Journal of Global Security Studies, 9(2), 2024, ogae009
https://doi.org/10.1093/jogss/ogae009
Research Article

OXFORD

Digital Targeting: Artificial Intelligence, Data, and Military Intelligence

Anthony King

University of Exeter, UK

Abstract

It is widely believed that we are on the brink of another military revolution. Today, states are actively seeking to harness the power of AI for military advantage. The question of AI is therefore of profound concern to security studies scholars concerned with global issues. Up to now, the literature has tended to concentrate on AI-enabled lethal autonomous weapons; scholars have been fascinated by the possible appearance of autonomous drone swarms and their implications for security, conflict, and war. This article takes an alternative view. It argues that AI has already begun to play a significant role in military operations and is likely to be more important in the future. However, the attention to lethal autonomous weapons is exaggerated. The armed forces have principally employed AI, not to automate weapons but to help process data. AI has been used to augment military intelligence. Above all, the armed forces have harnessed AI to accelerate and improve military targeting. The article explores two recent cases where the armed forces have used data and AI to target: COVID testing in Liverpool in 2020 and the US's Security Assistance Group-Ukraine in the Ukraine War in 2022.

Resumen

Existe la creencia generalizada de que nos encontramos al borde de otra revolución militar. Hoy en día, los Estados buscan, de manera activa, aprovechar el poder que ofrece la IA con el fin de obtener ventajas militares. Por lo tanto, la cuestión de la IA preocupa profundamente a los académicos del campo de los estudios de seguridad que se ocupan de cuestiones globales. Hasta ahora, la literatura había tendido a concentrarse en las armas autónomas letales derivadas de la IA, ya que los académicos estaban fascinados por la posible aparición de enjambres de drones autónomos y por sus implicaciones para la seguridad, el conflicto y la guerra. Este artículo toma una visión alternativa. Argumenta que la IA ya ha comenzado a desempeñar un papel importante en las operaciones militares y que es probable que este papel sea aún más importante en el futuro. Sin embargo, la atención prestada a las armas autónomas letales resulta exagerado. Las fuerzas armadas han empleado principalmente la IA, no para automatizar armas, sino para ayudar a procesar datos. La IA se ha utilizado para aumentar la inteligencia militar. las fuerzas armadas han aprovechado, sobre todo, la IA para acelerar y mejorar la selección de objetivos militares. El artículo explora dos casos recientes en los que las fuerzas armadas han utilizado tanto datos como IA para seleccionar los objetivos: Las pruebas de COVID en Liverpool en 2020, y la Fuerza de Asistencia de Seguridad de EE. UU. en la guerra de Ucrania en 2022.

Résumé

Beaucoup pensent qu'une révolution militaire se prépare. Aujourd'hui, les États cherchent activement à tirer parti de la puissance de l'IA sur le plan militaire. La question de l'IA inquiète donc fortement les chercheurs en études de la sécurité qui s'intéressent aux problématiques mondiales. Jusqu'ici,

King, Anthony (2024) Digital Targeting: Artificial Intelligence, Data, and Military Intelligence. *Journal of Global Security Studies*, https://doi.org/10.1093/jogss/ogae009

la littérature a eu tendance à se concentrer sur les armes létales autonomes alimentées par l'IA; les chercheurs se fascinent pour l'apparition potentielle de nuées de drones autonomes, et leurs implications en matière de sécurité, de conflit et de guerre. Cet article adopte un autre point de vue. Il affirme que l'IA a déjà commencé à jouer un rôle important au sein des opérations militaires, un rôle qui pourrait bien s'accroître à l'avenir. Cependant, l'attention accordée aux armes autonomes létales est disproportionnée. Les forces armées ont majoritairement employé l'IA pour traiter plus facilement des données, et non pour automatiser des armes. L'IA sert à renforcer les capacités du renseignement militaire. Les forces armées ont surtout exploité l'IA pour accélérer et améliorer le ciblage militaire. L'article s'intéresse à deux cas récents d'utilisation des données et de l'IA par les forces armées pour cibler: les tests Covid à Liverpool en 2020 et la Force d'assistance et de sécurité des États-Unis lors de la guerre en Ukraine en 2022.

Keywords: AI, Data, lethal autonomous weapons, armed forces, Russo-Ukraine War, COVID
Palabras clave: IA, Datos, armas autónomas letales, fuerzas armadas, Guerra ruso-ucraniana, COVID
Mots clés: IA, données, armes autonomes létales, forces armées, guerre russo-ukrainienne, Covid

Introduction

It is widely believed that we are on the brink of another military revolution. Artificial intelligence will revolutionize warfare, as gunpowder, tanks, aircraft, and the atom bomb did in previous eras. 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" (Kania 2017, 6). Similarly, Vladimir Putin declared: "Whoever becomes the leader in this sphere will become ruler of the world" (Horowitz et al. 2018, 16). In response to the challenge posed by China and Russia, the US has committed to a "Third Offset" Strategy. It will invest heavily in AI, autonomy, and robotics to sustain its advantage in defense. Colonel Andrew Cukor, a US Marine Corps Colonel who played an important role in Project Maven, declared that the US is in an "AI arms race" (Gonzalez 2022, 62). In September 2018, DARPA announced a $2 billion campaign to develop the next wave of AI (Waltzman 2020, 3; Baker 2021). The Department of Defence (DOD) issued its AI strategy in 2019 with a major increase in AI funding (Wyatt 2020, 10). Smaller states are equally committed to the military development of AI; the UK and Israel, for instance, are developing their capabilities in this area.

In the light of these dramatic developments, scholars working on global security have become deeply interested about the military application of AI. In particular, scholars have addressed the political, ethical, and military implications of the proliferation of AI-enabled lethal autonomous weapons. For instance, in their recent monograph on AI, Ben Buchanan and Andrew Imrie have claimed that AI represents the new fire (Buchanan and Imbrie 2022, 1–2). Lethal autonomy refers to many potential weapons, including nuclear ones (Johnson 2023). However, when scholars have discussed the problem of lethal autonomy, they most frequently have autonomous drone swarms in mind. They believe that the future battlefield will be dominated by swarms of Uncrewed Aerial Systems (UAVs) directed by AI, independently of any human direction. Until now, China and the US have only experimented with the possibility of autonomous swarms. Yet, the lethal autonomous drone swarm has captured the scholarly imagination. Scholars believe we are about to see an AI-driven revolution in lethal autonomy (Garcia 2018; Williams 2021; Johnson 2022, 334–341; Arkin 2010; Altmann and Sauer 2017; Haas and Fischer 2017; Kania 2017; Bode and Huelss 2018; Kissinger et al. 2021; Amoore 2009; Hambling 2015; Kania 2019; Scharre 2019; Brose 2020; Frantzmann Drone Wars 2021; Payne 2021; Russell 2021, 51; Payne '7–32; Ayoub and Payne 2016; Payne 2018).

Scholars are not deluded to be interested in autonomous weapon systems and drone swarms, in particular. They are right to have pointed out the potential of drones. In the last two decades, there have been some remarkable developments, drones have moved from playing a small surveillance role to becoming an indispensable battlefield weapon. Indeed, the autonomous drone swarm seems to be on the horizon. The Chinese have made significant advances in swarm intelligence. In 2017, a formation of 1000 UAVs flew at the Guanghzhou Airshow. In 2017, China Electronic

Technology Group flew a 119 fixed-wing UAV swarm (Kania 2017, 22–23; Kania 2019). In October 2016, the US's DOD demonstrated a swarm of 103 Perdix microdrones capable of "advanced swarm behaviours such as collective decision-making, adaptive formation flying and self-healing" (Altmann and Sauer 2017, 123). In 2022, the US Army procured and tested the TSM-800 drone swarm, manufactured by Booz Allen. At Fort Irwin, in recent trials, the US Army has successfully been able to fly a pre-programed swarm of 97 TSM-800 drones to attack a designated target. The US Navy has also tested super-swarms, which look and fly like flocks of birds, to deceive enemy radar. Many other countries, such as Israel, are experimenting with drone swarms.

When they predict the rise of drone swarms, academics extrapolate from the present to the future. This is a valid endeavor, especially at the policy level, but its epistemological dangers are evident. There is no evidence about the future. So any prediction, however plausible it might seem, can only be speculation in the proper philosophical sense. David Hume, the eminent Scottish philosopher, highlighted the dangers of prediction and presumption over two hundred years ago from his position of "determined scepticism." In a famous passage in his *Treatise of Human Nature*, David Hume showed that causality, so often presumed by philosophers and theologians, can never actually be assumed: "We have no other notion of cause and effect, but that of certain objects, which have been *always conjoined* together" (Hume 1985, 141). In the future, even the most apparently ineluctable causal links might not operate. Given the epistemological dangers of prediction, security scholars may have been too quick to draw causal conclusions about AI and the rise of autonomous weapons. They have presumed too much. Consequently, this paper takes an explicitly empirical approach. It focuses not on how AI might change military operations in the future, but on how the armed forces have actually employed AI in the recent past.

An empirical analysis of the actual military usage of AI suggests that the emphasis on lethal autonomy may be overwrought. Remote systems have proliferated widely—and very rapidly—in the last two decades. Automated weapons, like Aegis, Phalanx, Patriot, and SGR-A1, have been used for years. In the maritime domain, autonomous systems are already important; swarming underwater vessels are nascent, serving mainly as a mobile early warning system. Autonomous weapons systems are likely to become more important in the future. Yet, in the last decade, lethal autonomy has not been the primary military application of AI (Jensen et al. 2020, 540). As a number of scholars have noted, AI has become important to the armed forces in planning, cyber, and information operations. However, one of the most important areas of AI development has been in military intelligence and, above all, in targeting. AI has been employed for data collection, collation, and analysis. AI has been used to process data so that commanders have a better understanding of the battlespace and have been able to target more effectively (Berman et al. 2018; Ford and Hoskins 2022, 5; Goldfarb and Lindsay 2021).

Data refer to digital information stored in cyberspace; data refer to all the virtual material that is held on the internet, in the cloud, or on any computer system. Every activity in cyberspace—a text message, an internet order, a photograph—leaves a small trace of data. As a result of the rise of the internet and smartphones, there has been an explosion of data in the last twenty years. Consequently, 18 million gigabytes of new data are created globally every minute and that figure is accelerating (Suleyman 2023, 33). As Hal Varian, the chief economist at Google, stated "between the dawn of civilization and 2003 we only created 5 exabytes of information; now we're creating that amount every two days" (Gonzalez 2022, 134). In 2023, the world has generated 120 zettabytes of data; that figure is projected to be 181 zettabytes by 2025 (https://www.statista.com/statistics/871513/worldwide-data-created/). This mass of data is highly revealing; it provides novel insights into almost every activity. Many commercial companies and governments have tried to exploit data to their advantage. Data are also a potentially vast and fertile resource for the armed forces. Indeed, scholars have, therefore, questioned the centrality of the drone swarm in debates about AI. Data processed by AI is more mundane—but also potentially more revolutionary—for the armed forces. Above all, data offer the armed forces new possibilities for targeting opponents.

This article is, therefore, a modest attempt to rebalance the security study debates about AI. It moves the conversation from drone swarms and other lethal autonomous weapons to digitized, data-enabled military intelligence and targeting. This paper examines how data, processed by AI, has already been employed to improve targeting. To do this, and in the skeptical spirit of Hume, it does not predict or speculate. It examines two empirical case studies: the British Army's response to a COVID outbreak in Liverpool in late 2020 and the US Army's XVIII Airborne Corps' support to Ukrainian military operations during the Russo-Ukraine War. They are very different cases. In Liverpool, the British Army was trying to organize mass asymptomatic testing of the civilian population. It was a benign operation in support of civil powers, though it occurred in a time of national emergency

when infection rates placed unprecedented pressure on the ability of the UK's healthcare system to cope in the face of a rapidly mutating COVID-19 virus. The operation saved many lives in Liverpool, broke the chains of COVID-19 transmission across Merseyside, and accelerated the city's economic recovery. Importantly, it formed the basis of new targeted methods of testing, providing the blueprint for national delivery by the Department of Health as well as the framework into which a civilian follow-on force could take over. In 2022, the XVIII Airborne Corps commanded the Security Assistance Group-Ukraine, providing support to the Ukrainian War effort. That support was very wide-ranging, including mundane tasks like organizing logistics. However, XVIII Airborne Corps also assisted the Ukrainian military in identifying Russian targets by the use of data processed by AI. Many of those targets were subsequently struck with artillery or rocket fire, killing many Russian soldiers and officers. In both cases, these organizations employed data and AI to target their opponents more accurately (even if in Liverpool that adversary was a non-human virus). Together, these case studies may provide a useful insight into how the armed forces have actually harnessed AI in the recent past, and how, therefore, they might apply it in the near future of the next decade. Although they may seem mundane compared to killer robots and lethal drone swarms, the datafication of targeting, evident in Liverpool and by the Security Assistance Group-Ukraine, is likely to have profound effects on the armed forces, international relations, and great power competition in the near future. Global security scholars interested in AI may need to focus on these real-world implications of AI rather than on more fanciful visions of roving drone swarms.

Defense Policy, Data, and AI

In the last five years, the US, NATO, and some of its other members, such as the UK, have published AI strategies. They usefully highlight the focus for defense policymakers and the armed forces. Lethal autonomy and robotics are not irrelevant in these statements. The armed forces have employed robots and drones for about a hundred years, with increasing frequency. Remote systems have proliferated in the last two decades with the rise of the drone. In the last ten years, there has been a concerted effort to augment autonomy (Ministry of Defence 2023, 16,34,65). For instance, Bob Work, the former Deputy Defense Secretary in the Obama Administration, has emphasized the importance of devolving some narrow tasks to robots: "10 years from now if the first person through a breach isn't a friggin' robot, shame on us" (Gonzalez 2022, 29). Most armed forces are currently trying to introduce some form of human-machine teaming.

However, defense policymakers highlight data—not robotics or lethal autonomy—as the critical enabler in the coming decade. Above all, they claim that data will improve military intelligence; data will allow commanders to target across the battlespace to a hitherto unachievable depth, speed, and resolution. Because it can be transmitted so quickly and at such quantity, data will improve interconnections between the services so that the armed forces will be able to cooperate more closely with each other. In each case, data will allow the military to acquire targets and prosecute them more effectively. A brief survey of recent defense policy statements demonstrates that the armed forces are looking to exploit data for targeting.

The US's National Security Commission on Artificial Intelligence led by Eric Schmidt, the former CEO of Google, and Bob Work provides good evidence here. *The Final Report* begins with a sobering claim that the US is behind in the AI race. The threat here is not robotics and autonomy. Rather, the report lays out the priority of data and, therefore, intelligence from the outset:

> *AI will revolutionize the practice of intelligence*. There may be no national security function better suited for AI adoption than intelligence tradecraft and analysis. Machines will sift troves of data amassed from all sources, locate critical information, translate languages, fuse data sets from different domains, identify correlations and connections, redirect assets, and inform analysts and decision-makers (National Security Commission 2023, 23).

AI's prime function is not autonomous lethality on this account. It will be intelligence. It will allow the US forces to fuse intelligence for greater situation awareness and understanding. In particular, AI-enabled exploitation will facilitate improved targeting: "Traditional confines of the battlefield will be expanded through AI enabled micro-targeting, disinformation and cyber-operations" (National Security Commission 2023, 79). AI will allow opponents—either Russian military targets or an RNA-based virus—to be targeted precisely not only for kinetic strikes but with information, psychological, and cyber operations. The goal is ambitious: "Once the IC [Intelligence Community] has automated its processes within individual intelligence disciplines, it should fuse those individual processes into a continuous pipeline of all-source intelligence analysis processed through a federated architecture of continually learning analytical en-

gines" (National Security Commission 2023, 111). The aim is to create a single multi-domain targeting system that unites the efforts of all five domains, land, sea, air, cyber, and space. The Final Report rejects the notion that humans will become irrelevant in this process. AI will augment human targeting: "In war, many of the uses of AI will complement, rather than supplant the role of humans. It will improve the way service members perceive, understand, decide, adapt and act in the course of their missions" (National Security Commission 2023, 80).

The UK, the US's closest military and intelligence ally, is following a similar path. In September 2021, the UK government published its *National AI Strategy*. Data lay at the heart of its vision. It was investing in AI in order to exploit the potential of data. That paper is best read alongside its sister publication, the MOD's *Data Strategy for Defense*, which was published at the same time. *Data Strategy for Defense* was explicit about the challenge the UK faced: "Defence Data is an enduring strategic asset, effectively exploited and driving sustainable battlespace advantage" (Ministry of Defence 2021, 2). Admiral Sir George Zambellas, the former First Sea Lord, was quoted in the document: "The future performance in war will be dominated by the relentless and competitive exploitation of data" (Ministry of Defence 2021, 9). The former Prime Minister, Boris Johnson, described a scenario which it wanted the UK to achieve:

> We urgently need to invest in the technologies that will revolutionise warfare. In the future a soldier in hostile territory will be alerted to a distant ambush by sensors on satellites or drones, instantly transmitting a warning, using Artificial Intelligence to devise the optimal response, and offering an array of options, from summoning an air strike to ordering a swarm attack by drones, or paralysing the enemy with cyber weapons. (Ministry of Defence 2021, 4).

Data are central to these capabilities. Like the US, the British Ministry of Defence also sees organizational obstructions to the exploitation of data. At present, in the UK, "defence data operates in contractual, technical and behavioural silos" (Ministry of Defence 2021, 9). The result is there is a major challenge for data structure, curation, and exploitation. However, through major investment, *Data Strategy for Defense* articulates a plan for overcoming these obstacles so that British defense will operate with a single, fused dataset, immediately accessible to analysis by algorithms to facilitate rapid, accurate decisions. The aim, in short, as in the US, is to be able to orchestrate air, sea, and land forces with cyber and space domains. In the most recent defense policy statement, The Defense Command Paper Refresh of 2023, data—processed by AI—was central to UK strategy: "Over the last year, the Armed Forces of Ukraine have shown the game-changing impact of the most advanced intelligence, surveillance and targeting software ever deployed. We have witnessed how communications infrastructure, digitization of data, and increasing automation and autonomy are vital for data security, information operations, communications, targeting, interoperability, and lethality" (Ministry of Defence 2023, 34). The UK wants to implement this approach. The UK must learn a new way of warfare: "joint and all-domain, underpinned by data and information, both open-source and highly classified" (Ministry of Defence 2023, 8). For the UK, data, processed by AI, are primarily about intelligence. Exploiting data for targeting is central here.

NATO has always been slower to develop new strategies and policies because of its multinational basis. However, even NATO has recognized the potential of AI to transform military operations and has recently sought to embrace AI. In October 2021, it published a summary of its *Artificial Intelligence Strategy* (NATO 2021). The published document was anodyne. The strategy proposed that by forging partnerships with the academy and private sector, NATO could develop a responsible AI strategy. To do that, it proposed six principles of AI: lawfulness, responsibility and accountability, explainability and traceability, reliability, governability, and bias mitigation. The key to this strategy was the construction of a "robust, relevant, secure data infrastructure" (NATO 2021). Data are central to NATO strategy, as it was in US and UK policy. NATO wants to accelerate the adoption of AI to foster cooperation between its allies so that they remain interoperable and can share data with each other. The Strategy does not mention targeting specifically but with its heavy emphasis on regulating AI so that it is used responsibly, the document implies that targeting will be a major use of AI by NATO. It seems likely that data will also be employed to accelerate and enhance NATO targeting..

The AI policies of the US, UK, and NATO are interesting. They do not dismiss the possibility of autonomous lethality. It is very likely that remote and autonomous platforms will play a greater role in future operations—eventually. Human-machine teaming is discussed in these documents. Yet the focus is elsewhere. Above all, big data are the central point of all these policies. In each case, the US, UK, and NATO want to harness the power of big data, analyzed at speed and scale by algorithms, to improve their understanding of the battlespace and, therefore, their targeting. With the help of AI, the armed forces aspire to fuse masses of data from satellite, signal, hu-

man, and open-source intelligence, so that they can target more rapidly and with greater fidelity. AI—and the data it analyses—is not a weapon system itself, still less a platform—even an autonomous one—in these policy documents. It is an intelligence capability. As the tech entrepreneur, Peter Thiel has observed: "Though less uncanny than Frankenstein's monster, these tools are nevertheless valuable to any army—to gain an *intelligence* advantage" (Crawford 2021, 193). Data and AI are a medium for enhanced situational awareness and targeting. They are also a medium for generating insights, pattern and trend analysis, and evidencing possible new strategies and ways of tackling problems. They can inform the "where" and "how" the armed forces might wish to target something.

In this way, the armed forces may be following the commercial sector. Big Data and AI have transformed business because they have allowed executives a new insight into their organizations, their markets, and their customers. Data are knowledge. Data provide companies with a new source of intelligence about their own activities and those of their customers. Amazon, for instance, has exploited data and algorithms to outcompete adversaries through ever-greater efficiency. It is able to target customers better than its rivals. It would seem most likely that the armed forces are trying to harness the power of AI and data in a compatible way. Many scholars are concerned that AI will automate weapons; autonomous swarms will colonize the battlefield. In fact, data will transform—and is already transforming—the armed forces' understanding of the battlefield. Data represent a new source of intelligence for the armed forces, so that they might be faster and more efficient in their deployment and use of their forces. In short, AI might be not so much about autonomous drone swarms but digitizing targeting.

AI in Action

Contemporary defense policy in no way dismisses the potential of robotics and lethality. Nevertheless, it affirms that against much of the current scholarship, governments, defense ministries, and the armed forces will use AI and data for intelligence and targeting. Data and AI will augment these areas most quickly and profoundly. However, there is always a major gap between policy and practice. Consequently, it is necessary to consider not only how the armed forces intend to use AI, but how they have actually used it and, therefore, how they might employ it in the future. The British Army's response to COVID in Liverpool in 2020 and the Security Assistance Group-Ukraine in 2022 are pertinent here. These examples are instructive about how data and AI have been exploited by the armed forces.

COVID Response in Liverpool

On March 23, 2020, the UK went into its first national COVID lockdown. The lockdown was released in May, though some restrictions stayed in place throughout the summer. By the autumn, COVID cases began to rise again in the UK. Liverpool, a city in the northwest of England (with 0.5 million inhabitants and a regional population of 1.6 m), had been badly effected by COVID and lockdown. High levels of poverty increased the lethality of COVID. Half of Liverpool's economy depends on visitors, who were no longer able to go to the shops, bars, restaurants, hotels, theaters, and key venues because of COVID restrictions. So, the city was losing lives and livelihoods. On October 30, 2020, Liverpool's COVID Gold Command and central Government agreed to pilot supervised mass testing for COVID infection using lateral flow devices for people with or without symptoms of COVID, living or working in the City of Liverpool. On November 6, 2020, the Liverpool mass asymptomatic serial testing (MAST) pilot was in place, pioneering the UK's first whole town testing approach and buying valuable time for the UK Government to build up its production and distribution of COVID-19 vaccine stocks. Over the next two months, a third of the city's population were tested; infection rates fell to around a fifth, and COVID hospitalization to around a quarter (https://www.liverpool.ac.uk/research/research-themes/infectious-diseases/coronavirus-research/covid-smart-pilot/). The city's visitor economy was able to open in December 2020 when all the surrounding cities were still locked down, saving thousands of jobs..

The mass testing process had, of course, a civilian lead with the city's COVID Gold Command holding authority over the process, comprising leaders from local government, NHS, public health authorities, police and other emergency services, and academia. However, it was immediately apparent that none of these organizations had the personnel or resources to conduct mass testing alone against an invisible "enemy". Consequently, soon after Liverpool took the decision to do mass community testing, the Ministry of Defense ordered the Headquarters Standing Joint Command (HQ SJC) to support the process under the Military Assistance of Civil Authorities Act. It deployed a task force under 8 Engineer Brigade, commanded by Brigadier Joe Fossey, to the city in the same month. 8 Engineer Brigade consisted of Headquarters 8 Engineer Brigade and troops drawn from a variety

of engineer, infantry, cavalry, artillery, and logistics regiments.

In spring 2020, Liverpool had anticipated that COVID would escalate, requiring real-time intelligence to guide responses. Professor Iain Buchan, Chair in Public Health and Clinical Informatics, Associate Pro-Vice Chancellor for Innovation at The University of Liverpool, and a leading public health physician and data scientist, led the design of a data linkage and AI-automated intelligence system called Combined Intelligence for Population Health Action (CIPHA, www.cipha.nhs.uk), which was deployed in summer 2020. CIPHA was visible to the Government, whose military public health division at Porton Down, was evaluating whether new lateral flow tests for COVID might work in people without any symptoms of infection but who were carrying the virus and could pass it on. On October 30, 2020, Liverpool's COVID Gold Command, who had been following the lateral flow laboratory results from Porton Down, agreed with Government to pilot mass testing for all people, with or without symptoms of COVID, to try and suppress the spread of the virus. In five days, testing centres were set up across the city with the help of 8 Engineer Brigade. The Liverpool example is an interesting case in its own right. It was a genuine operation to which the Army applied data.

In fact, the Liverpool operation might be more evidentially significant. This was not an urban insurgency; the army was not fighting guerrillas. Yet, the challenge it posed the armed forces was not entirely different to the kinds of urban insurgencies that armed forces have often faced and which, indeed, the British Army did face in Iraq between 2003 and 2008. In Liverpool, the British Army was faced with an unidentified threat to the civilian population in an urban environment. The Army was asked to help identify concentrations of the COVID virus and to help suppress outbreaks of infection.

It is noticeable that the participants in Liverpool saw it in military terms. For instance, Professor Iain Buchan described the COVID situation in Liverpool in October 2020 as a "battlefield situation." Because of high levels of socio-economic deprivation, the threat of COVID was serious. It was deeply stressful for the professionals tasked to control the outbreaks: "it was emotionally hard-work and deeply motivating. We got little sleep" (Professor Iain Buchan, Chair of Public Health and Civic Informatics at Liverpool University, personal interview, July 12, 2022). Intensive care units were full, people were dying, and families already living in poverty were suffering job losses from lockdowns; the city and the NHS were under enormous stress. At various points in the crisis in Liverpool, Buchan himself received threats from members of the public opposed to testing and fear of the Government introducing 'COVID passports.' It was doubtful whether any of these threats were serious, but they demonstrated the conflictual nature of the public health response to COVID and the challenging information arena; a scared public and conspiracy theories exacerbated the tensions. Buchan drew an epistemological parallel between a health crisis and a military operation. In both cases, there was a lack of sufficient information. Yet, leaders had to make decisions quickly in the face of a mounting crisis; they had to act and then react to the results of their actions (Buchan, personal interview, July 12, 2022).

Although he fully recognized his mission was to support the civil authorities, Brigadier Joe Fossey, commanding 8 Engineer Brigade, a veteran of Iraq and Afghanistan, also understood the challenge in military terms:

> I recognised we knew very little about the virus. My first question was where is the bug? As we started to look for Covid-19, I was thinking in physical terms. I needed to find "it." I wanted to find the "Taliban." Or I wanted to find "Taliban-associated people." This quickly evolved into asking where I could find COVID—the infected people. As we started to gather the data, I was able to start asking clearer questions. And as we started to answer those questions, it made our response much more targeted and I was able to use the resources at my disposal much more effectively (Brigadier Joe Fossey OBE, OF-6, Commander 8 Engineer Brigade, personal interview 14 June 2022).

Although it was a very different operation to a military operation which targeted actual enemy fighters, the use of data to help understand the situation and to identify citizens at risk had some intriguing parallels. In this way, the Liverpool case study might represent a useful analogue to the kinds of operations on which the armed forces have used or are using data. Consequently, the Liverpool case may be at least indicative of sharper military applications of data.

Many scholars worry that humans are about to be superseded by machines; or that human-machine teaming is the future. Liverpool shows something quite different. The crucial enabler here was not AI, nor even perhaps the data, but the human teams that worked together to complete a mission. In Liverpool, the Brigadier and his headquarters formed a very close relationship with Professor Buchan. A career Royal Engineer, Fossey was well used to fusing geographic and intelligence data for tactical action and schooled in positioning data as a core decision factor while on exchange with the US Army Staff in

the Pentagon from 2016 to 2018. According to Brigadier Fossey, "it was a really important fusion of academic, public sector and commerce" (Fossey, personal interview June 14, 2022). Indeed, Buchan recalled their comradeship of that period emotionally: "There was a strong relationship of trust between our military colleagues and public health workers on the ground. There was a lot of respect. It felt like one team" (Buchan, personal interview, July 12, 2022). The support from 8 Engineer Brigade in this situation—and the civil-military team's solidarity—became crucial in sustaining the effort: "It was very moving. The discipline was great. . .I enjoyed working with the military. They were disciplined, respectful, kind, and dependable. I was working with people who were honourable" (Buchan, personal interview, July 12, 2022).

8 Engineer Brigade deployed into a mature institutional environment. They were subordinated to the civil powers, the Liverpool City Council, the Liverpool City Region Combined Authority, the NHS, and the Merseyside Police. Nevertheless, bringing a powerful headquarters of more than fifty officers, over 2,000 troops, and many vehicles and resources, the Brigade was able to exercise considerable agency in the support of the COVID testing. 8 Engineer Brigade partnered very closely with the health authorities in the city to draw upon their information. They were assisted here by improvements in health data management over the preceding years. In 2019, Liverpool City Region Combined Authority had supported a plan to develop the first UK Civic Data Cooperative (CDC, www.civicdatacooperative.com). The aim was to collate and fuse health data from various sources to improve the delivery of health and social care services, public health services, and health research. This initiative was accelerated due to COVID and resulted in the CIPHA system described above. The CIPHA Task Force was led by the University of Liverpool and Mersey Care NHS Foundation Trust and worked with GPs and civic leaders on data-sharing with the Civic Data Cooperative. Over 90 days in the summer of 2020, CIPHA deployed a cloud-based persistent longitudinal care record for 2.7 m residents plus a data analytic engine on top of these linked data. The system involved a series of dashboards providing near-real-time COVID intelligence. CIPHA was fully operational by October 2020 (Buchan 2022b). CIPHA proved to be vital for 8 Engineer Brigade as they developed their plan for Liverpool, although there was some initial resistance; the NHS did not want to share its data with the British Army. The MOD, in turn, had to adjust some permissions and authorities to unlock and be in a position to integrate its geospatial data and analytics software. However, because of the close relations that developed between 8 Engineer Brigade and the civil authorities in Liverpool and, in particular, between Professor Iain Buchan and Brigadier Fossey, the testing team was able to overcome these data silos. They were able to share and pool intelligence. It was crucial to the operation.

Once 8 Engineer Brigade had access to the CIPHA dashboards (with aggregate, not personally identifiable, data), and fused them with the own, locally engineered "LyverEye" geospatial tools, they could themselves develop a better appreciation of the problem they faced and begin to answer the three key questions that the Brigadier had identified: 'Where is COVID? Where are we? Where do we need to be?' (Fossey, personal interview, June 14, 2022)

The questions seemed simple. Yet, they were, in fact, crucial issues. In order to test most effectively, it was imperative to work out where the spikes in infection might be concentrated and, therefore, to locate testing centers in places that were most likely to be used by the locals. Intelligence was clearly critical here. It was imperative to determine, as accurately as possible, where the infection was spreading in the city.

The 8 Engineer Brigade consisted of two thousand soldiers. It was a major resource in comparison with their civilian partners. However, it was still a small number of personnel for the problem that they faced; Liverpool is a large city; soldiers could not work 24 hours a day. The Brigade had to try to be accurate in its deployments and efficient in its use of personnel. It could not erect testing sites everywhere. The Brigade had to be very careful about where to put their testing sites if they wanted to maximize footfall. The aim was to maximize the efficiency of the use of military forces through the collation and fusion of data. Initially, the Brigade had little choice in the testing sites. It adopted a wards and electoral divisions approach to testing in a way that those combating the 1847 typhus epidemic in Liverpool would have recognized. The initial sites were located in easy and obvious places to which access was already agreed by the council. Consequently, one officer noted: "It was a bit of a knee-jerk reaction. We put the sites in random spots, with agreed access, as speed was the priority" (Major Tom de Silva, OF-3, GEO cell, 8 Engineer Brigade, personal interview, July 4, 2022).

The Brigade realized that this approach was inadequate. The question was "how to carve up the city and allocate resources"; "It required proper military planning" (de Silva, personal interview, July 4, 2022). In developing a more refined plan for testing, the Brigade GEO [Geographic] cell was critical. The GEO cell consisted of a small group of specialists in mapping, surveying, and terrain analysis. The GEO cell was tasked with gener-

ating a better intelligence picture of the city, in collaboration with CIPHA, so that the centers of highest risk of infection might be located, and, therefore, testing sites positioned optimally. It consisted of only two, relatively low-ranking—but key—individuals, Captain (later Major) Tom de Silva, and a staff sergeant, Arran Burt. Both were in their twenties; both were seen as ideal targeteers for an Information Age problem by Brigadier Fossey. Initially, 8 Engineer Brigade's GEO cell used the city's ward boundaries to gain an understanding of the city. They then divided these into sectors on the basis of population density: so-called Modifiable Area Unit Problems. These areas were colored-coded, with purple assigned to the most densely populated areas. On the basis of this basic analysis of population structure, it was then initially a case of mathematical optimization to calculate where to locate the testing sites. The Brigade had a good idea of where testing sites were necessary, simply on the basis of the population density: "We needed so many sites to test so many people. This is where the data started to help. We used data to work out where the people were" (Fossey, OF-6, personal interview, June 14, 2022). With more data, the Brigade might have identified even better sites. Indeed, even with the data it had, "if the brigade had had another 20 hours to plan, it would have saved a lot of money" (de Silva, personal interview, July 4, 2022). The Brigade's targeting evolved as its data improved.

The Brigade eventually procured better data. The Brigade was looking for additional proxy data that might help it identify the locations of COVID concentrations. The UK Health Security Agency suggested that the Brigade might usefully look at waste water in Liverpool: "We used waste-water outlets. You can analyze water samples and it gives you hits per part per million. With that data, we could get to the hotter spots. There were loads of asymptomatic people. The waste water told you where COVID-19 people were or might be. It allowed us to target better" (Fossey, OF-6, personal interview, June 14, 2022). Consequently, staff took data provided by the UK Joint Biosecurity Centre, which recorded waste water's viral load. The idea was to detect COVID in human waste flushed down the toilet in specific neighborhoods. These data were not comprehensive. There were large parts of the city that did not record waste water: "The data did not line up. It does not cover all the wards. For instance, Everton, which was in Merseyside Water, was not covered" (de Silva, personal interview, July 4, 2022). de Silva continued: "In the wards for which there was evidence, it was possible to map the spread of infections more accurately." 'Where is the virus concentrated?' I can see it. I know where the infections are. That is useful. It confirmed assumptions" (de Silva, personal interview, July 4, 2022). In particular, this method of looking at waste water answered the Brigadier's question, "Where is the Covid?." It revealed precisely where infected people were actually going to the toilet; whereas testing recorded only an individual's postcode. 8 Engineer Brigade combined these data from waste water with the evidence from NHS records of COVID testing and infections in CIPHA (Fossey, OF-6, personal interview, June 14, 2022). The result was that the Brigade was able to identify concentrations of infection in Liverpool. The Brigade found that accessing and cross-cuing a variety of data was instructive. It underpinned the Brigade's agility in responding to a dynamically changing environment and "adversary".

There was a close connection between infection rates and poverty. Concentrations tended to occur in the poorest areas. So, the Brigade had to plot its health data with its social data. The Brigade developed a good understanding of population densities in Liverpool. These data indicated a more profound challenge which the Brigade faced in testing the population. In urban areas, very high population density has always been associated with poverty. It was the same in Liverpool in 2020. The densest neighborhoods were also the poorest. Indeed, the Brigade developed a "neglect map" on the basis of its population data (de Silva, personal interview, July 4, 2022). The neglect map was a complex product. It sought to identify the densest populations in Liverpool, correlating that data with information about people's exposure to testing sites. The Brigade tried to calculate "how many people have not been within a 15-minute walk of a testing site for the longest time" (de Silva, personal interview, July 4, 2022). The Brigade discovered that as a result of easier access and lower density, the operation had initially "favoured the worried well and the affluent"; test sites were biased to more affluent areas (de Silva, personal interview, July 4, 2022). Here, more people complied with the rules and conformed to the testing regime. Combined with the viral load data, it showed that the real problem was in the poorest and most densely populated parts of Liverpool. The largest spikes were in the poorest areas, where the general health of the population was already lower, and a larger proportion were employed in the gig economy, a labor market that relies on temporary and part-time positions filled by independent workers rather than those in full-time employment. 8 Engineer Brigade decided to prioritize testing in these areas. However, the challenge of putting testing sites in these neighbourhoods and encouraging citizens to use them was considerable. People in these areas did not generally own vehicles. There were other forms of resistance. The inhabitants of poor neighborhoods tended to mistrust the authorities. They avoided getting tested for fear of find-

ing they were positive. If they had contracted COVID, they would have to isolate and could not go to work. For families and individuals on low income, this was potentially disastrous. Consequently, the Brigade had to locate its testing sites in places that maximized the chances that locals would actually use them. They used gyms or community centers: "People look for places they regularly use within their world. Everything seemed random to us as we didn't know how the population normally behaved" (de Silva, personal interview, July 4, 2022). The data also revealed that static testing sites were of limited effect. After ten days, everyone in that area who was going to come for a test, had tested. Consequently, the Brigade used a few static hubs surrounded by mobile ones. The mobile tests centers were crucial in the areas that were not testing.

The Brigade calculated that to be effective, mobile testing sites had to be within 800 meters of people's homes. The GEO cell modeled the location of sites. The cell found that it was misleading to locate sites by lineal Euclidian distance from the population centers. In a city, people had to walk to sites via streets and so the actual distance might be much further. Consequently, the cell inserted a Manhattan system algorithm into their mapping data to work out the average walk for inhabitants for a particular neighborhood (de Silva, personal interview, July 4, 2022). The cell then also looked at the data on footfall in the sites that the Brigade had established. They could see which sites were most effective; as well as the traffic flow during the day. They could see surges at certain times such as in the morning, or oscillations between the morning and the evening. The Brigade also tried to identify places with which locals were familiar and at which they felt at ease: "Data from different sources was combined and analysed where possible or analysed separately and the intermediate results brought together in combined intelligence" (de Silva, personal interview, July 4, 2022). For example, under special data sharing powers (Control of Patient Information notice), data analysis from the Office for National Statistics (ONS) was combined. One of the CIPHA teams at the University of Liverpool, Mark Green, embedded in ONS, used the Internet User Classification of small areas to analyze the testing uptake in the Liverpool pilot. That showed it was not only financial and social deprivation but also "digital poverty" that explained a large part of the variation in testing uptake (Green 2021 et al. 2021). Taking these factors into account, Mark Green worked with fellow geodata scientists in 8 Engineer's Brigade GEO cell to produce maps of the optimal placement for testing sites. All those relations informed decision-making (de Silva, personal interview, July 4, 2022).

Once the Brigade had located the best sites for their testing centers, they then engaged in a process with which was common in Afghanistan; they conducted key leader engagement. They conducted the equivalent of "shuras to persuade leaders to get your population to a testing site" (de Silva, personal interview, 4 July 2022). Iain Buchan also played a crucial role in these information campaigns. The Brigade never used fear to encourage testing; it disincentivized the population. Rather, every Tuesday and Thursday, the Brigade drove through its key neighborhoods to inform the inhabitants of the location of mobile sites. Faith leaders and gyms provided further conduits for information.

The deployment of 8 Engineer Brigade to Liverpool in support of civil authorities was a notable success, in spite of the initial skepticism and occasional resistance of the local population. By mid-December, detection had increased by 20 percent; case rates were down by 20 percent. The number of COVID hospitalizations in the city had been reduced by 43 percent (https://www.liverpool.ac.uk/research/research-themes/infectious-diseases/coronavirus-research/covid-smart-pilot/). In addition, hospitality re-opened in December for Christmas, while other cities remained closed. This was very important for a city that was so dependent upon its hospitality sector and visitor economy (Buchan 2022a). Crucially, data shaped the Brigade's response, modified its intelligence requirements, and changed the way the force was employed. 8 Engineer Brigade's 90-day operation in Liverpool between October and December 2020 is small case study. It was a minor military operation in a critical civil situation—not a military one. However, it is potentially useful in showing how the armed forces might employ data in future operations. It is interesting that other armed forces, such as the Dutch Army used data in similar ways during the pandemic (Hoijitink 2022).

Security Assistance Group-Ukraine

It is not possible to extrapolate from the Liverpool case directly to show how the armed forces would apply data in the future on an actual military operation. That would be an evidential leap. However, it was notable that Iain Buchan and members of 8 Engineer Brigade understood the virus as an analogue for an urban insurgency. On another operation, in which the armed forces were fighting an actual urban insurgent, data might prove similarly instructive. Just as waste water and NHS COVID

reports allowed 8 Brigade to identify virus concentrations, data might facilitate the identification of the enemy quickly and efficiently. Indeed, by aligning the Liverpool case with the example of the Security-Assistance Group-Ukraine, which has been involved in support for an intense war-fighting operation, it may be possible to see that the Liverpool case is actually highly pertinent in understanding how the armed forces have used and are likely to exploit data in the near future.

The Russo-Ukraine War began on February 24, 2022, when Russian forces invaded Ukraine in an act of unprovoked aggression. It has been a brutal and bloody war, characterized by series of grueling sieges: Kyiv, Kharkiv, Mariupol, Severodonetsk, and Bakmhut. Much of the fighting has been reminiscent of the First World or Stalingrad. Over 200,000 Russian soldiers and over 100,000 Ukrainians have been killed or wounded in the fighting. There is no immediate end to the war at this point.

However, while the Russo-Ukraine War has been a violent and brutal conflict, it has also involved some very significant actions in which the most advanced technologies, including AI, have played a central role. There are a number of incidents that illustrate the application of AI to this conflict, including cyber defence and attacks by both sides, and information operations disseminated on the internet. However, notably, AI has also been employed for targeting. There are a number of examples of this application. However, one incident stands out with particular clarity.

On May 1, 2022, General Valery Gerasimov, the chief of the Russian defense staff, President Putin's closest military aide, and the most senior Russian general, was visiting a Russian army headquarters in the tiny village Zabavne, just north of Izyum. The headquarters was devastated by a Ukrainian artillery strike; probably by a US-provided HIMARS. Major General Andrei Simonov, head of the Russian Army's electronic warfare division, and about twenty staff officers were killed in the strike. Gerasimov himself was wounded. A shrapnel shard punctured his thigh. It was a minor injury and he quickly recovered.

The strike is pertinent to AI. It now seems likely that Gerasimov was struck as a result of a targeting process orchestrated by the US in support of the Ukrainian armed forces. Much of this targeting process still remains highly classified but enough evidence has now filtered into the public domain to be able to reconstruct some elements of it. Following the Russian invasion, XVIII Airborne Corps, under Lieutenant General Christopher Donohue, assumed command of the Security Assistance Group-Ukraine (SAG-U). This command, based in Wiesbaden, Germany, had coordinated the training of Ukrainian forces since 2015. However, once the war started, the role of the Assistance Group expanded dramatically. The command was no longer merely administering training for the Ukrainians. It began to provide essential command support to the Ukrainian Armed Forces. Some of this support involved planning and delivering logistics. However, the SAG-U seem to have also provided immediate operational support to Ukrainian forces, including, crucially, targeting. Precisely because the role was so demanding and complex, General Donohue deployed XVIII Airborne Corps' Forward Headquarters to the SAG-U base in Wiesbaden in Germany. Its main headquarters, providing support, remained at Fort Liberty (Bragg), North Carolina. 82nd Airborne Division, subordinated to Donohue and co-located at Fort Liberty, deployed a forward headquarters to Rseszow in Poland at the same time.

XVIII Airborne Corps had begun to develop a data-centric approach before its deployment to Weisbaden. From 2019 to 2022, the Corps had been commanded by Lieutenant General Erik Kurilla. Kurilla is widely regarded as a remarkable commander. He had had a stellar career as an officer in the Rangers, 82nd Airborne Division, and the US Special Operations Forces; he was appointed to Assistant Commander Joint Special Operations Forces Command, in 2012–14. In Mosul in 2005, he was involved in a close fight with insurgents in which he was wounded but nevertheless continued to engage enemy soldiers and command his troops, for which he was awarded the Bronze Star.

As a result of his work with US Special Operations Forces, Kurilla had been exposed to the way in which they had employed data, processed by AI, to identify enemy targets. The Special Operations Forces have often been the beneficiary of the most advanced technologies and equipment; and this was the case with big data. While deployed to Afghanistan as brigadier general in the Special Operations Forces, he had employed some innovations introduced under Project Maven. Project Maven was a Department of Defense program initiated in 2017 that sought to automate the analysis of video footage from drones to help identify enemy targets; algorithms trained to recognize signatures had helped process this mass of data. Project Maven has subsequently expanded to process other data sources. Kurilla had seen the potential that data exploitation through AI processing might bring for Task Force 58 in Afghanistan. Indeed, following his experiences there, he had told senior US officers, "I have seen what it can do. We are never going back" (Lieutenant-General, OF-8, US Air Force, personal interview, May 25, 2023). He had then sought to implement these techniques of data analysis when he com-

manded 82nd Airborne Division and XVIII Airborne Corps.

Kurilla commanded XVIII Airborne Corps until 2022, when he handed over to his successor Lieutenant-General Christopher Donohue, as the Corps deployed to Weisbaden. Donohue was well-positioned to extend Kurilla's work on big data processing. Donohue's shared a similar background to Kurilla. He had served with the Rangers and the Special Operations Forces, and in Delta Force, in particular, for much of his career. He had fought in Iraq and Afghanistan with Delta Force, eventually commanding the unit in the war against ISIS. Consequently, by the time he assumed command of XVIII Airborne Corps, like Kurilla, he had already seen data-enabled operations at work. The Special Operations Forces had originally begun to draw on data systematically, when General Stanley McChrystal commanded the Joint Special Operations Command in Baghdad in 2004. McChrystal had employed data, with the help of civilian experts, in the hunt for Abu al-Zarqawi and the fight against Al-Qaeda. Donohue had served in Iraq at this time. He had also held a job in the Department of Defense when Project Maven was running in 2017–18; there, he had reportedly learned all he could from US Marine Colonel Drew Cukor, who was administering that project (Lieutenant-General, OF-8, US Air Force, personal interview, May 25, 2023; Scharre 2023, 57). Building on Kurilla's work, Donohue had applied these methods of data mining to subsequent operations in Afghanistan as a special forces operator and then as commander of 82nd Airborne Division; he was one of the last US soldiers off the ground in Kabul in August 2021 at the end of the evacuation.

Kurilla and Donohue wanted to exploit the potential of data. To do this, they had to make some radical changes to their Headquarters. At XVIII Airborne Corps, Kurilla appointed a civilian Chief Technical Officer, Schulyer Moore, who had been a former director of science and technology for the Defense Innovation Board. Donohue created a Data Cell in the Corps, which employed civilian and military data experts. Donohue subsequently appointed Jared Summers to the Moore's role in 2022. Summers served as Chief Technical Officer throughout 2022 with the Corps for the Ukraine War. Summers had been a well-known Silicon Valley entrepreneur and executive. Between 2016 and 2021, he had acted at Exxon's Chief Technical and the Chief Data Officer. Donohue had hired him to ensure that XVIII Airborne Corps became a "data-centric" organization. He eventually left the role in January 2023, after the Corps had returned from Wiesbaden. Notably, Summers was awarded the Meritorious Civilian Service Award for his work, and on his retirement from the post, Donohue described his contribution: "Jared was exactly the right person to serve as our first Chief Technology Officer—and he has really laid the groundwork for organizations across the Department of Defense to emulate" (Visser 2023).

How did data help XVIII Airborne Corps to target Russian forces and ultimately, perhaps, to wound General Gerasimov on May 1, 2022? As already noted, in the past 20 years, there has been a data explosion. Humans are increasingly leaving digital traces of their activities in cyberspace, which, if one has enough relevant data, and one knows how to exploit it, can be plotted and analyzed. Throughout the current war, Ukraine, supported by its allies, has systematically exploited data from open-sources, decrypted mobile phone and radio messages, and satellite images. They have used the imagery posted by Ukrainian and Russian civilians and soldiers to identify Russian targets. The December 31, 2022, strike on the barracks in Mariivka, in which the Ukrainians claimed they killed 600 Russian recruits—the Russians admitted about 80—was due to Russian soldiers posting pictures on social media. US software monitoring open-source traffic seems to have identified the imagery and was able to recommend the strike. Similarly, XVIII Airborne Corps seems to have been able to collect, fuse, and analyze data from different sources, especially satellite imagery, to develop very accurate targets. On May 1, it seems possible that the Corps played a role in triangulating a number of sources to geolocate Gerasimov with complete precision.

XVIII Corps seems to have played a critical role in developing a data-enabled system of targeting for the Ukrainians, but even with a Chief Technical Officer and a Data Cell, the Corps itself could not process all the data it required alone; it did not have the expertise to curate the mass of data or to write the algorithms to be able to process them. Consequently, the Corps—and the US military more widely—relied on a partnership with a civilian defense tech company, Palantir Technologies, to develop and refine targeting software. Palantir was established in 2003 by the controversial Silicon Valley entrepreneur, Peter Thiel. It was part of his move from global libertarianism to republican nationalism. Following the 9/11 attacks, he wanted to align a traditionally skeptical, leftist Silicon Valley with US national security interests. Palantir was designed to contribute directly to US security by providing software support to the Department of Defense. After a relatively slow start, Palantir began to develop software for US forces that could analyze data and identify terrorist and insurgent networks. In 2009, Palantir began to sell their software directly to US units on operations in Iraq and Afghanistan. The Special Operations Forces were the first to buy their soft-

ware in 2010 (Barno and Bensahel 2023, 164). By 2011, more than three dozen Special Operations Forces and marine units, and several army units were using Palantir software (Barno and Bensahel 2023, 165). The Army also denied the requests of at least 17 brigades for Palantir software in the next three years (Barno and Bensahel 2023, 164). These units found the Palantir software better at disaggregating a mass of data accurately and was far easier to use that the Army's digital Distributed Common Ground System. Major General John Toolan, the US Marine commander of ISAF's Regional Command South-West in Afghanistan in 2011, noted: "Palantir reduced the time required for countless analytical functions" (Barno and Bensahel 2023, 165). By 2011, Palantir had a small foothold in the US forces. It was at this point that Kurilla and Donohue first encountered the company.

Following the assassination of Osama bin Laden in May 2011, Peter Thiel subsequently claimed that Palantir had played an essential role in identifying his location. Business Week described Palantir as "The War on Terror's secret weapon." It was not true. Palantir data analysis played at best a small role (Chafkin 2021, 153). Indeed, some intelligence officers dismissed Palantir's capability as exaggerated. Nevertheless, on the basis of its initial work between 2009 and 2011, Palantir was able to build very effective software for the campaign against ISIS between 2014 and 2018. Palantir became skilled a curating data for US forces (Chafkin 2021, 283–90). It developed a series of bespoke applications that sat on the top of specific bits of data (Chafkin 2021, 153). These applications sifted the data and automatically sent warnings of key indicators. For instance, in the fight against ISIS, the software was able to build up a picture of the ISIS leadership network and their possible locations.

Having developed a capable software, Palantir enhanced XVIII Corps' targeting process. It adapted the software and algorithms it refined during the campaign against ISIS for the war in Ukraine. In his *Washington Post* article, David Ignatius has described this process in as much detail as possible, given the classification of the targeting process:

> The "kill chain" that I saw demonstrated in Kyiv is replicated on a vast scale by Ukraine's NATO partners from a command post outside the country [e.g. XVIII Airborne Corps]. The system is built around the same software platform developed by Palantir that I saw in Kyiv, which can allow the United States and its allies to share information from diverse sources—ranging from commercial satellite imagery to the West's most secret intelligence tools. . . The system I saw in Kyiv uses a limited array of sensors and AI tools, some developed by Ukraine, partly because of classification limits. The bigger, outside system can process highly classified data securely, with cyber protections and restricted access, then feed enemy location data to Ukraine for action. (Ignatius 2022)
>
> By applying AI to analyse sensor data, NATO advisers outside Ukraine can quickly answer the essential questions of combat: Where are allied forces? Where is the enemy? Which weapons will be most effective in against enemy positions? They can then deliver precise enemy location information to Ukrainian commanders in the field. (Ignatius 2022)

Ignatius was careful and oblique in his article. It is possible to reconstruct events from his descriptions of targeting processes inside and outside Ukraine, though. Palantir seems to have helped XVIII Airborne Corps process a mass of open-source, encrypted, and satellite data in order to identify Russian headquarters in precise locations a long way back from the front-line. The result is that the Ukrainian forces have been able to kill over thirty Russian general officers, and destroy a number of command posts in the course of the war. The similarity between operational questions, which the Ukrainians and their US allies used AI to resolve, and those which Brigadier Fossey sought to answer in Liverpool, is striking.

The role of XVIII Airborne Corps as the Security Assistance Group-Ukraine in 2022 was very different from 8 Engineer Brigade's performance in Liverpool in 2020; they were respectively committed to completely different missions. However, there was a family resemblance between them. In both cases, the respective formations used mass data, processed with the help of AI to identify targets: COVID-infected individuals in Liverpool, Russian commanders and command posts in Ukraine. By looking at the digital traces left by infected individuals or Russian commanders in cyberspace, and triangulating data from alternative sources, 8 Engineer Brigade and XVIII Corps were able to target more accurately and quickly. Both organizations show how data has already been successfully processed by AI on military operations.

Conclusion

Killer drone swarms have beguiled many security studies scholars interested in AI. Many presume that the rise of the AI-enabled drone swarm presages a revolution in military affairs. This article takes an alternate view. It entirely agrees that the armed forces may be on the edge of an AI revolution. It is theoretically possible that au-

tonomous drone swarms will become important in the near future. However, up to now, AI has not been primarily used to produce robotic or autonomous weapons systems. In the last two decades, the armed forces have sought to exploit big data to generate a richer, deeper understanding of the battlespace, plotting traces left in cyberspace by their adversaries. Because there is such a vast quantity of digital data in cyberspace, the armed forces have begun to exploit the potential of AI, algorithms, and machine learning to identify patterns and signatures, to improve their awareness and so that they do not miss crucial pieces of information. In some cases, data have been analyzed by simple methods. In Liverpool, 8 Brigade did not routinely employ machine learning programs to analyze their data. In Wiesbaden, XVIII Airborne Corps seems to have used very sophisticated software and algorithms assisted by Palantir to process a diverse and complex data set, derived from digital satellite imagery, open-sources, and encrypted messaging. The Security Assistance Group-Ukraine and the Liverpool COVID cases demonstrate the armed forces using data for intelligence purposes and, specifically, for targeting. Intelligence, not lethal autonomy, has been primary. Indeed, even if autonomous lethal weapon systems, like drone swarms, do develop at some point in the future, they will rely on data, processed by AI, for their intelligence. Intelligence has been and is likely to remain the primary military function for AI. It seems very likely that, on the basis of the current evidence, the attention scholars have placed on lethal autonomy may be exaggerated.

Data offer new possibilities for military intelligence and targeting. Yet, that does not mean data or AI are invulnerable. The Israel Defense Forces have become one of the most data-enabled militaries in the world. Its strikes against Hamas targets in Gaza in 2021, Operation Guardian of the Walls, have been described as "the first digital war." The IDF employed AI and data to mount a series of strikes, supported with cyber operations. Nevertheless, on October 7, 2023, hundreds of Hamas fighters infiltrated into Israel from Gaza to attack civilian and military targets alike; in one day, they killed approximately one thousand two hundred Israelis, abducting over two hundred more. It was the worst attack that Israel has ever experienced. Israel's sophisticated constellation of sensors, and its signal, image, and human intelligence networks all failed utterly. It was a catastrophic intelligence failure, especially since Israel received a warning from Egypt days before the attack. AI did not help Israel at all. AI has a second vulnerability. AI relies entirely upon its data. Consequently, AI-enabled targeting can only be as good as its data. Biased data, which are very common, or corrupted or poisoned data compromise targeting. They will obstruct targeting or, even worse, lead to false targeting. An adversary may actively seek to manipulate data to deceive and confuse. Humans will, therefore, remain essential to the effective application of AI.

The limitations of AI are evident. Nevertheless, data and AI have primarily been used to enhance military intelligence and, above all, to target more accurately, quickly, and more deeply across the battlefield. Big data sets are likely to be exploited even more in the coming decade. This has very important implications for scholarship on AI. Scholars have substantially focused on the question of autonomous weapons and drone swarms. They have been concerned with the ethical implications of the appearance of automated weapons, controlled by AI, not by humans. Should we allow machines to kill? Many believe that autonomous weapons, which operate without human control, must be unethical.

The cases of Liverpool and the Security Assistance Group-Ukraine suggest that the current debate about ethics and lethal autonomy may be misdirected. Scholars are concerned that AI will take over, excluding humans "from the loop." In fact, the ethical question posed by AI today is different—and perhaps more pressing. In particular, in order to harness AI for intelligence and targeting, the armed forces require the immediate support from other organizations that are experts in data. Often, these experts are private tech companies like Google, Amazon Web Services, or Palantir. In Liverpool, 8 Engineer Brigade relied on the NHS, water companies, geospatial, and open-source data. In Ukraine, XVIII Corps relied on Palantir. To harness this expertise, civilian data scientists, engineers, and programers have been integrated into military headquarters, working alongside military staff, in order to curate the data, and to develop workable algorithms. Professor Iain Buchan recorded eloquently how closely he worked with 8 Engineer Brigade. His collaboration was unproblematic because it was a humanitarian mission and the right people could talk to each other in a data-informed way. Similarly, General Donohue hired Jared Summers as his Chief Technical Officer, overseeing a data cell that included civilians. In effect, civilian contractors were being integrated into the kill chain. In other cases, this private-public sector partnership may be more problematic. We are currently witnessing the rise of a Military-Tech Complex, which is potentially undermining existing norms, ethics, and laws around armed conflict. Some scholars have begun to ana-

lyze the emergence of this new political economic regime in the defense and security sectors (Evron and Bitzinger 2023; Valvida et al. 9(2); Aradau and Blanke 2015; 2022; Amicelle 2022). The rise of the Military-Tech Complex is a potentially historic development that reconfigures the armed forces as an institution. It has very serious organizational, political, legal, and ethical implications. Scholars might more usefully focus on this transformation, which is actual today, rather than the more speculative issue of whether machines might take over the battlefield.

Acknowledgments

I am grateful to Professor Iain Buchan, Brigadier Joe Fossey, Major Tom de Silva, whose assistance was essential to the Liverpool case study, two anonymous referees, and the editors of the journal for their advice on this article.

Funding

I am grateful for the support of a Leverhulme Major Research Fellowship, Urban Warfare: past, present, and future, which provided the funding for this research.

References

Altmann, Jürgen, and Frank Sauer. 2017. "Autonomous Weapon Systems and Strategic Stability" *Survival* 95 (5): 117–42.

Amicelle, Anthony. 2022. "Big Data Surveillance across Fields" *Big Data & Society* 9 (2).

Amoore, Louise. 2009"Algorithmic Warfare: Everyday Geographies of the War on Terror" *Antipode* 41 (1): 49–62

Aradau, Claudia, and Tobias Blanke. 2015. "The (Big) Data Security-Assemblage" *Big Data & Society* 2 (2).

Arkin, Ronald. 2010"The Case for Ethical Autonomy in Unmanned Systems" *Journal of Military Ethics* 9 (4): 332–41.

Ayoub, Kareem, and Kenneth Payne. 2016. "Strategy in the Age of Artificial Intelligence." *Journal of Strategic Studies* 39 (5–6): 793–819.

Baker, James. 2021. *Centaur's Dilemma*. Washington, DC: Brookings Institute Press.

Barno, David, and Nora Bensahel. 2023. *Adaptation under Fire: How Militaries Change in Wartime*. Oxford: Oxford University Press.

Berman, Eli, Jacob Felter, and Joseph Shapiro. 2018. *Small Wars, Big Data: the Information Revolution in Modern Conflict*. Princeton, NJ: Princeton University Press.

Bode, Ingvild, and Hendrik Huelss. 2018. "Autonomous Weapons and Changing Norms in International Relations" *Review of International Studies* 44 (3): 393–413.

Brose, Christian. 2020. *The Kill Chain*. New York: Hachette.

Buchan, Iain. 2022a. "Civic Informatics in Covid-19 Response: Clarifying Mass Testing and Reopening Mass Gathering" 30 April 2022.

Buchan, Iain, 2022b. "Closing the Data-Action Gap for Better Health and Care: a Civic Blueprint," 16 June 2022

Buchanan, Ben, and Andrew Imbrie. 2022. *The New Fire: War, Peace and Democracy in the Age of AI*. Cambridge, MS: MIT Press.

Chafkin, Michael. 2021. *The Contrarian: Peter Thiel and Silicon Valley's Pursuit of Power*. London: Bloomsbury.

Crawford, Kate. 2021. *Atlas of AI*. London: Yale University Press.

Evron, Yoram, and Richard Bitzinger. 2023. *The Fourth Industrial Revolution and Military-Civil Fusion*. Cambridge: Cambridge University Press.

Ford, Matthew, and Andrew Hoskins. 2022. *Radical War: Data, Attention and Control in the Twenty-first Century*. London: Hurst and Company.

Frantzmann, Seth. 2021 *Drone Wars*. New York: Nashville: Post Hill Press /Bombadier.

Garcia, Denise. 2018. "Lethal Artificial Intelligence and Change" *International Studies Review* 20 (2): 334–41.

Goldfarb, Avi, and Jon R Lindsay. 2021. "Prediction and Judgement: Why Artificial Intelligence Increases the Importance of Humans in War" *International Security* 46 (3): 7–50.

Gonzalez, Robert. 2022. *War Virtually*. Oakland, CA: University of Oakland.

Green, Mark, Finana Marta-Garcia, Barr Ben, Burnside Girvan, Cheyne Christopher, and Hughes David. 2021. "Evaluating Social and Spatial Inequality of Large Scale Rapid Lateral Flow SARs-CoV-2 Antigen Testing in Covid-19 Management: an Observational Study of Liverpook, UK (November 2020 to January 2021)" *The Lancet Regional Health—Europe* 6 July 2021, 1–11 https://www.thelancet.com/journals/lanepe/article/PIIS2666-7762(21)00084-3/fulltext

Haas, Michael-Carl, and Sophie-Charlotte Fischer. 2017"The Evolution of Targeted Killing Practices" *Contemporary Security Policy* 38 (2): 281–306.

Hambling, David. 2015. *Swarm Troopers*. Archangel Ink.

Hoijitink, Marijn. 2022. "Prototype Warfare: Innovation, Optimisation and the Experimental Way of Warfare" *European Journal of International Security* 7 (3): 322–36.

Horowitz, Michael G Allen, Elsa Kania, and Paul Scharre. 2018. *Strategic Competition in an Era of Artificial Intelligence*. Washington DC: Centre for New American Security.

Horowitz, Michael, 2019. "When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence and Stability" *Journal of Strategic Studies* 42 (6): 764–88.

Hume, David. 1985. *A Treatise on Human Nature*. Oxford: Oxford University Press.

Ignatius, David. 2022"How Algorithms Tipped the Balance in Ukraine" *Washington Post* 20 December. Accessed November 2, 2023 https://www.washingtonpost.com/opinions/2022/12/19/palantir-algorithm-data-ukraine-war/

Jensen, Benjamin, Christopher Whyte, and Scott Cuomo. 2020. "Algorithms at War: the Promise, the Peril and Limits of Artificial Intelligence" *International Studies Review September* 22 (3): 325–57.

Johnson, James. 2023. *AI and the Bomb: Nuclear Strategy in the Digital Age*. Oxford: Oxford University Press.

———. 2022. "Inadvertent Escalation" *European Journal of International Security* 7 (3): 337–59.

Kania, Elsa. 2017. "*Battlefield Singularity: Artificial Intelligence, Military Revolution and China's Future Military Power* Center for a New American Security November 28. Accessed April 16, 2024.

———. 2019. "Chinese Military Innovation in Artificial Intelligence: Hearing of the US-China Economic and Security Review Commission" Center for a New American Security 7 June. https://www.cnas.org/publications/congressional-testimony/chinese-military-innovation-in-artificial-intelligence. Accessed April 18, 2024.

Kissinger, Henry, Eric Schmidt, and Daniel Huttenlocher. 2021. *The Age of AI and Our Future*. London: John Murray.

Ministry of Defence. 2023. *Defence's Response to a More Contested and Volatile World*, CP 901 July. https://assets.publishing.service.gov.uk/media/64b55dd30ea2cb000d15e3fe/Defence_Command_Paper_2023_Defence_s_response_to_a_more_contested_and_volatile_world.pdf

———. 2021. "*Data Strategy for Defence* September," https://www.gov.uk/government/publications/data-strategy-for-defence/data-strategy-for-defence, Accessed October 11, 2023.

NATO. 2021. "Summary of the NATO Artificial Intelligence Strategy." https://www.nato.int/cps/en/natohq/official_texts_187617.htm

National Security Commission on AI. 2023. *Final Report* https://nscai.wpenginepowered.com/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf, Accessed October 11, 2023.

Payne, Kenneth. 2021. *I, Warbot*. London: Hurst.

Payne, Kenneth. 2018. "'Artificial Intelligence: a Revolution in Strategic Affairs" *Survival* 60 (5): 7–32.

Russell, Stuart. 2021. "AI and Warfare'," *Reith Lecture 2021* https://www.bbc.co.uk/programmes/m00127t9. Accessed April 18, 2024.

Scharre, Paul. 2023. *Four Battlegrounds*. London: W.W. Norton and Company.

———. 2019. *Army of None: Autonomous Weapons and the Future of War*. New York: W.W. Norton and Company.

Suleyman, Mustafa with Michael Bhaskar, 2023. *The Coming Wave*. London: The Bodley Head.

Valvida, Ana, Claudia Aradau, and Sarah Perret. 2022. "Neither Opaque nor Transparent: a Transdisciplinary Methodology to Investigate the Datafication of EU Borders" *Big Data & Society* 9 (2).

Visser, D. 2023"'XVIII Airborne Corps Honors Outgoing Chief Technology Officer" *Defence Visual Information Service* January 20 2023, https://www.dvidshub.net/news/437019/xviii-airborne-corps-honors-outgoing-chief-technology-officer. Accessed April 18, 2024.

Waltzman, Rand, Lillian Ablon, Christian Curriden, Gavin S. Hartnett, Maynard A. Holliday, Logan Ma, Brian Nichiporuk, Andrew Scobell, and Danielle C. Tarraf. 2020. *Maintaining the Competitive Advantage in Artificial Intelligence and Machine Learning*. Santa Monica, CA: Rand.

Williams, John. 2021"Locating LAWS: Lethal Autonomous Weapons, Epistemic Space and "Meaningful' human Control" *Journal of Global Security Studies* 6 (4): 1–17

Wyatt, Andrew. 2020."Charting Great Power Progress toward Lethal Autonomous Weapon System Demonstration Point" *Defence Studies* 20 (1): 1–20.

King, Anthony (2024) Digital Targeting: Artificial Intelligence, Data, and Military Intelligence. *Journal of Global Security Studies*, https://doi.org/10.1093/jogss/ogae009