict in Ukraine can in some ways be viewed as the first digital war'. 94 The war has involved an explosion of data. The wars in Nagorno-Karabakh and Gaza are also immediately relevant for understanding the military application of AI.

The recent operations of the Israel Defense Forces (IDF) and the current war in Gaza are also instructive. In May 2021, the IDF conducted an eleven-day campaign, called Operation Guardian of the Walls, against Hamas in Gaza. It was described as the 'first AI war', as AI was employed extensively to facilitate targeting. Following the attacks of 7 October 2023 (see chapter 10), Israel has been engaged in a major war with Hamas. The campaign has been brutal, with many thousands of civilians killed and hundreds of thousands more displaced. Nevertheless, the IDF have once again drawn on AI to help them target Hamas militants.

The war in Gaza and the Russo-Ukraine War may be a turning point in the history of war. They may mark the moment when AI first began to be indispensable to military operations. These wars may disappoint the AI proponents, though. There is no sign in Ukraine that AI is about to take over, despite both sides' profligate use of drones and loitering munitions. On the basis of the evidence from Ukraine, AI will not automate war—that is more fantasy or science fiction than reality. Nevertheless, the war in Ukraine has categorically demonstrated that AI has indeed become crucial to military operations. Although President Zelensky, General Zaluznyi, General Syrskyi, and their subordinates still make all the decisions for the Ukrainian military, AI has played a crucial role, harvesting intelligence from a great quantity of diverse data. AI algorithms have helped the Ukrainians to plan and helped them to target the enemy. It has enhanced their military capability. The war shows the salience of AI in contemporary warfare. This connection is likely to deepen in the next decade. AI is

20 CHAPTER 1

becoming more potent every week, and the armed forces will draw ever more heavily on it. Even if we dismiss the apocalyptical claims about military revolution, AI will inevitably continue to reconfigure warfare. Like gunpowder, railways, telegraphy, automobiles, aeroplanes, wireless, and nuclear weapons, AI will inevitably have a major impact on the way wars are fought now and in the future.

To this end, it is necessary to examine how the armed forces are actually harnessing AI for military operations. Most major military powers are already trying to use AI. A global survey of all these powers would be welcome. Yet a complete survey of how every military force is using AI would be impractical. The empirical focus of this book is, therefore, deliberately circumscribed to achieve a level of evidential adequacy. However, while it is impossible for me to be comprehensive, it is useful to employ a comparative method. In their excellent recent work on technology and civil-military fusion, Yoram Evron and Richard Bitzinger use comparison to great effect. 95 They select four case studies—the US, China, Israel, and India—to show how these states have differentially adopted or failed to adopt new military technologies. The comparisons provide a better understanding of the process in each state, as well as the general pattern of change. I have followed Evron and Bitzinger's method here, adopting a comparative approach focusing on examples from the US, the UK, and Israel. Because the armed forces of these states are Western or Westernised powers, it has been easier for me to gain access to them than it would be to gain access to those of Russia or China. There are also good substantive reasons for focusing on these three powers. The US and Israel are pioneers in the application of AI to military operations. They provide excellent evidence about the military application of AI. And despite the small size of the British armed forces, the UK remains a major European power; as such, it is a leading proponent of the military application of AI. France, Germany, and other European countries are certainly looking to employ AI, but the UK usefully stands as an example of how a medium-sized NATO member is adopting this technology. The evidence presented here is certainly not comprehensive.

In the following chapter, I discuss AI as a technology. However, a major part of the analysis examines not AI as a discrete technology but rather the way in which the armed forces have reorganised themselves in order to be able to employ AI. This is a vital and often under-appreciated issue. AI has not simply automated war or the armed forces, nor will it. In order to exploit AI, the armed forces have already begun to reform their organisational structures and practices. Profound institutional reconfigurations are occurring. The organisational transformations are just as important as the technological developments, because without those alterations in human organisation, it is impossible to use AI. The armed forces are, therefore, changing their command hierarchies and the structure of their headquarters; they are altering their doctrine and practices.

Above all, a profound organisational transformation is taking place. A new partnership between the armed forces and commercial tech companies—such as Google, Amazon Web Services, Microsoft, SpaceX, Palantir, and Anduril—is appearing. In this book, I plot the emergence of this new relationship between the armed forces and tech companies.

The armed forces have, of course, long been dependent on the private sector. In the twentieth century, and especially during the Cold War, private arms companies were contracted to produce weapons and platforms for the armed forces. A military-industrial complex developed. Since the 1990s, private military and security companies have been contracted to perform specific services in support of the armed forces; for the most part, they have provided dining facilities, technical support, and close security. Occasionally, they have provided combat forces—traditional mercenaries. Outsourcing has become a major feature of the defence sector.

The relationship which is crystallizing today between the armed forces and tech companies is different. Tech companies are not providing the armed forces with pristine platforms or weapons. Neither are they supplying peripheral support services. They are providing software, data, and expertise. In addition, they do not merely deliver these AI-enabled services and then leave it to the armed forces to apply them—on the contrary, software and data are immediately related to current operations and need constant revision. Consequently, to harness AI, tech companies are being integrated into the armed forces and into military operations themselves. They are actively partnering with active military forces and deploying their employees forward into operational headquarters. There, the civilian data scientists, programmers, and coders are integrating with military personnel. The pursuit of AI is thus precipitating a major organisational restructuring. A hybrid private sector-public sector, civil-military configuration—a military-tech complex—is emerging. The appearance of this strange new complex is of profound significance not just to warfare but also to civil-military relations. The rise of a military-tech complex raises serious political, legal, and ethical questions which are equally as vexing as current debates about military automation. The problem is not that computers are about to take over strategy and war but that private-sector tech companies are increasingly influencing the conduct of war.

It is already possible to see the emergence of a military-tech complex in Ukraine. In order to harness AI, the Ukrainian armed forces have relied not only on traditional allies, such as the US, but also on close partnership with private-sector tech companies; they have needed the support of Google, Microsoft, Starlink, Palantir, and Anduril. They have fought the Russian invasion with the assistance of tech companies which have provided them with the data, the AI, and the software to be able to execute operations effectively. As General Hockenhull himself noted, 'Much of that digital capability is coming

22 CHAPTER 1

from commercially available services rather than necessarily traditional military capabilities'. ⁹⁶ 'Commercial networks' have been a 'force multiplier'. For instance, 'The availability of commercial satellites has enabled an extension of reach in the Ukrainian military's situational awareness and their ability to conduct surveillance and reconnaissance. We're seeing artificial intelligence used alongside commercial software applications to increase the speed of action.'⁹⁷

It is vital that we recognise and try to understand this military-tech complex, especially since, as we have seen, so much of the literature has fetishized AI as a technology, ignoring its organisational aspects. It is also necessary that we acknowledge that any account of the military application of AI and the military-tech complex can be only preliminary. The armed forces are only just beginning to employ AI. The military application of AI is a very new development, one that in most cases has transpired in the last five years. The armed forces and tech companies are at the very beginning of a profound transformation. Studying AI may, therefore, have some equivalence to studying the genesis of strategic bombing forces or tank warfare in the 1920s and 1930s. The potential of AI is clear. The outlines might be visible, but we are examining a volatile process, not a stabilised institution. Analysing the process of construction is always far more difficult than understanding the finished edifice. In the case of AI, it may be even more difficult. The military application of AI is diffused across a transnational organisational complex. The network is still crystallizing. Finally, AI and the military's use of it are developing so rapidly that it is nearly impossible to map the landscape with complete confidence. Even the AI pioneers themselves have been staggered by the pace and scale of the changes—as Hinton's and Russell's warnings illustrate.

Consequently, this book is avowedly provisional. In it, I describe the application of AI to recent military campaigns, especially in the Russo-Ukraine War, and I take examples from US, British, and Israeli armed forces as they try to apply AI to their operations. Only at the end of the book do I offer some tentative predictions about the future trajectory of military transformation and therefore the likely character of warfare between AI-enabled, digitised militaries. Yet, for all my efforts to adopt an empirical method and to limit my claims to what is empirically verifiable, I must allow that even if the picture I depict in this book is broadly accurate for now, it may be overtaken by events. No one knows, for instance, how quantum computing will transform AI and therefore military operations too. However, AI is an existential security issue. Scholars are duty-bound to analyse its development and its implications as best they can. Although this book must be only preliminary, offering conditional findings, it seems imperative for me at least to proffer some interpretation about the military implications of AI. It would be a dereliction of duty to do otherwise.

INDEX

Adarga AI, 79, 83, 94 AlphaFold, 3 adversarial generative AI, 140 AlphaGo, 2, 28, 29, 154-55 aerial combat, simulation of, 11, 16-17, 102 al Qaeda, 87, 90, 92, 93 aerial systems, uncrewed: Project Maven Altmann, Jürgen, 10, 12 and, 67, 116-17. See also drones al Zarqawi, Abu Musab, 92-93 Afghanistan: drone surveillance in, 117; IEDs Amazon, 3, 37-40; based on explosion of in, 84; key leader engagement in, 125; data, 27, 38; computing facilities of, 29; Palantir software in, 86–87, 159; Special establishing office near the Pentagon, Operations Forces in, 90, 92; US military 76; failed cloud computing contract and, 76; human workforce of, 38-40, 42; operations in, 19, 44, 50 Ahmad, Tariq, 135 investment in research and development, AI (artificial intelligence): adversarial, 140; 64-65; using algorithms to influence demanding more skilled human operators, consumers, 139 156; exponential progress of, 4-5; faulty Amazon Web Services, 38; aiding Ukraine, data and, 175, 176; in financial markets, 172, 174; armed forces developing rela-4; first-wave, 26, 27; fragility of, 119, 151; tions with, 81; in military-tech complex, generative, 4, 31-35; human labour indis-21; Royal Navy battle-management syspensable to, 153-57; investment in R&D, tem and, 109; UK Ministry of Defence contract with, 78 64-65; making probabilistic inferences, 17; misattribution of agency to, 149-50, Amicelle, Anthony, 155 152, 153, 157, 168, 169-70; origins of, Anduril: armed forces developing rela-23-26; performative definition of, 23-24; tions with, 21, 81; employing Special requiring data, computing power, and Operations veterans, 94; investment in expertise, 169; revolutionary powers of, research, 64; sensor system of, 108-9; 1-5; in scientific and medical research, Thiel's investment in, 70; UK Ministry of 2-3; second-generation, 26-31; as a Defence working with, 79 service requiring constant human effort, Antal, John, 11, 179 165, 169; sub-fields of, 23; as a tool for Anthropic, 32 human teams to use, 157. See also busi-Anthropocene, 1 ness and commercial applications of AI; antibiotic resistance, 3 Antonov, Anatoly, 173-74 military applications of AI Airbnb, 36, 42 Apple: based on explosion of data, 27; airpower, 166-67 investment in research and development, AI strategy. See policies for AI strategy; 64-65; refusing to unlock iPhone, 67; start-up funding for, 63-64 strategy AlexNet, 29, 32 Arkin, Ronald, 12 Armenian diaspora, 144-45, 147 algorithms: automating cyber operations, 146; in information and psychological Arquilla, John, 12 operations, 147; optimised and updated, 119; Aushev, Yegor, 137 predictive, 126-27; in second-generation Australian Army, 151-52 AI, 27-28; social media using, 138-39, 140 automation: in commercial workforce, 42; Alibaba, 27 of data processing, 57; excessive at Tesla, AlphaDogfight, 11, 16-17 41; unlikely as fully functional, 155-56

220 INDEX

automation of war: AI as we currently know it and, 23; armed forces seeking, 7; commentators believing in imminence of, 12, 41; data processing instead of, 57; fears regarding, 5–12; human-machine team and, 149–50; imagined future of, 166, 167; improbable with AI, 31, 35, 42, 167; with non-human decision-making, 7; overstated risks of cyberwar and, 132–33; sceptical views of, 15–17, 18, 55; scholars ignoring limitations of, 14; self-driving cars and, 36. See also military applications of AI

Babbage, Charles, 24 back-propagation, 28, 29 Baidu, 27, 36 Baker, James, 11, 149-50, 152 Bakhmut, Battle of, 179-80 Banko, Michele, 26-27 bank software, for monitoring transactions, battle-management systems, 106-9, 168; Anduril's sensors and, 108-9; of Australian Army, 151; Israel's Torch, 80-81, 107, 152; of Royal Navy, 109; Ukrainian, 108; US forces' DCGS, 116; US forces' JADC2, 101, 103 battle networks, digital, 46-47 Battle of Bakhmut, 179-80 Bawab, Muhammed, 127-28 Ben-Ari, Eyal, 91 Berman, Eli, 115 Bezos, Jeff, 37-39, 68, 76 bias, human, 151 bias or gap in data, 15-16, 30, 34, 175 Biden, Joseph, 174 big data, 36, 47, 58, 115, 150 Bigelow, Julian, 25 Bigley, Kenneth, 93, 112 Bing, 33 bin Laden, Osama, 87 biotechnology, 1, 48, 70 Bitzinger, Richard, 20 Blank, Julius, 62 bots, 139-40, 144, 147 Bowden, Mark, 87 Bowen, Bleddyn, 16 BRAWLER, 102 Brexit, 4, 54 Brill, Eric, 26–27 Brin, Sergey, 68

Brown, Jason, 117-18

Buchan, Iain, 120-21, 130

Buchanan, Ben, 10 Budanov, Kyrylo, 141–42, 147 Burton, Arran, 123 Bush, Vannevar, 62 business and commercial applications of AI, 3–4, 35–37, 42, 58. *See also* Amazon

Cambridge Analytica, 83, 139
Cameron, James, vii
Cameron, Lindy, 136
capitalism, Marx on, 153
Carter, Ashton, 73–74
cartography, military, 113
Cattler, David, 137
causation, 18, 30
centaur model, 149–50, 169
Chafkin, Max, 69
Chat-GPT, 4, 31–33, 34
Chernobrov, Daniel, 144–45
chess, 2, 26

China: Australia challenged by, 151; cyberespionage by, 132, 135–36; cyber specialists in, 133; drone swarms of, 13; emerging as power rival, 44–45; human labour force of tech companies in, 41; increasing use of defence software, 79; intending to have premier AI-enabled military, 12–13; military technologies and, 20; planning experiments and, 110–11; possible war between US and, 181–82; UK AI strategy and, 54; US AI strategy and, 47, 49; US tech sector and, 68, 70, 71

civil-military relations, transformation of, 170–71, 175, 183

Clausewitz, Carl von, 53, 132

cloud: Copilot on, 33–34; data servers on, 29 cloud-based training, 78

cloud computing: for the Pentagon, 76; for researchers and students, 71

Cohen, Jared, 70

Cohen, Stephen, 84

Cold War, 44, 53, 90; archaic procurement model of, 73; military-industrial complex in, 21, 81

command and control: battle-management systems and, 107, 108; UK's Spearhead programme, 103–6

commanders: in civilian-military ensemble, 165; emotional commitments of, 7; functions supported by AI, 100, 114; substituted by AI, 7–8. *See also* decision-making by commanders; headquarters

command hierarchies, changing, 20 commodity fetishism, 153

INDEX 221

decision-making, military: by AI in warfare, computer vision: drone surveillance and, 117; Project Maven and, 118; satellite images 7; complexity of, 8; by drone swarms, 13; human-machine team and, 151; NATO's and, 103 computing power: exponential increase in, AI capacities and, 57; not reducible to AI 29-30; for large language models, 32; calculations, 15, 17; supported by AI, 59 decision-making by commanders: battle required by AI, 168 conspiracy theories, 139 networks and, 46; complex process of, context, not recognized by AI, 30-31, 34, 15; generative AI and, 35; helped by UK's Spearhead, 105, 106; in NATO exercise, 36, 42 contracting: in business and commerce, 42. 56–57; processes required for, 99–100; See also procurement psychological inhibitions and, 7; of US convolutional neural network, 103 Joint Force, 50. See also decision-making, Copilot, 33-34 military deepfakes, 140-41, 147 counterinsurgency operations, 86, 115; Liverpool as analogue for, 120 deep learning, 15, 23, 27, 29, 32 counterterrorism, and Special Operations DeepMind, 1, 2-3, 29, 154 Forces, 89-90, 91, 92 defence ministries, viii, ix Covid testing in Liverpool, 116, 119-25, 130 Defense Innovation Unit (DIU), 73-74, 76, 118 creativity: in AlphaGo, 2; large language Delta, 108, 173 deregulation, Schmidt's advocacy of, 70 models and, 33 CrowdFlower, 118 de Silva, Tom, 123 Cukor, Drew, 72, 117-18, 160 DeVries, Kelly, 61 Cuomo, Scott, 15-16 diasporas, internet activism of, 143-45 cybernetics, 24 DigitalGlobe, 118 cyber operations: AI used in, 58, 132-33, Dillman, Linda, 3-4 168; autonomous, 146-47; at Battle of disaster assessment, 75 Bakhmut, 180; civilians participating in, disinformation, 139, 140, 141, 142 143-45; contrast with military actions, Distributed Common Ground System 145-46; human actors needed for, 147; (DCGS), 84, 87, 88, 116 severe limitations of, 145-46; three forms distributed denial of service (DDoS) attack, of, 132 135, 136 Donahue, Christopher, 117, 158-62, 164-65 cyberspace: Israeli intelligence in, 97; in Douhet, Giulio, 166-67 multidomain operations, 51-52; in UK defence, 54; in US National Military Dreyfus, Hubert, 26 Strategy, 48 drones: AI-enabled, 11; Amazon's expericyberwar, 6, 12, 131-33 ments with, 40; at Battle of Bakhmut, cyborgs, 1, 183 180; big data from, 150; ground forces including, 150-51; of Hamas destroying Israeli surveillance, 176; land warfare not Daniels, Owen, 112 DARPA (Defense Advanced Research Projtransformed by, 167; Maven processing ects Agency), 13, 155 video from, 74, 117; to replace humans, Dartmouth seminar, 25, 62 12; in Russo-Ukraine War, 19, 142, 167; data: bias or gap in, 15-16, 30, 34, 175; critisensors on, 54; as ubiquitous weapon, 13. cal for UK's Spearhead, 104; explosion See also aerial systems, uncrewed in, 27; inability of AI to go beyond, 42; drone swarms, autonomous: Australian Army incomplete and inaccurate in war, 15; in and, 151; dominating future battlefield, military intelligence, 48-49; in second-12; fears regarding, viii, 8, 9, 10; fictional generation AI, 26-27, 30; as series of assassination by, 9; potential of, 13, 167; binaries, 27; in servers of tech primes, supposedly speeding up conflict, 178 30; sources of, 58, 129; used as singular dynamic targeting, 127, 158 noun, ix data-wiper malware, 136 eBay, 84

Eisenhower, Dwight D., 44, 81

Elbit Systems, 77-78, 80-81, 107, 152

decision-making: AI's lack of judgement for,

15; Amazon strategy and, 38-39

222 INDEX

ENIAC (Electronic Numerical Integrator Gerasimov, Valery, 157-64, 177, 178 and Computer), 24 Germany: behind the US in military applica-ESET, protecting Ukrainian interests, 172 tion of AI, 76-77; defense budget of, 64; increasing use of defence software, 79; Esper, Mark, 45 ethics: of automation, 57–58; of data-enabled looking to employ AI, 20 operations, 178; of IDF's targeting, 130; globalists, in tech sector, 67, 68, 69, 71 of lethal autonomous weapons, 175; Go. See AlphaGo outsourced to non-human agents, 8; Gödel, Kurt, 25 of Project Maven, 119; supposedly made GOFAI (good old-fashioned AI), 26 Goldfarb, Avi, 14-15 by AI, 12 Etzioni, Oren, 31 Gonzalez, Roberto, 7 Google (Alphabet): applying AI to its mar-Evron, Yoram, 20 ket, 36, 42; armed forces developing Facebook (Meta): applying AI to its marrelations with, 81; based on explosion ket, 42; based on explosion of data, 27; of data, 27; buying DeepMind in 2014, computing facilities of, 30; election influ-2; computing facilities of, 29-30; conenced by data from, 139; investment in tract for Maven and, 67-68, 116, 118, 119; research and development, 64-65; large investment in research and development, language model of, 32 64-65; large language model of, 32; in facial recognition programs, 29; bias in, 30; military-tech complex, 21; Schmidt's Ukrainian use of, 141 executive roles in, 6, 70; self-driving car of, 36; supporting Ukraine, 21, 172, 174; Fairchild, Sherman, 63 Fairchild Semiconductor, 62, 63 Winograd schemas and, 31 Farrell, Theo, 151 Gorgon Stare, 117 Fedorov, Mykhailo, 108, 137, 172-74 Gospel (Habsora), 127, 128-29, 130 Ferguson, Niall, 173 Gotham, 87-88 fetishism: human-machine team as form of, GPUs (graphical processing units), 29 153-54; Marx's concept of, 153 Gray, Bill, 17 fire: in military history, 10. See also Green, Mark, 130 Prometheus Grinich, Victor, 62 fire perimeter model, 75 Guardian AI platform, 93 First Offset Strategy, 44 gunpowder revolution, 61 first-wave AI, 26, 27 Hagel, Chuck, 44-45 fiscal-military state, 171 Hall, Bert, 61 Flynn, Michael, 86-87 fog of war, 53 Hamas: attacking Israel on 7 October 2023, Fossey, Joe, 120-21, 130 175-76; IDF targeting of, 19, 97, 116, 126, Fourth Industrial Revolution, 5 127-29, 130 France: behind the US in military applica-Hambling, David, 10, 12 tion of AI, 76-77; defense budget of, 64; Hamilton, Tucker, 17 Hassabis, Demis, 2, 8, 154 increasing use of defence software, 79; looking to employ AI, 20 Hawking, Stephen, 8 Frantzman, Seth, 11 headquarters: civilian technicians integrated Frey, Carl Benedikt, 35 into, 160-61, 164-65, 169; human collaboration for targeting and, 130, 158, Galbreath, David, 151 164; human-machine team in, 150, 152; Gallant, Yoav, 177 legal status of technicians in, 177; organ-Garcia, Denise, 7, 12 isational changes in, 20, 160, 164; Spear-Gates, Bill, 68 head in, 104; tech company employees in, Gaza: current war in, 19, 97, 116, 128-29, 177, 21, 171. See also commanders; staff officers Helsing, 79, 83 181; security threat in, 80

Hermes, 110-11

Hezbollah, 97

Hinton, Geoffrey, viii, 5, 6, 9, 12, 14, 22, 28, 52

generative AI, 4, 31-35; adversarial, 140; as

lacking understanding, 112; likely job losses

from, 35. See also large language models

INDEX 223

Hockenhull, Jim, 19, 21-22 targeting by, 116, 125-29, 130, 150; tech Hoerni, Jean, 62 company integrated with, 78; Torch and, 80-81, 107-8, 152; in West Bank and Hsu, Jeremy, 3 Gaza, 80, 125-26, See also Gaza Hui, Fan, 154 human-machine team, 149-53; agency and, 149-50, 152, 157, 169-70; alternative to Jensen, Benjamin, 15-16 concept of, 165, 169; Australian Army Jobs, Steve, 68 and, 151-52; brittleness of AI and, 155; Johansson, Scarlett, 140 excluding human labour from analysis, Johnson, James, 7–8 153-57; as form of fetishism, 153-54 Johnson, Matthew, 155-57 human-robot teams, 150-51 Joint All-Domain Command and Control Hume, David, 18 system (JADC2), 101, 103 Hunter, Cameron, 16 Joint Artificial Intelligence Center (JAIC), Hussain, Junaid, 142, 147 Huttenlocher, David, 5-7, 8, 17, 71, 131 Joint Enterprise Defense Infrastructure (JEDI), 76 Ignatius, David, 162-63 joint force commander, 51-52 Igor software, 84, 89 Joint Special Operations Command (JSOC), Imbrie, Andrew, 10 92-94, 159-61, 173 improvised explosive devices (IEDs), 84, Joint Task Force Ares, 142-43 102 - 3India, and military technologies, 20 Karp, Alex, 13, 68, 84, 85, 163 industrial revolutions, 5 Kasparov, Garry, 2 information and psychological operations, Kendall, Frank, 50-51, 174 132, 138-43; in Russo-Ukraine War, key leader engagement, 125 141-42; three elements of, 147 Kissinger, Henry, 5-7, 8, 12, 14, 17, 71, 131 intelligence, military: activities included in, Kleiner, Eugene, 62, 63 57; for counterterrorism in Iraq, 92–94; Kochavi, Aviv, 127, 130 Israel's Unit 8200 and, 97; role of AI for, Krizhevsky, Alex, 29 15, 19, 48-49, 52-54, 58; sensors for, Kropyva, 108 Kurilla, Erik, 159-60, 162 46-47. See also targeting intelligence services, commercial, 105 Kurzweil, Ray, 1 intelligence tests, biased, 30-31 intelligent machines, 24-26 large language models, 31-35; GPUs used Iran: AI-enabled targeting in, 115; cyber in, 29; hallucinations in, 111; limitations specialists in, 131, 133 of, 34-35; limited intelligence of, 34; Iranian nuclear facilities, 97. See also Stuxnet military planning and, 110-12. See also generative AI Iraq, 44, 85-86, 90, 92-94, 118, 160 Isaacson, Walter, 173 Last, Jay, 62 ISIS, campaign against, 87-88, 90, 92, Lattice system, 108-9 118-19, 142-43, 147, 160, 162 Lavender, 128-29, 130, 150, 152 Israel: accused of genocide in Gaza, 177; AI laws of armed conflict, 177-78 capabilities and, 13; attacked by Hamas Legg, Shane, 2 on 7 October 2023, 175-76; cyber attacks Levchin, Max, 69, 83-84, 89 by, 134; cyber capabilities of, 133; defense Levesque, Hector, 31 budget of, 64, 65; four pillars of security Lindsay, Jon, 14-15, 133 in, 57; military application of AI in, 20; littoral combat ship, 155-56 military-tech integration in, 79-81, 96-97; Liu Guozhi, 44 procurement in, 77-78. See also Gaza Loebner, Hugh, 33 Israel Aerospace Industries, 80 logic, in first-wave AI, 25-26 Israel Defense Forces (IDF): collateral damlogical positivists, 25 age caused by, 128; defence industries Lovelace, Ada, 24 as partners to, 80; main mission of, 125; Lovelock, James, 1 Special Operations Forces of, 96-97; Luckey, Palmer, 68, 108

224 INDEX

Machiavelli, Niccolò, 171-72 182-83; mostly in last five years, 22; as machine intelligence, 24-26 organisational story, 62; in recent wars, 19-20; scepticism about, 14-17, 18; slowmachine learning: counterterrorism in Iraq and, 93; decision-making and, 15; fusing ing military operations, 178-80; specific information with, 52, 54, 127; Hinton's functions helped with, 60; tech collaborole in, 5; neural networks of, 30; Projration in, 148; today's uses of, 12-14, 168; ect Maven and, 117; self-driving car and, useful examples of, 15. See also automa-36; of structural destruction in satellite tion of war; cyber operations; decisionmaking, military; military-tech complex; images, 103; targeting by IDF and, 127; three methods of, 23, 28 planning; targeting MAD (mutually assured destruction), 44 military-industrial complex: altered or dis-Major Combat Operations Statistical Model placed, 169; in Cold War, 21, 81; in Israel, (MCOSM), 101-2 80; retired generals and admirals in, 85 military-tech complex, 183; emerging, malware, 131, 132, 133, 135; aimed at Ukraine, 172; autonomous defence against, 146; 21-22, 76, 79, 81, 169, 170-71; introduclimitations of, 146; in Stuxnet, 134 ing private political interests, 171-72, 174; ManTech, 102 lifeworld of cooperation in, 82-83; politimapping: Covid testing and, 122-23; in milicising national defense strategy, 174-75; as profound historic development, 170, tary history, 113 maritime warfare, 181-82 183; as revision of Weberian settlement, Martin, Ciaran, 146-47 171; Special Operations Forces and, 98. Marx, Karl, 153-54 See also tech companies Mattis, James, 47-48, 74-75, 76 Milley, Mark, 19, 174 Maven, 52, 67, 72-76, 116-19, 152, 159, 160 Minsky, Marvin, 25 misinformation, 140 McCarthy, John, 25 McChrystal, Stanley, 86, 92, 93-94, 160-61 missile defense, 46 McCord, Brendan, 118 missiles, in maritime warfare, 181-82 McCulloch, Walter, 28 mission definition, 100 mercenaries, 21, 170, 171-72, 177, 180 Mitchell, Billy, 166 Messenger, Gordon, 103 models, in second-generation AI, 26-27, Metaconstellation, 87-88, 162 29, 30 Microsoft: based on explosion of data, 27; Moore, Gordon, 62 cancelling biased program, 30; cloud of, Mullen, Mike, 131 33-34; computing facilities of, 29-30; multidomain operations, 48, 51-52; in urban failed cloud computing contract and, warfare, 56-57 76; helping Ukraine, 21, 136, 137, 172, Musk, Elon, 8, 37, 40-41, 68, 69, 162, 172-75 174; investment in research and development, 64-65; large language models of, Nadella, Satya, 68 32, 33-34; in military-tech complex, 21; Nagorno-Karabakh wars, 11, 19, 143-45, North Korea attack on software of, 134; 147, 179 Royal Navy battle-management system Napoleon, 113 and, 109; supplying US despite employee Nash, John, 25 complaints, 68; Windows used in Stux-National Security Commission on Artificial net, 134 Intelligence (NSCAI), 6, 48-49, 52, 70, Microworld of UK's Spearhead, 104-6, 152 75, 161 military applications of AI: central to NATO: policies for AI strategy of, 56-57; defence policy, 13; changing the nature of Ukraine defence and, 163; US defence warfare, 7; data processing as prime funcpolicies and, 44 tion of, 55; as existential threat, 7, 13, 22; naval warfare, 181-82 experts' fears regarding, 5-12; historical Ndungu, Tonee, 4 evidence about, 18-22; human control of, Neads, Alex, 151, 152 148, 151; less effective than military lead-Netanyahu, Benjamin, 177 ers believe, 7; major powers using, 20; Netflix, 28 as major technological transformation, neural networks, 5, 28-29, 32

INDEX 225

Newell, Allen, 25, 26 and, 57-58; of every major military North Korea, cyber capabilities of, 133 power, 57-58; of NATO, 56-57; of UK, NotPetya, 135, 136, 145 53-55; of US, 13, 44-53 Price, Rov. 38 Novacene, 1 Noyce, Robert, 62, 63 Prigozhin, Yevgeny, 170, 180 nuclear facilities, cyberattacks against. private military and security companies, 170. See also mercenaries See Stuxnet nuclear weapons, 6, 44, 134, 173 procurement: in British system, 77-79; in Israel, 77-78; by Pentagon, 72-76, 77, 79; Obama, Barack, 45, 70 system of Special Forces, 90-91 OpenAI, 4, 29, 31 productivity: of Amazon's pickers, 40; Operation Glowing Symphony, 142-43, 147 generative AI and, 4, 35; large language Operation Guardian of the Walls, 116, models and, 34 127-28, 176, 179 Project Maven. See Maven Operation Orchard, 134 Prometheus, 1, 5 Operation Swords of Iron, 116, 128 protein structure, 3 Oracle, 76 prototyping method of procurement, 74, 78 Putin, Vladimir, 12, 158, 179 organisational transformation, 20-21, 183. See also military-tech complex Osborne, Michael, 35 quantum computing, 5, 22, 23, 70-71 Page, Larry, 68 Rafael Advanced Defense Systems, 80 Palantir Technologies, 83-89; armed forces Raman, Kal, 39 developing relations with, 81; data-Reagan, Ronald, 69 processing goals of, 83; founded by Thiel, Rebellion Defence, 77, 79 70, 83; human expertise in, 88-89; interregulatory reform, 71-76, 78, 169 personal networking in, 85, 87; investreinforcement learning, 23, 28, 29, 32; to ment in research, 64; security applications identify IEDs, 103 of software in, 84; selling software directly Revolution in Military Affairs, 12, 107, 180 to military units, 85-87, 89; Special Rhombus Power, 83, 93 Operations Forces and, 94; suing the US Rid, Thomas, 132, 139 Army, 88; supporting Ukraine, 21, 162-64, Roberts, Sheldon, 62 174; targeting software of, 162-65; UK robotics: assisting humans in specific func-Ministry of Defence contract with, 78-79. tions, 155; military application of AI to, See also Thiel, Peter 57; US investment in, 13; in US National Panetta, Leon, 131, 133, 145 Defense Strategy, 48 Payne, Kenneth, 7, 11, 12, 14, 16–17 robots: in Amazon fulfilment centres, 39-40; armed in future combat, 167; PayPal, 69, 83-85, 89 Australian Army using, 151; in automated Pentland, Alex, 27 Petraeus, David H., 87 warfare, 9, 11; in ground forces, 150-51; Philip II, 171 in human-robot teams, 150-51; to replace Piacentini, Diego, 39 humans in war, 12; Third Offset Strategy Pitts, Warren, 28 and, 45-46 planning: facilitated by AI, 58, 100-101, Rock, Arthur, 63 168; large language models and, 110-12; rockets, in maritime warfare, 181-82 predictive computer programs for, 102; Ronfeldt, David, 12 process of, 100-101; UK Spearhead Roosevelt, Franklin D., 62 programme for, 103-6; and the use of Roper, Will, 117 AI in more complex operations, 112–13; Rosenberg, Jonathan, 70 US tools used for, 101-3. See also battle-Rosenblatt, Frank, 28 management systems; decision-making route planning, 105-6 by commanders Roy, Anshu, 93-94, 160, 161 policies for AI strategy, 43-44; of China, Rumelhart, David, 28 44–45; data as support for, 57–59; ethics Russell, Bertrand, 25

226 INDEX

Russell, Stuart, viii, 9-10, 12, 14, 22, 52 Sedol, Lee, 2, 154 Russia: aggressions of, 44, 47; cyberattacks self-driving cars, 36-37, 46 by, 135; cyber specialists in, 133; informa-Sensity, 141 tion operations of, 139; US AI strategy sensors: Anduril's automated system of, 108-9; of battle networks, 46-47; of Russo-Ukraine War: Battle of Bakhmut in, Israel in the Occupied Territories, 57, 179-80; drones in, 19, 142, 167; full-scale 126, 127; necessity of degrading enemy's invasion in, 136, 158; importance of AI in, sensors, 179; overload of data from, 53; urban, 56; of US Joint Force, 50 12–13, 19; information and psychological operations in, 141-42; military-tech com-Shamir, Eitan, 91 plex in, 21–22; open-source data in, 162; Shanahan, Jack, 52-53, 56, 72, 74-75, 117-19 and predictions by US's MCOSM pro-Shockley, William, 62 gram, 102; as presage of the future, 180-Shotwell, Gwynne, 174 81; Russian cyber operations in, 136–37, Silicon Valley, 61-66; DIU headquarters in, 140-41; Russian malware in, 136-37; and 73; Pentagon support for, 63; reoriented sinking of Russian ship Moskva, 181; Spefrom libertarian to nationalist, 66-72, cial Operations Forces in, 90; targeting 174; venture capital and, 63-64, 67 in, 168; tech companies influencing US Simon, Herbert, 25, 26 policy on, 174; tech primes' support for Simonov, Andrei, 158 Ukraine in, 172; Ukrainian cyber operasimulations, 16; of aerial combat, 11, 16-17, 102 tions in, 137–38, 141–42; Ukrainian intelsituational awareness: across battlespace, ligence in, 54; US support for Ukraine in, 47; data processing for, 57, 58; in multidomain operations, 52; Palantir software 158-64; wounding of General Gerasimov in, 157–64, 177, 178 and, 88; self-driving car and, 36; in UK Ryan, Mick, 150-51, 152 intelligence policy, 55; of Ukrainian military, 22; in urban warfare, 103; in US sabotage, using cyberspace, 132, 133-35, 136 intelligence policy, 49-50 Sanders, Patrick, 132 Slaughterbots (film), 9 Sandworm, 137 Smith, Brad, 136 Sariel, Yossi, 150, 152 Smith, Brian Cantwell, 25-26 satellites: Battle of Bakhmut and, 180; Meta-Snowden revelations, 132 social media: algorithms used by, 138-39, constellation program and, 87; naval warfare and, 181; sensors on, 54, 55; 140; Armenian diaspora and, 144-45; surveillance data from, 118; Ukrainian bots and, 139-40, 144, 147; Budanov's use military and, 22. See also Starlink of, 142; in information and psychological Sauer, Frank, 10, 12 operations, 147; as open-source data, 162; Scale AI, 110-11 Russian subversion and, 139-40 Scharre, Paul, 11, 36 sociology, vii-ix; technological determinism Schmidt, Eric, 5-7, 8, 9-10, 14, 17, 48, 68, and, 60-61 70-72, 110, 131 software: as main product of tech companies, Schwarzenegger, Arnold, vii 72-73; in second-generation AI, 27-28 second-generation AI, 26-31; fallibility of, Solomonoff, Ray, 25 30–31; improbability of full automation Soviet Union, 44 under, 40; as probabilistic and inductive, space: in multidomain operations, 51; in UK defence, 54; in US National Military 26-27, 30, 31, 32, 42; three critical enablers of, 27. See also large language models Strategy, 48 Second Offset Strategy, 44 SpaceX: and travel to Mars, 40; in militarysecurity studies: automation of war and, 10, tech complex, 21; providing services in 12, 41; cyber attacks and, 133; human-Ukraine, 173-74 machine teams and, 151; ignoring Spearhead, 103-6, 152 organisational transformations, 97-98; Special Competitive Studies Project (SCSP), limitations of military AI and, 10; powers 110, 111-12 of AI and, viii; Project Maven and, 116; Special Operations Forces: counterterrortechnological determinism in, 61 ist role of, 89-90, 91; drowning in data,

INDEX 227

95-96; of Israel Defense Forces, 96-97; large budgets of, 90; Palantir software used by, 86-87; procurement system of, 90-91; specific missions of, 92, 93; tech companies partnered with, 89–96, 98; transnational relations of, 91-92; unique in politico-military hierarchies, 91; unique status in US armed forces, 86, 90; in wounding of General Gerasimov, 157 spying, as cyber operation, 132, 135-36, 137 staff officers: becoming more essential, 113; data and, 101; large language models and, 110, 111; predictive calculations by, 102; relieved some of the burden of planning, 103, 105-6; supporting commanders' decisions, 164-65. See also headquarters Starlink: armed forces developing relations with, 81; Ukraine and, 21, 162, 172-75 Stephens, Trae, 108 stock market, 4 Stone, Brad, 39 Stop Killer Robots campaign, viii, 8-9, 10 StormCloud, 109 strategic bombing, 166-67 strategic studies, vii strategy: experts' fears about AI and, 6-7; made by AI, viii, 8; made by company executives, 39, 42; tech companies' involvement in, 174-75. See also policies for AI strategy Stuxnet, 97, 134, 146 subversion: as cyber operation, 132; Russian active measures and, 139. See also information and psychological operations Suchman, Lucy, 10 Suleyman, Mustafa, 1-2, 33 Sullivan, Jake, 174 Summers, Jared, 160 Sunak, Rishi, 4-5 supervised learning, 23, 28, 29; NATO policy on targeting and, 56 surveillance systems, 12; drones in, 13; failure of Israeli system, 175-76; of Ukrainian military, 22. See also sensors Sutskever, Ilya, 29 Swift, Taylor, 140 Syria, 90, 103, 118, 134 Taiwan, imagined Chinese assault on, 182

Taiwan, imagined Chinese assault on, 182
Taliban, 90
targeting: agency of AI in, 149–50; AI
requiring more people for, 130; for Covid
testing, 116, 119–25, 130; of customers
by companies, 115; dynamic, 127, 158;

of General Gerasimov, 157-64, 177, 178; human-machine team and, 149-50; human teamwork in, 129-30; important role of AI in, 46-47, 58, 168; by Israel Defense Forces, 116, 125–29, 130; linking disparate data for, 129; in multidomain operations, 52; NATO policy and, 56; speed and precision of, 178; susceptibility of AI to errors in, 15-16; by UK forces, 55; by US Air Force, 51. See also intelligence, military; Maven Task Force Dragon, 159, 160, 161, 162-63, 164-65, 177 Tay (chatbot), 30 teamwork: of humans for targeting, 129-30; of military personnel and technicians, 169 tech companies: armed forces needing to collaborate with, 66; based on explosion of data, 27; competing for best talent, 65–66; competing with one another, 76; defence ministries and, viii, ix; dynamic market for software of, 72-73; helping Ukraine, 136, 137; integrated into military operations, 21; with offices near the Pentagon, 76; with offices near UK Ministry of Defence, 79; operating as part of state forces, 171; selling software directly to military units, 89; Special Operations Forces partnering with, 89–96, 98; teams of experts in, 156-57; using algorithms to influence consumers, 139. See also military-tech complex; tech primes technological determinism, 60-62, 153 technology: of China in new century, 44; as a social product, 60-61; of US in Cold War, 44 tech primes: in disputes with US government, 67-68; influencing state interests, 172; investing in large language models, 33-34; and investments in research and development, 64-65; needing access to operational data, 169; Russo-Ukraine War and, 172; vast computing facilities of, 29-30; venture capital and, 63-64. See also tech companies

Telegram, 141, 144

The Terminator (film), vii, 53
terrorist attacks on 11 September 2001, 69, 83, 90
terrorist cells in Gaza and West Bank, 125–26
terrorists, targeting of, 150
Tesla, 36, 37, 41
Thiel, Peter, 58, 68–70, 71, 72, 83–85, 87, 88–89. See also Palantir Technologies

228 INDEX

Third Offset Strategy, 13, 44-46, 57; autonomous systems in, 45-46, 47-48; procurement reform and, 73; targeting and, 116 Toolan, John, 87 Torch, 80-81, 107, 152 Tossell, Ben, 33 trace italienne, 62 Traitorous Eight, 62, 63 transistors, 24, 28 Trenchard, Hugh, 166 Trump, Donald, Thiel's support for, 68 Trump administration, 45 Tunnell, Harry, 85-86 Turing, Alan, 24-25 Turing test, 25, 33 Twitter, bots on, 140 Uber, 36

UK: AI as opportunity for, 4-5; AI capabilities and, 13; behind the US in military application of AI, 76-77; cyber capabilities of, 133; defense budget of, 64, 65, 77; military application of AI in, 20; policies for AI strategy of, 53-55; procurement systems in, 77-79; Spearhead planning programme for, 103-6, 152; Special Operations Forces in, 96

Ukraine: AI-enabled intelligence in 2014, 47; battle-management systems of, 108; IT Army of, 137-38, 141, 147; Russian cyberattacks of 2014-2017 on, 135; US support for, 158. See also Russo-Ukraine War

understanding: lacked by generative AI, 112; not recognized by AI, 30-31, 36, 42; in US intelligence policy, 49

Unit 8200, 97, 116, 126, 127, 133, 134, 177 unsupervised learning, 23, 28, 29, 32

urban operations: planning of, 102-3; targeting in, 126, 128

urban warfare: AI-enabled, 182; building destruction in, 103; multidomain approach to, 56-57

US: cyber capabilities of, 133; defense budget of, 64, 65; drone swarms and, 13; as a pioneer in military application of AI, 20; possible war between China and, 181-82

US Air Force, 17, 50-51, 84, 117

US Army, 51-53

US Marine Corps, 48, 87, 110, 182

US Navy littoral combat ship, 155-56 US policies for AI strategy, 13, 44-53; joint forces in, 49-50, 51; massive datasets and, 48–49, 52; of separate services, 50–53

US presidential election of 2016, 139, 140

Varian, Hal, 27

venture capital, and Silicon Valley, 63-64, 67, 169

Vera, Alonso, 155-56

Vietnam, 44, 89

Virilio, Paul, 178

viruses, biological, 116, 119-25, 130

viruses, in computers, 131, 132, 133, 134, 137, 146

Wagner Group, 170

Walmart, 3-4, 36, 39

war: becoming slower, 178-80, 182; being reconfigured by AI, 20; between China and US, 181-82; as complex environment, 14-15, 16, 31; definition of, 132; incomplete and inaccurate data in, 15; influenced by private-sector tech companies, 21, 174; recent evidence from, 19-20, 22; trending towards attritional and positional war, 183. See also automation of war

warbots, 11

war-gaming, 102

War on Terror, 70, 87, 90

wastewater, viral load in, 123-24

waterfall system, 72, 73, 77, 79

Waymo, 36, 37, 46

weapons, autonomous and lethal, 8-12; Australian Army and, 151; ethical concerns about, 175, 176; as eventual possibility, 46, 57-58, 167-68; inaccurate obsession with, 52-53; of Israel, 57; scholars concerned about, 59. See also drone swarms, autonomous

weapons, nuclear, 6, 44, 134, 173

Weber, Max, 171

Weinberger, Sharon, 87

West Bank, 80, 125-26

Whyte, Christopher, 15-16

Wiener, Norbert, 24

Williams, John, 12

Winograd schemas, 30-31, 33

Wittgenstein, Ludwig, 25

Wong, Felix, 3

Work, Robert, 45–47, 48, 57, 72, 74, 83, 133

XVIII Airborne Corps, 158-64, 177

Yon, Michael, 159

Zambellas, George, 54 Zelensky, Volodymyr, 19, 140-41, 173, 174, 179