1 War Virtually

This book is about the pursuit of a dream—a dream that, over time, may turn out to be a nightmare. It's the story of how a group of scientists and engineers are racing to develop, acquire, and adapt computerized, data-driven technologies and techniques in order to automate war, predict conflict, and regulate human thought and behavior. The advent of artificial intelligence—particularly machine learning—is accelerating the military's relentless drive toward virtual combat zones and autonomous weapons, in the United States and elsewhere. To the outside world, this sounds like the stuff of fantasy, but from the inside, science fiction appears to be on the verge of becoming science fact. At this stage of history, it's still not clear whether the outsiders or the insiders will be correct in their interpretations.

Military planners and policymakers are attempting to harness the latest scientific and technical knowledge to prepare for war, virtually. The technological fantasy of virtual warfare is alluring—even seductive—for it suggests that someday we may conduct wars without soldiers, without physical battlegrounds, and maybe even without death.[1] Although there is no agreed-upon definition for virtual war, as a starting point we might think of it as a confluence of long-term trends, tools, and techniques: war conducted by robotic systems, some of which are being programmed for

ethical decision-making; the emergence of Silicon Valley as a major center for defense and intelligence work; algorithmically driven propaganda campaigns and psychological operations (psyops) developed and deployed through social media platforms; next-generation social science models aimed at discovering what drives human cooperation and social instability; and predictive modeling and simulation programs, including some ostensibly designed to foresee future conflict.[2] Although these projects have different historical trajectories, they all have something in common: they're predicated on the production, availability, or analysis of large amounts of data—big data—a commodity so valuable that some call it "the new oil."[3]

In the United States, those undertaking such work are employed in military and intelligence agencies, defense conglomerates and contract firms, university laboratories, and federally funded research centers. The protagonists of the story include computer scientists, mathematicians, and robotics engineers, as well as psychologists, political scientists, anthropologists, and other social scientists. At its core, this book is about how these men and women are attempting to engineer a more predictable, manageable world—not just by means of electronic circuitry and computer code, but also by means of behavioral and social engineering—that is, *human* engineering. Under certain conditions, cultural and behavioral information can become a weapon, what in military terms is called a force multiplier—a way of more effectively exerting control over people and populations.

Given the breathtaking scope of the proposed technologies and their potential power, it's easy to overlook their limitations and risks, since so many of them are still in the realm of make-believe. It's even easier to overlook the serious ethical and moral dilemmas posed by autonomous weapon systems, predictive modeling software, militarized data, and algorithmically driven psyop campaigns—particularly at a time when some observers are warning of an "AI [artifical intelligence] arms race" between the United States and rival powers.[4]

The rush to create computational systems for virtual warfare reveals a fatal flaw that's been with *Homo sapiens* as long as civilization itself: *hubris,* that persistent and terrible human tendency to embrace blind ambition and arrogant self-confidence. The ancient Greeks understood this weakness, and learned about its perils through myths such as the

tragedy of Icarus, a young man so enthralled with the power of human invention that he forgot about its limits. But instead of tragedy, our myth-making machinery produces technological celebrities like Tony Stark, Iron Man's brash, brilliant alter ego. There's little room for hubris—much less ethical ambiguity—in the Manichean fantasy worlds of Hollywood superheroes and American politics. But it's important to remember how, in a heavily militarized society like our own, overfunded technology projects and reckless overconfidence can quickly turn to disaster.

UPGRADE

The latest generation of military tools is a continuation of long-standing trends toward high-tech warfare. For example, US scientists have experienced changing patterns of military influence over their work during the course of at least a century. In the early 1960s, as the United States was about to escalate its war in Vietnam, a well-known physicist famously told Defense Secretary Robert McNamara that "while World War I might have been considered the chemists' war, and World War II was considered the physicists' war, World War III . . . might well have to be considered the social scientists' war."[5] By that time, military and intelligence agencies were integrating knowledge from psychology, economics, and anthropology into their tactical missions, provoking controversy and criticism from social scientists concerned about the lethal application of their work.[6]

But what's happening today is broader in scope than anything the military-industrial complex has created before. If you think of the earlier phases of high-tech conflict as versions 1.0, 2.0, and 3.0, then you might say that in the twenty-first century, a major upgrade is under way: chemists, physicists, and social scientists are now working together with roboticists and computer scientists to create tools for conducting data-driven warfare. The advent of War 4.0 is upon us, sparked by the so-called Revolution in Military Affairs—the idea that advanced computing, informatics, precision strike missiles, and other new technologies are the answer to all of America's security problems. In recent years, observers have warned of a drift toward "future war," the rise of "genius weapons," and "T-minus AI."[7]

Like most updates, the latest version of warfare is built upon what came before. More than a half-century ago, the US military launched an advanced electronic warfare campaign targeting enemy convoys traveling across the Ho Chi Minh Trail, a network of roads linking North and South Vietnam. For the Vietcong, the route was a vital lifeline for transporting equipment, weapons, and soldiers. The US military program, dubbed Operation Igloo White, used computers and communication systems to compile data collected by thousands of widely dispersed electronic devices such as microphones, seismic monitors, magnetic sensors, and vehicle ignition detectors. Despite high hopes and a gargantuan price tag, the program was not nearly as effective as its architects had hoped.[8]

Such efforts weren't limited to the collection of hard data—sometimes, they were based on "soft" social science data. A case in point: the Phoenix Program, a brutal counterinsurgency initiative launched by the CIA and the Defense Department in 1968. At about the same time that Operation Igloo White was under way, military officials and intelligence agents were using IBM 1401 mainframe computers to compile ethnographic and demographic information collected by US civil affairs officers. Eventually, they created a database of suspected Vietcong supporters and communists. American advisors, mercenary fighters, and South Vietnamese soldiers then used the computerized blacklist—called the Vietcong Infrastructure Information System—to methodically assassinate more than twenty-five thousand people, mostly civilians, under the aegis of the Phoenix Program. For its users, the computer program magically transformed what would otherwise appear to be a subjective, arbitrary, bloody assassination campaign into a seemingly rational, objective, and antiseptic process of social control.[9]

War 4.0 differs from earlier forms of automated conflict and computerized weapon systems. While it's true that US military personnel used computers as early as 1946, when they programmed ENIAC (the Electronic Numerical Integrator and Computer) to develop better ballistic trajectory charts and hydrogen bombs, today military and intelligence agencies and firms are using not only advanced computational hardware and software, but also vast amounts of data—and from infinitely more sources. The term *big data,* ambiguous as it is, hints at the scale of change. Apart from the expansion of electronic sensors ranging from high-resolution satellites

Figure 1. At the height of the US war in Vietnam, American government agencies and the military used IBM mainframe computers for the Phoenix Program. Photo courtesy of Michigan State University Archives.

and drones to closed-circuit TV cameras, billions of people around the world leave enormous amounts of digital residue behind when using the internet, social media, cell phones, personal fitness trackers, and virtual assistants like Apple's Siri or Amazon's Alexa.[10] Both actual (face-to-face) and virtual (face-to-screen) interactions are subject to closer surveillance than ever before. Military and intelligence agencies don't always have easy access to this data, but many of the corporations that control such information—such as Amazon, Google, and Microsoft—have forged close relationships with the Pentagon and the US intelligence community.

Another difference is that the technologies often rely on algorithms to construct behavioral models for anticipating or even predicting human behavior, in virtual and actual realms. Algorithms provide the means by which large amounts of raw data about our virtual lives can be processed and reassembled as probable outcomes, political preferences, propaganda, or products. If you've ever used Facebook, Instagram, Amazon, Netflix,

or Google, you probably have an intuitive sense of how the algorithms work. Unless you're willing and able to opt out by changing your privacy settings—which is typically a cumbersome, confusing, time-consuming process—companies constantly track your internet searches, online purchases, and webpage visits, then feed the data into mathematical formulas. Those formulas, or algorithms, use that data to make calculations, essentially educated guesses about what you might like, and then "recommend" things to you—clothes, shoes, movies, appliances, political candidates, and much more.[11] Algorithms are what fill your news feeds with articles based on your previously monitored online reading or internet browsing habits, and Big Tech firms have built an industry on them by using your data to help their clients target you for online ads. These techniques have helped Facebook, Google, and Amazon dominate the world of digital advertising, which now far eclipses print, TV, and radio ads.[12] When people are transformed into data points, and human relationships become mere networks, the commodification of personal information is all but inevitable without meaningful privacy regulation. What this means in practical terms is that all of us risk having our digital lives become part of the military-industrial economy.

From the perspective of a data scientist, handheld internet-ready digital devices have transfigured billions of people worldwide into atomized data production machines, feeding information into hundreds, if not thousands, of algorithms on a daily basis. The militarization of this data is now a routine part of the process, as suggested by recent reports detailing the Defense Intelligence Agency's use of commercially available geolocation data collected from cell phones.[13] Military and intelligence agencies can use such data not only for surveillance, but also to reconstruct social networks and even to lethally target individual people. A dramatic case occurred in September 2011, when, in a joint drone operation authorized by the Obama administration, CIA and US military personnel assassinated Anwar al-Awlaki—an ardent US-born Muslim cleric—in Yemen. Those who organized the drone strike targeted Awlaki based on the location of his cell phone, which was monitored by the National Security Agency as part of a surveillance program. Two weeks later, a CIA drone attack using the same kind of data killed another US citizen: Awlaki's sixteen-year-old son, Abdulrahman al-Awlaki.[14]

Although Awlaki was intentionally assassinated by US forces, other Americans—and many thousands of civilians in Afghanistan and other parts of Central Asia and the Middle East—have been inadvertently killed by drones.[15] These cases foreshadow a major flaw in the latest iteration of automated war: the imprecision of the technologies, and the great margins of error that accompany even the most sophisticated new weapon systems. In their most advanced form, the computerized tools make use of artificial intelligence, such as iterative machine learning techniques. Although proponents argue that the weapons perform at levels comparable or even superior to humans, they rarely provide conclusive evidence to support their claims. Yet the march to adopt these machines continues apace. The Pentagon's quest to develop AI for military applications has led to the creation of an Algorithmic Warfare Cross-Functional Team, also known as Project Maven. Among its first objectives was to analyze thousands of hours of video footage from drones to produce "actionable intelligence" that might be used to locate ISIS fighters in Syria and Iraq (see chapter 3).[16]

Still another characteristic that differentiates these novel forms of virtual war from earlier attempts is heavy reliance on a stripped-down, portable version of cultural and behavioral knowledge—culture in a box.[17] The problem is that the information is often superficial, shallow, devoid of context. In the world of business, an overly simplistic understanding of cultural dynamics might mean losing potential customers. On the battlefield, it can mean someone getting killed.

PIVOT POINTS

How and when did the shift to virtual war begin? Or, to put it in slightly different terms, how and when did data become a weapon? There are no easy answers to the question, but we can trace several interrelated, incremental changes that began to emerge over the past decade and—little by little—pushed things in this direction. Some of these transformations were technological, some were geopolitical, some were cultural, and some were economic. In addition, billions of people around the world began to communicate and interact with others in substantially different ways—

most significantly, online. It's helpful to think about the quest for an automated battlefield as a kind of convergence, as the end point of these changes.

Among the most significant factors propelling the trend toward data-driven warfare is the rapid diffusion of internet-ready smartphones across the globe, beginning in about 2007.[18] Since the advent of the internet in 1991, *Homo sapiens* had been gradually spending more time online, but the portability and convenience of smartphones amplified that pattern—so much so that by 2019, American smartphone users were spending an average of more than three hours a day on their mobile devices—apart from the time spent on desktop or laptop computers.[19] During the era of COVID-19, this undoubtedly increased as people worked, attended classes, and even socialized in virtual realms. From the perspective of institutions seeking to monitor people's ideas, interactions, interests, or idiosyncrasies, smartphones, tablets, and other mobile devices have become powerful tools for collecting huge quantities of data.

To make matters worse, virtual life has been an easy target for spies of all kinds—and a windfall for intelligence agencies around the world. Classified documents from the US National Security Administration (NSA), leaked by Edward Snowden in 2013, revealed the scale of surveillance. The NSA had spied on US citizens and citizens from other countries by "listening in" through the internet. The agency had stored data in server farms and then analyzed it, using algorithms to search for patterns. It would be difficult to overestimate the significance of Snowden's revelation. "Although the NSA was authorized by the US administration to execute such global surveillance in order to prevent terrorist attacks, the fact that the US government spied on its own citizens created a dangerous precedent," wrote a critic.[20]

Another factor that made an impact on the growth of virtual forms of war—not only in the United States, but also in Europe, Russia, China, and other regions—was the meteoric rise of the Islamic State of Iraq and Syria, or ISIS.[21] The group, which sprouted from the ashes of Al Qaeda, grew rapidly in 2013 and 2014, during a period of extreme political and social turmoil in the Middle East. The US-led invasion and occupation of Iraq—and the subsequent fragmentation of Iraqi society—played a leading role in creating the conditions that allowed ISIS to flourish.[22] For more than

five years, ISIS ruled a self-styled caliphate that seized and maintained political control over large swaths of northern Iraq and southern Syria. Its officials collected taxes, enforced a brutal interpretation of Sharia law, and even issued a new currency: gold and silver dinars.

ISIS launched a sophisticated social media campaign appealing to young people who had faced discrimination, segregation, and harsh treatment as members of minority Muslim communities in many different regions of the world, including North America, Europe, and Central and Southeast Asia.[23] The organization relied on propaganda messages, which included spectacularly violent video clips, to attract recruits, and they were astonishingly effective: by June 2014, approximately forty thousand people from more than eighty nations had affiliated themselves with ISIS in Iraq and Syria, including many Europeans.[24] Nearly five thousand of the recruits were women. Never before had an army relied so heavily on virtual communication as the basis for mobilizing troops. Not surprisingly, American, European, Russian, and Chinese military officials ramped up efforts to counter violent extremists—particularly those claiming to defend Islam—through various forms of cyberwarfare. These projects intensified once attacks by "homegrown" extremists, presumably radicalized in online spaces, began to spread.[25]

The explosion of ISIS onto the world scene led the US military to adopt radically different methods for fighting insurgents. For nearly a decade, American forces in Iraq and Afghanistan had been using a modern interpretation of classic counterinsurgency doctrine. This approach, which was closely associated with General David Petraeus, advocated a return to classic "small wars" techniques developed by David Galula, a French military officer who fought in the Algerian war of independence, and other colonial-era military theorists.[26] Once it became clear that American counterinsurgency efforts were failing, several influential military planners—most notably US Army Lieutenant General Michael Flynn, director of the Defense Intelligence Agency from 2012 to 2014 and US national security advisor for four months in 2017—pushed to pursue a data-intensive strategy, based on easily accessible open-source data and fine-grained "human intelligence" gathered by those in close contact with civilians.[27] Flynn advocated a hybrid approach that might be called computational counterinsurgency, in which social scientists would cooperate with data scientists. At the same

time that he was publicly pushing for the military to employ "cultural experts, social experts, archaeologists, [and] anthropologists," he was also working with computer scientists from Johns Hopkins University to trace insurgent networks in Iraq using massive datasets.[28]

Yet another metamorphosis that has pushed war virtually forward over the past decade is a shift in global geopolitics. After the attacks of September 11, 2001, the efforts of the US government had been geared toward protecting the country from Islamic extremism. By 2011, those efforts had begun to shift almost imperceptibly toward a more familiar form of great-power rivalry. As China's economic and political power and influence grew, and as Russia began to reassert itself aggressively on the world stage by invading Crimea and then Ukraine, many observers started to compare the geopolitical landscape to that of previous centuries.[29] However, unlike in previous periods, military officials began preparing to launch and defend against cyberattacks of all kinds: propaganda and disinformation campaigns, malware designed to infect government computers, electronic sabotage of power grids and water treatment plants, and much more.[30] These patterns took shape during the Obama years, and they intensified during the Trump presidency. Other trends that may have played a role include public condemnation of Russian involvement in the 2016 US presidential elections, an escalating trade war with China, and deteriorating diplomatic relations with Iran during the Trump era. American policymakers' pivot toward Russia, China, Iran, and other rival powers has allowed the Pentagon, and the US Congress, to slide back toward a technology-heavy agenda—one focused less on training and educating military personnel than on building machines that will create work for voters living in congressional districts. Think of it as Eisenhower's military-industrial complex, revamped for the twenty-first century.

Taken together, these transformations propelled the trend toward virtual war, but they didn't guarantee it. US defense and intelligence agencies are expansive bureaucracies with competing interests and points of view, and they've never been monolithic. Although technology firms and military contractors jumped at the chance to promote high-tech solutions for a dangerous world, not all military and intelligence officials were convinced that these tools would work. Some who were less tech-savvy resented the idea that they might be asked to radically change their ways. Others were wor-