#### **ORIGINAL ARTICLE**



# Blurred lines: the convergence of military and civilian uses of AI & data use and its impact on liberal democracy

Shama Ams<sup>1</sup>

Published online: 29 August 2021 © The Author(s), under exclusive licence to Springer Nature Limited 2021

## Abstract

In this paper, the sociocultural, ethical, and political impact of civilian and military uses of AI and data will be explored. In an increasingly multi-polar world, a fierce global contest has emerged between NATO, China, and Russia concerning the ethics, governance and regulation of data, artificial intelligence, autonomous decision systems (ADS), and autonomous weapons systems (AWS). The use of AI and data systems like AWS in the military has been widely criticized for use cases like an algorithm determining targets for drone strikes. These systems carry the risk of algorithmic bias due to flaws in underlying training data and its interpretation, difficulty in maintaining meaningful human control, the potential for more conflict due to fewer barriers to military engagement, and uncertainty in accountability for machine error. This represents one of the principle challenges of "remote warfare" conducted through AWS. In turn, the interchange between AI and data technologies for civilian and military purposes risks blurring the traditional legal and normative lines between these domains. To address these challenges, it is important to consider the increasing convergence of civilian and military logics in the deployment of new technologies, following on a longstanding trend of military to civilian transfers of technology, research and development (R&D), hardware, software, culture, and personnel. It is thus argued that the trends toward integrating civilian and military law enforcement domains threaten to erode important normative and legal safeguards around human rights which are central to liberal democracy. By blurring the lines between civilian and combatant in the eyes of law enforcement, one risks accelerating the retreat of liberal democracy globally, giving rise to authoritarian police states.

**Keywords** AI  $\cdot$  Autonomous weapons systems  $\cdot$  Policing  $\cdot$  Militarization of police  $\cdot$  Liberal democracy  $\cdot$  Authoritarianism  $\cdot$  Institutions

Shama Ams shama.ams@cantab.net

<sup>&</sup>lt;sup>1</sup> Department of Politics and International Studies (POLIS), Centre of Development Studies, University of Cambridge, Cambridge, UK

#### Abbreviations

| ADS    | Autonomous decision systems                               |
|--------|---|
| AI     | Artificial intelligence                                   |
| AWS    | Autonomous weapons systems                                |
| CCP    | Chinese Communist Party                                   |
| DOD    | US Department of Defense                                  |
| EU     | European Union  |
| FBI    | Federal Bureau of Investigation                           |
| ICBM   | Intercontinental Ballistic Missiles                       |
| ICE    | Immigration Customs Enforcement                           |
| ICRC   | International Committee of the Red Cross                  |
| LAWS   | Lethal Autonomous Weapons Systems                         |
| LEISI  | Law Enforcement Information Sharing Initiative            |
| NATO   | North Atlantic Treaty Organization                        |
| PPP    | Public Private Partnership                                |
| PRC    | People's Republic of China                                |
| R&D    | Research & Development                                    |
| UN     | United Nations  |
| UN CCW | United Nations Convention on Certain Conventional Weapons |
|        |   |

## Introduction

For centuries, militaries have competed to deliver the most innovative, technologically advanced tools to stay one step ahead of potential threats from their rivals. These tools have often employed certain automated functions ranging from rudimentary sensors in land mines to the invention of the Norden Bombsight and V-1 buzz bomb in World War II, "...computer systems...linked to sensors involved in the dynamic control and application of lethal force (Craig and Chen 2017, 13). At the height of the Cold War, the USSR put in place a system known as Dead Hand or "The Perimeter," which relied on an automated control mechanism for the deployment of nuclear-armed intercontinental ballistic missiles (ICBMs). Although Dead Hand is not currently in use, it can be "turned on" by the Russian Federation should it be deemed necessary (Hoffman 2018). The development of these technologies follows militaries' longstanding institutional priorities in areas such as speed, stealth, precision, efficiency and the promise of fewer human soldiers in harm's way.

Today, the competition for automated superiority has manifested not just in the realm of hardware like missiles, fighter jets, and drones, but also in software and digital tools, like AI-enabled algorithms. In the past decade, the development and sophistication of AI has grown exponentially, largely due to the increased availability of vast quantities of data and drastically improved computing power, often exceeding the projected pace set by Moore's Law.<sup>1</sup> To punctuate the gravity and

<sup>&</sup>lt;sup>1</sup> In 1965, Gordon Moore, former CEO of Intel, predicted that the number of transistors on a microchip will double every two years, enabling an exponential expansion in the micro-processing industry over time.



scale of this trend, Russian President Vladimir Putin noted in 2017 that, "...he one who becomes the leader in this sphere [AI] will be the ruler of the world" (The Associated Press 2017). In the press conference, Putin envisioned a future in which the outcome of military engagements would be settled by drones, and therefore, "...it would be strongly undesirable if someone wins a monopolist position" (The Associated Press 2017). The risks associated with AWS have been heightened by the increasing use of AI and data in remote warfare, in which state and non-state actors have turned to AI-driven hardware like drones as a less costly way to achieve military objectives than deploying human forces (Rogers and Michael 2020). The prospect of increased automation as well as physical and psychological distance in military engagements presents a related challenge around the need to provide meaningful human control or "human in the loop" when deploying potentially lethal systems (Amoroso et al. 2018).

Against this backdrop, there has been marked growth in military uses of AI on the battlefield, which has been a source of alarm for the international community (United Nations Institute for Disarmament Research 2014), most prominent among these are autonomous weapons systems (AWS). Many, including U.N. Secretary General António Guterres, have called for autonomous weapons systems, for instance, to be banned altogether (Guterres 2019). Yet, during a 2018 UN Convention on Certain Conventional Weapons (CCW), many countries, including the USA, the United Kingdom, Israel and Russia blocked a proposed ban. Among the concerns raised by these countries were the restrictions on research and development that could result from the law, which, they argue, would work against their national interests. In response to the global defenders of AWS, many UN signatories to the AWS ban, including Austria, Brazil, and China,<sup>2</sup> have suggested that the development of AWS risks setting in motion a potentially catastrophic military arms race that could lead to further instability around the world.

In the absence of international law circumscribing the use of AWS, militaries around the world have begun developing their own codes of conduct governing the deployment of AWS. These codes often reflect the strategic and tactical priorities of the militaries concerned and vary according to the laws, norms, values, and interests of the country deploying AWS. The latitude granted to militaries to govern the use of AWS by a lacuna of international consensus parallels that which has been granted to civilian law enforcement to employ autonomous decision systems in surveillance, targeting suspects, and sentencing—even in countries with robust human rights and legal protections. However, underlying this, there is an increasing convergence of civilian law enforcement with militaries concerning the use of AI and data systems. This has followed from the convergence of other overlapping elements of civilian and military law enforcement, including technology, research and development (R&D), hardware, software, culture, and personnel. The convergence of civilian and military domains, in many respects, embodies the legacy of total war, typified during the Second World War, in which countries mobilized their populations in a

<sup>&</sup>lt;sup>2</sup> China states that its call is to ban the use of fully autonomous weapons, but not their development or production. Source: "Campaign to Stop Killer Robots" 2018.

dual use of civilian manufacturing capacity for military objectives (Chickering et al. 2005). The result was a paradigmatic shift in standards of warfare which has insinuated military logics so far into areas of law enforcement traditionally considered to be civilian that the distinction between the two domains may no longer hold. The result is an erosion of liberal democracy in places like the USA that risks plunging countries into the depths of authoritarianism, particularly as it relates to policing.

To evidence this process, the paper begins by exploring the nature of AI-enabled technologies deployed in military and civilian contexts. Here, these systems are conceived in the broader context of the social, political, and ethical controversies which surround them. Next, the paper explores the historical and institutional factors shaping modern military and civilian law enforcement. The paper then examines the cases of the USA and China to understand the nature and development of civilian and military logics concerning the merging of technology, research and development (R&D), hardware, software, culture, and personnel expressed in two different forms of government, one democratic, the other authoritarian. The paper ends by reflecting on the potential trajectory of this trend in light of recent events surrounding police brutality and the militarization, typified by the murder of George Floyd on May 25, 2020.

### Methodology

Methodologically, the paper relies on a case study model examining the exchange of laws, norms, culture and personnel between military and civilian law enforcement arms through a historical institutionalist lens. The USA and China have been selected purposively as both countries have strong civil-military institutional, personnel and knowledge sharing and lead the world in AI and data technological development. In social science, according to Yin and Schramm, the case study method attempts to "...illuminate a decision or set of decisions: why they were taken, how they were implemented, and with what result" (Schramm et al. 1971; Yin 1994, 12). The case study method affords the researcher the ability to investigate "...a contemporary phenomenon within its real-life context, especially when the boundaries between phenomenon and context are not clearly evident" (Yin 1994, 13). By digging into the context of specific cases, and understanding the similarities or differences between cases, one contextualizes the nature of observation and outcome. Moreover, case studies mediate the challenge of coding more variables of interest than data points. They also rely on varied sources of evidence in a triangulating fashion, and build on prior theoretical frameworks for data collections and analysis (Yin 1994, 13).

# **Theoretical framework**

Theoretically, the paper is also underpinned by an institutional framework that assesses the impact of established modes of practice in law enforcement institutions over time. This approach can also be described as historical institutionalism.



Fioretos, Falleti, and Sheingate describe historical institutionalism in political science as, "...a research tradition that examines how temporal processes and events influence the origin and transformation of institutions that govern political and economic relations" (Fioretos et al. 2016, 2). Although the phrase, "institutions matter," is a common refrain in political science, from a historical institutionalists perspective, institutions represent an essential lens through which to conceive the evolution, growth, and character of underlying governing and economic structures "... across time and place" (Fioretos et al. 2016, 1). In particular, historical institutionalism has illuminated the ways in which states' behaviors diverge from the interests of the societies they represent, or how "...configurations of institutions in the past structure politics in the present and in ways that, often, run counter to the interests or preferences of individuals" (Fioretos et al. 2016, 7). In this sense, historical institutional ism is a useful theoretical tool to understand how law enforcement institutions develop, evolve and consolidate patterns of practice over time.

#### Civilian and military AI and data systems in context

Before diving into these issues, it is worth defining civilian and military AI and data systems. As noted above, autonomous weapons systems have existed in military contexts for decades, from the most rudimentary land mines to the Soviet Union's autonomous nuclear deterrent, Dead Hand. However, as Amanda Sharkey notes (Sharkey 2017), while there has been considerable debate among experts concerning the definitional boundaries of autonomous weapons, some common themes have emerged. For example, the US Department of Defense defines AWS as weapons that are able, "...once activated, to select and engage targets without further intervention by a human operator" (Department of Defense 2017). Meanwhile, the International Committee of the Red Cross (ICRC) defines AWS as "...weapons that can independently select and attack targets, i.e., with autonomy in the 'critical functions' of acquiring, tracking, selecting and attacking targets" (ICRC 2014). In other words, AWS represent systems which can make independent determinations in selecting targets for surveillance or attack. In this sense, many have pointed out that AWS represent systems which lack meaningful human control, which could pose significant and potentially catastrophic risks (Amoroso et al. 2018).

This challenge has raised ethical concerns about the use of AWS across different sectors of the international community from the UN, signatories to the AWS ban, as well as major technology entrepreneurs and scientists like Bill Gates, Elon Musk, and Stephen Hawking. However, the AI systems embedded in AWS represent the same computational functions as those autonomous decision systems found in self-driving cars, financial trading instruments, and medical diagnosis (European Union 2018), but with appreciably different objectives. In the context of civilian law enforcement agencies; however, the objectives and incentive structures shaping the use of ADS in surveillance, targeting suspects, and even securing convictions, mirror those of militaries. Theoretically, such a potential convergence should be buffered by the separation of these two domains by their respective regulatory and normative standards—one governed by the laws of armed conflict, the other by domestic legal provisions. In practice, however, regulatory and normative standards often converge as ADS technologies become an increasingly convenient solution to practical law enforcement challenges. Rogers, for instance, notes how autonomous drones have been used by governments like China to monitor protests in Hong Kong (Rogers 2019). Similarly, in the USA, as of August 2015, police in North Dakota have been permitted to use drones equipped with less-than-lethal weaponry such as Tasers, pepper spray and rubber bullets for crowd control. The legislation permitting the use of these armed drones passed in North Dakota less than 5 months after police in Baltimore, Maryland, was criticized for using surveillance drones in response to protests which emerged in response to the death of Freddie Gray in police custody (Bourne 2015).

Given that American police have routinely (and justifiably) faced criticism for brutality and implicit bias, particularly when dealing with minority communities, local police departments may feel pressure to seek automated solutions to issues like crowd control during protests or riots, by, for instance, programming rules of engagement into autonomous drones. Proponents of this solution could argue that the crowd control algorithm would be regularly tested and audited for bias in a way that could result in fairer and more transparent outcomes than would be possible with normal procedures involving human officers. While there may be some advantages of using ADS in policing, doing so without robust safeguards or meaningful human control (Amoroso et al. 2018) could result in dangerous and potentially catastrophic consequences.

A turn toward the use of ADS in civilian law enforcement, for example through the use of facial recognition algorithms and autonomous drones, represents an institutional practice that extends from the histories of the agencies concerned. In the USA, for instance, one of the most important tasks for local law enforcement in the eighteenth and nineteenth centuries was the protection of property, which included retrieving escaped slaves and returning them to their owners. The function of local police departments, particularly in the American South, as instruments of social control later found expression in the latter half of the nineteenth century, when local police departments refused to enforce laws like the 1867 Reconstruction Act when the Ku Klux Klan terrorized African Americans as well as white Republicans (Brandwein 2011). In these and subsequent cases in the twentieth century and beyond, the police served to bolster the existing white-supremacist power structure that identified those outside the structure as criminals, bereft of rights ostensibly afforded to them as American citizens under the US constitution (Alexander 2010). In this sense, the historical institutions of policing in the USA were primed for the criminalization of marginalized communities. These groups were often deemed to be terrorists and therefore no longer entitled to legal protections as "civilians" merely for advocating on behalf of their constitutional rights. The most infamous example of this at the federal level was when the Federal Bureau of Investigation (FBI) considered Dr. Martin Luther King Jr. to be such a threat to the existing social order that the agency spent years attempting to undermine him, branding him as a terrorist and a Communist sympathizer. An uncovered memo shows the FBI agents called Dr. King the "most dangerous and effective Negro leader in the country." (Cage 2014).

Currently, the risk of ADS in policing is compounded by the fact that where civilian and military law enforcement institutions intersect, there is a tendency for civilian law enforcement tactics and procedures in surveillance and targeting to mimic those of the military, which has been shown to result in increased civilian deaths (Lawson Jr and Edward 2018). This tendency is particularly pronounced in countries where there are weak protections for speech and privacy. It is in this context that the ethical, social and political concerns voiced by the international community about AWS become even more profound. Indeed, the ethical challenges of AWS are inextricably linked with those of civilian forms of ADS used in law enforcement.

Given their potential to impact modern and remote warfare, AWS have, understandably, garnered attention among academics, international lawyers, ethicists, and military experts. In particular, there has been a lively debate among experts opposing and in favor of AWS in combat. Many experts oppose the adoption of AWS in warfare, citing potential violations of human dignity exacerbated by an increased propensity toward military engagement (Saxon 2016). Others point out the difficulty of AWS to "...fully comply with international humanitarian law, except...in some very narrowly subscribed circumstances" (Sharkey 2016). Sharkey further notes that "...apart from problems with the principles of distinction and proportionality in determining the legitimacy of targets, AWS are, by definition, less predictable than other weapons systems." This means that "...it is unclear as yet how we could guarantee the quality of Article 36 weapon reviews for both hi-tech and low-tech nations" (Sharkey 2016). The unpredictability of AWS suggests that it would be difficult to apply a consistent regulatory standard or prevent machine error with a high degree of confidence.

At the same time, there is growing concern about the ethical implications of ADS across a variety of domains, including human resources, finance, insurance, and law enforcement. The common concern across these areas is about the nature of algorithmic bias embedded in the underlying training data which risks reinforcing problematic social perceptions or stereotypes based on statistical patterns and the models used by algorithms to interpret them. This has gained particular attention in the latter category of law enforcement, as AI-enabled algorithms have been used for determining bail, predictive policing and surveillance (Propublica 2016).

Independent of one another, AWS and ADS present thorny ethical challenges in their respective domains of military and civilian law enforcement. When these two spheres begin to merge, the combined ethical as well as practical challenges begin to mount. Even as exchanges of technology, skills and expertise between military and civilian law enforcement has remained commonplace for centuries, the dimensions through which these traditional exchanges have taken place have deepened in recent years. Nowadays, the exchanges are not merely confined to unclassified technology transfers, but extend into areas of research and development (R&D), hardware, software, personnel and culture. This depth of embeddedness between civilian and military law enforcement may intensify the ethical and practical challenges associated with AWS and ADS as these technologies are developed, shared, and deployed.

In the following section, the exchange of technology, personnel and culture between civilian and military arms of the state will be explored. These exchanges become institutional mechanisms in which norms, procedures, and practices are diffused, assimilated and eventually established. Both themes will be explored in theory and in practice in the USA and the People's Republic of China (PRC). Even as they represent competing visions of global AI and data governance, both countries have strong civil-military institutional, personnel and knowledge sharing and lead the world in AI and data technological development.

# Blurring lines: exchange of technology, hardware, software personnel and culture

Militaries have long histories of their technologies being adapted for civilian purposes (Buzman and Sen 1990). From portable two-way radio communications to nuclear technology, the internet, and satellite navigation, technological innovations on the battlefield have often propelled advances in modern civilian life. In recent years, however, the pendulum of R&D spending has swung in the direction of civilian uses, particularly within the Information and Communication Technology (ICT) sector. This section will explore instances of military to civilian technology transfer as well as emerging challenges in such transfers in reverse.

#### **Research and development**

A number of joint civil-military research and development (R&D) initiatives have emerged in the USA including the Defense Technology, Defense Laboratories and Federal laboratories (University of Southern Mississippi 2018). The research laboratories are designed to promote and share "...best practices in technology transfer and community engagement" (University of Southern Mississippi 2018). The goal of these laboratories is to create an environment in which innovations can flourish for the benefit of national defense as well as promoting local entrepreneurship and economic development through public–private partnerships (PPPs) (University of Southern Mississippi 2018). The US Department of Defense operates more than 60 laboratories and engineering centers across the USA, employing over 38,000 scientists and engineers across 22 states (Ormond and Williams 2015).

For example, in the small town of Vicksburg, Mississippi in which the US Army Core of Engineers is based, community leaders have begun connecting with engineer Research and Development Center (ERDC), the ERDC Information Technology Laboratory, ERDC Environment Laboratory, and the ERDC Coastal and Hydraulics Laboratory to explore areas of collaboration and potential PPP. The US Army has encouraged efforts to promote technology transfer and economic spinoff from its facilities, with hopes of fostering technology-led economic development (University of Southern Mississippi 2018). These civil-military partnerships have been forged with the explicit aim of allowing military technological advances to stimulate economic growth in often remote areas of the country in which military installations are based and beyond. It demonstrates a long-standing cultural norm of technology, knowledge, and funding transfer between civilian and military domains that has become deeply rooted and institutionalized.

Knowledge transfer in R&D also takes place dynamically between the civilian and military spheres as well as the public and private sectors. For example, a 2012 US National Defense Report details how Mymic, a small business specializing in modeling and simulation, created the Learning Enriched Virtual Environment product that takes soldiers into an Afghan home where they converse with its residents in a non-offensive manner while also looking out for threats. The underlying software was converted for port security applications. Using the software, truck drivers entering a port are taught how to look for hazardous material spills, terrorist activity, or other issues of concern to the Occupational Safety and Health Administration. This sort of technology transfer is indicative of what James Der Derian describes as "virtuous" warfare, in which "...military war games and computer video games blend, mock disasters and real accidents collide, producing on screen a new configuration of virtual power" (De Derian 2009). While it is standard practice for some professions to use computer simulations for training, the practice requires additional scrutiny in the context of AWS, ADS, and remote warfare which risks distorting the perceptions of the true costs of war. Mymic has sold its system to the Virginia Port Authority in Hampton Roads, Virginia. The company's Critical Incident Response Training Simulation for combat medics was adapted into a first responder simulation for fire departments and EMT. Other examples of civil-military R&D technology transfer include games for team training by the US Airforce operations center being subsequently used as a police operations center (Magnuson 2012). The ease with which military technologies are adapted for civilian purposes (and vice versa) in both public and private sectors further illustrates the embeddedness, in some areas, of civil-military R&D in the USA.

In China, there has also been a significant national push toward integrating civilian and military technologies, particularly in data and artificial intelligence. For example, the Chinese Communist Party's (CCPs) Military-Civil Fusion (MCF) strategy, aims to enable China to advance its military's technological capabilities by eliminating barriers between the country's civilian research and commercial sectors as well its military and industrial sectors. The stated goal of this integrated strategy is to establish China as a world class military by 2049. A 2020 State Department report notes that the CCP is systematically reorganizing the Chinese science and technology enterprise to ensure that new innovations simultaneously advance economic and military development. Chinese President and CCP General Secretary Xi Jinping personally oversees the strategy's implementation. He chairs the CCP's Central Military Commission and the Central Commission for Military-Civil Fusion Development. The State Department further notes that CCP is implementing this strategy through its own R&D efforts as well as by "...acquiring and diverting the world's cutting-edge technologies-including through theft-in order to achieve military dominance" (US State Department 2020). Key technologies being targeted under MCF include quantum computing, big data, semiconductors, 5G, advanced nuclear technology, aerospace technology, and AI (US Department of State 2020).

#### Hardware

However, as stated previously, the USA also maintains a strong integration between military and civilian law enforcement. Beyond incubation hubs for R&D such as the ERDC, there are significant transfers of hardware from the US military to local American police departments. In particular, through the 1033 Program, which came about through the National Defense Authorization Act for FY 1990 and 1991, local police departments are entitled to request surplus military equipment, including assault rifles, submachine guns, grenade launchers, armored personnel carriers (APCs), and AI-enabled surveillance tools. This exchange of military hardware has led to public concerns about increasingly militarized police forces in the USA (BBC 2020). By using military hardware, including weapons, intended for theaters of war, it follows that local police forces may begin to adopt military tactics. Although there are specialized units within police forces tasked with dealing with high-risk encounters, such as SWAT (special weapons and tactics) teams in the USA, these forces have traditionally been used in very specific circumstances. Indeed, as the transfer of military hardware to local police forces has become more prevalent, the number of SWAT teams issuing "no-knock" warrants has also grown. Criminologist Peter Craska estimates that the use of SWAT teams to execute search warrants has increased 15-fold from 1980 to 2000 (Craska 2007).

Whereas the US military's role is to protect the homeland from foreign threats to US citizens, interests, or government property, the remit of local police is circumscribed by state and local laws. Police forces are intended to serve communities by keeping the peace, enforcing the laws of the land, and maintaining order. In recent years, as military hardware has become widely available to and widely deployed by local police forces in the USA, the scope of their remit as well as their tactics have become blurred.

For example, in July 2020, President Donald Trump sent American troops, and unidentified military officers to quell protests in Portland Oregon, with an additional surge planned for Chicago (NBC Chicago 2020). Many experts suggest that this action, apart from being politically motivated, was unlikely to be constitutional, and may therefore be challenged in the courts. Moreover, in June 2020, a predator drone operated by US Customs and Border Patrol (CBP) was spotted overhead in Minneapolis, MN, while conducting surveillance on protests in response to the murder of George Floyd. This drone was diverted from its usual route on the Canadian border intended to provide "operational awareness" for the ongoing protests (Heilweil 2020). However, the fact that such actions were taken with scant regard for longstanding constitutional practice and cultural norms demarcating military and civilian law enforcement on American soil and with compliance from certain military units underscores how accustomed some military and civilian law enforcement officials have become to the blurring of their responsibilities. This reflects an extant erasure of the traditional guardrails of liberal democracy inasmuch as civilian law enforcement is being overlaid with military tactics for the purpose of suppressing or otherwise discouraging citizens' asserting their constitutional rights. Indeed, it also highlights the extent to which civilian and military domains have become blurred as America withdraws its colonial frontier from Iraq and Afghanistan. As the USA

withdraws from foreign theaters of war, its military infrastructure turns inward, further reinforcing military logics in civilian contexts, both ideologically and practically. In the following section, this phenomenon will be explored in relation to the personnel and cultural interchange between militaries and local police departments.

#### Personnel and culture

#### USA

In addition to the exchange of hardware and software capabilities, the USA offers a model on exchange of military and civilian personnel can take place. In particular, veterans of the US military have had a long tradition of transitioning to other roles in law enforcement at federal, state, and local levels. At the state and local level, even as veterans represent six percent of the general population in the USA, nineteen percent of police officers are veterans, according to an analysis of US Census data performed by Gregory B. Lewis and Rahul Pathak of Georgia State University for The Marshall Project (Weichselbaum and Schwartzapfel 2017). Policing is the third most common occupation for American veterans, behind truck driving and management (Marshall Project 2017).

This increasing integration between the military and civilian law enforcement has been associated with and increased use of force on the part of local police. In a 2017 investigation, The Marshall Project found that officers in Boston and in Miami with military experience were more likely to have a use-of-force complaint filed against them. In addition, one-third of the 35 fatal police shootings in Albuquerque from January 2010 to April 2014 involved police who were military veterans.

Texas researchers looked at 10 years of Dallas police and military records going back to January 2005. They examined an officer's on-duty shooting history, race, gender, age-range, veteran status, branch of military and whether the person was deployed to Iraq or Afghanistan. In total, 516 police officers, with and without US Armed Forces experience, were examined. According to the study, nearly one-third of officers involved in a shooting had a military background, whereas military veterans made up only 16 percent of officers who had no shooting incidents.

This prevalence of excessive uses of force among veterans in local police departments is not surprising given the different standards, laws, norms, and responsibilities of the military operating in combat zones overseas versus in a civilian context. Veterans returning from deployment often report struggling to transition from military to civilian operating procedures and rules of engagement. Indeed, in a study conducted by the Department of Justice, one veteran focus group participant noted the following:

"In SWAT, no one can get shot. When we enter a building or room [in the military] we yelled 'down' and shot anyone who didn't, but not in SWAT. You have to make a judgment call. By military standards, I am successful if I take less than 13 percent casualties but in SWAT, you can't take any casualties." (Department of Justice 2009).

Although there is a concerted effort to support the integration or re-integration of military personnel into federal, state, local, and tribal law enforcement, the transition can often be difficult for many service members. In addition to growing accustomed to softer standards in the rules of engagement many veterans also often struggle with disparities in their rank, mental health challenges such as PTSD, diminished autonomy, as well as heightened levels of vigilance developed through years of combat experience that may not always be suitable in civilian settings.

As these tendencies cement into established institutional norms, they contort the way civilians ought to be treated. This is felt most prominently by poor, minority or other marginalized communities which typically experience greater interface with law enforcement. The increasing militarization of police ultimately reflects deeper consequences associated with the internalization of America's military institutional norms, culture, and infrastructure as its colonial frontier in the Middle East shrinks. With fewer foreign deployments relative to the first decade of the twenty-first century, the US military's influence on civilian law enforcement has only grown, particularly during the Trump administration. This often results in American citizens being treated with suspicion for expressing their First Amendment rights. In this way, the incompatibility of veterans' military training in civilian policing has become painfully clear. When law enforcement standards begin to merge by virtue of increased military personnel, equipment, and tactics in local police forces, there is a commensurate risk that the outcome for civilian law enforcement becomes more militarized.

#### China

President Xi Xingping's centralization of executive control in China has resulted in the consolidation of the Chinese People's Armed Forces within the umbrella of the military, a move which effectively removes the distinction between civilian police and military forces. Both law enforcement arms now report directly to President Xi's Central Military Commission (Chan 2017). This consolidation of military and civilian arms of law enforcement effectively formalizes the exchange of personnel, culture, and practices between the two branches. Beyond centralizing power, the move also serves to unify norms, practices, and procedures in both military and civilian engagements. In practice, this means that for the average Chinese citizen there may be no meaningful distinction between the regulations, cultural norms, and practices of the country's military and civilian personnel. This integration also factors into the country's approach to data and AI, particularly in the national social credit system. Through AI-enabled tools of surveillance such as facial recognition algorithms and predictive modelling of behavior, Chinese citizens are actively monitored and evaluated by authorities according to activities deemed to be socially beneficial, such as volunteering for charity or donating blood, or socially negative, such as failing to sort recycled waste or violating traffic rules. In the case of Chinese civilian and military technology ecosystem, there seems to be a clear level of integration that offers a model for what a nearly complete integration of civilian and military knowledge, technology, hardware, personnel, and culture can look like.

#### Software: data sharing and AI capabilities

Unlike China, as evidenced by the case of TikTok (Jennings 2019), there has been widely publicized trepidation on the part of the private sector to cooperate with law enforcement on AI development for national defense. For example, in 2018 Google decided not to renew its contract with the Pentagon on Project Maven, which uses artificial intelligence to interpret video images and could be used to improve the targeting of drone strikes (Wakabayashi and Scott 2018). The tech giant cited ethical concerns about the program voiced by its employees, which culminated in wide-spread protests. However, where there is an emerging rift between public and private sectors regarding the end game for AI, autonomous weapons, and autonomous decision systems, AI capabilities and data sharing between the US military, other federal law enforcement agencies, as well as state and local authorities remains robust and, indeed, only continues to strengthen.

In 2018, for example, the US Department for Homeland Security implemented an AI-enabled automated service designed to "...improve the efficiency of requesting and sharing investigative information" (ICE 2019), called the Law Enforcement Information Sharing Initiative (LEISI). This program, which sits within Immigration and Customs Enforcement (ICE), and Homeland Security Investigations (HSI), aims to transform the DHS Law Enforcement Information Sharing Environment by integrating "...cultures, governance, business processes and technologies and with external partners to ensure the right information is delivered to the right person(s) at the right time in the right way" (ICE 2019). The LEISI algorithm's developmental aim is to consolidate not just information sharing but "...cultures, governance, and technologies..." to deliver information in the "...right way..." (ICE 2019). However, the "right" procedures, norms, and practices associated with military and civilian cultures, governance and technologies, as yet, will necessarily vary. Even as intelligence sharing remains an effective way to prevent crimes, the distinction in remit between local, federal, civilian and military law enforcement arms is critically important. Otherwise, there is a risk of slippage in and blurring of the procedures, norms, and cultures between civilian and military law enforcement, particularly in relation to data privacy. This trend also risks amplifying the existing ethical challenges in ADS across several domains of civilian life, including law enforcement, compounded by ethical and practical concerns associated with military uses of AI and data.

What is more is that, according to DHS, Immigration Customs Enforcement will be leading the law enforcement data sharing, including biometric data for all DHS law enforcement component agencies. This, DHS claims, is aimed at overcoming "...policy issues that may inhibit law enforcement information sharing, and develop approaches to overcome traditional barriers to information sharing" (ICE 2019). While intelligence sharing is admittedly a hugely important way to prevent crimes, the manner in which the data is being shared and accompanying AI-enabled tools deployed warrants scrutiny.

For instance, the rationale behind DHS' designating ICE as the hub for this information sharing is unclear. In recent years, ICE has garnered widespread criticism for unlawful detention of aliens, residents, and US citizens alike. These practices culminated in the Trump administration's Zero Tolerance Policy, in which children, including infants and toddlers, were separated from their parents at the US border and detained in inhumane conditions while awaiting a hearing (Propublica 2019). It has also been criticized for deploying unidentified federal agents to carry out unlawful detentions of American citizens in Portland, Oregon in response to protests against police brutality (Hannon 2020). The fact that DHS has designated ICE to coordinate this inter-agency and cross-jurisdictional information sharing program despite the whirlwind of controversy surrounding it, in many ways, telegraphs DHS's intent. Ostensibly, ICE's coordination is aimed at preventing serious crimes, maintaining convicted sex offender records, and criminal history information sharing programs. However, given ICE's track record, without a way to probe or audit the LEISI system for algorithmic bias, there is a serious and glaring risk of potential abuse.

The potential for abuse remains the most significant risk when it comes to the transfer of military personnel, codes of conduct, practices, and technology into civilian spheres. The sort of abuse that occurs as the lines between civilian and military domains blur may not be intended but nevertheless more likely to occur as institutional, legal and normative barriers become eroded. In this paper, it is argued that these barriers are central to liberal democracy, and that their slow erosion has given rise to authoritarian tendencies among civilian law enforcement agencies. As we have seen previously, increased militarization among policing in the US has resulted in increased civilian deaths (Lawson Jr and Edward 2018), a factor that was made painfully clear with the murder of George Floyd. This has been exacerbated by the internationalization of America's military institutional infrastructure as the country withdraws from the Middle East, which has at times been weaponized against marginalized communities as they demand their constitutional rights. What we have discovered in this paper is that the forces driving the militarization of police are comprised of overlapping dimensions of civil-military linkages in R&D, hardware, personnel and culture, which have consolidated around AI, data, AWS, and ADS technologies. Absent appropriate safeguards on the operational use of these technologies in both military and civilian domains, there is a growing risk of authoritarian threats to the foundations of democracy, possibly on the order of those seen when the US capital was stormed by insurrectionists (BBC 2021).

## Conclusion

The senseless murder of George Floyd following in long and horrific pattern among law enforcement of killing unarmed black people is indicative of what many have described as the militarization of American policing (Kraska 2007). The process of militarization however, has not occurred in a vacuum. There are a number of overlapping factors which produced this outcome, including increasing levels of exchanges in R&D, hardware, software, personnel and culture between military and civilian law enforcement, accelerated by policies like the American War on Drugs and the internalization of America's military institutions domestically as the country



decreases its colonial footprint abroad. These factors have also found expression in China where the merging and consolidation of civilian and military law enforcement personnel, AI and data-enabled technologies, tactics, and culture has been intentionally sought through the vehicle of an authoritarian state. To avoid what appears to be a troubling "mission creep" between civilian and military law enforcement in the new frontier of AI and data-enabled technologies, it is important for governments to be aware of the existential risks posed to liberal democracy, and make concerted efforts to protect human rights in order to prevent their abuse in these areas. Otherwise, as the existing ties between civilian law enforcement strengthen, the laws, practices, procedures and cultural norms disguising military and civilian life erode as do distinctions between civilians and combatants. Such would be a tragedy if the lines between civilians and combatants were unclear for a soldier or police officer, far worse if these lines were blurred in the eyes of an algorithm widely used and accessible to both.

# References

- Alexander, Michelle. 2010. *The New Jim Crow: Mass Incarceration in the Age of Colorblindness*. The New Press. New York, NY.
- Allen, Craig, and Taniel Chen. 2017. Artificial Intelligence and National Security. Cambridge: Belfer Center.
- Amoroso, Danielle. 2017. The Ethical and Legal Case Against Autonomy in Weapons Systems. Global Jurist.
- Amoroso, D., et al 2018. Autonomy in Weapon Systems Military Application of Artificial Intelligence as a Litmus Test for Germany's New Foreign and Security Policy. Heinrich Boll Stiftung. Großbeeren, Deutschland.
- Angwin, Julia, Jeff Larson, Surya Mattu, and Lauren Kirchner. 2016. Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks. New York: Propublica.
- BBC. 2021. Capitol riots: A visual guide to the storming of Congress.
- British Broadcasting Channel (BBC). 2020. Portland protests: Mayor demands federal officers leave city. London
- Borenstein, Jason. 2008. The Ethics of Autonomous Military Robots. Studies in Ethics, Law, and Technology 2 (1): 1036.
- Bode, Ingvild, and Hendrik Huelss. 2018. Autonomous weapons systems and changing norms in international relations. *Review of International Studies* 44 (3): 393–413.
- Bourne, Kylie. 2015. Police militarisation takes off with weaponised crowd-control drone. The Conversation, UK
- Brandwein, Pamela. 2011. Rethinking the Judicial Settlement of Reconstruction. Cambridge: Cambridge University Press.
- Buzman, Barry, and Gautaum Sen. 1990. The Impact of Military Research and Development Priorities on the Evolution of the Civil Economy in Capitalist States. Cambridge: Review of International Studies, Cambridge University Press.
- Cage, Beverly. 2014. What an Uncencored Letter to MLK reveals. New York: The New York Times.
- Celentino, Joseph. 2016. Face-to-face with facial recognition evidence: Admissibility under the postcrawford confrontation clause. *Michigan Law Review* 114 (7): 1317–1353.
- Chan, Minnie. 2017. Xi Jinping rolls out leaner top line-up for China's military machine. Hong Kong: South China Post.
- Chickering, Förster, Greiner, Chickering, Roger, Förster, Stig, Greiner, Bernd, and German Historical Institute. A World at Total War Global Conflict and the Politics of Destruction, 1937–1945.

Cambridge: German Historical Institutes, Cambridge UP, 2005. Publications of the German Historical Institute. Web.

- Coeckelbergh, Mark. 2011. From Killer Machines to Doctrines and Swarms, or Why Ethics of Military Robotics Is Not (Necessarily) About Robots. *Philosophy & Technology* 24 (3): 269–278.
- Corn, Geoffrey S. 2016. Autonomous Weapons Systems: Managing the Inevitability of 'taking the Man out of the Loop'. In Autonomous Weapons Systems: Law, Ethics, Policy, 209–42. Cambridge University Press.
- De Boisboissel, Gerard. 2017. Is It Sensible to Grant Autonomous Decision-making to Military Robots of the Future? In 2017 International Conference on Military Technologies (ICMT), 2017, 738–42.
- Der Derian, J. 2009. Virtuous War. London: Routledge.
- Dwoskin, Elizabeth. 2018. Amazon Is Selling Facial Recognition to Law Enforcement—For a Fistful of Dollars. *The Washington Post*.
- Ekelhof, Merel A.C.. 2018. Lifting the Fog of Targeting: "Autonomous Weapons" and Human Control through the Lens of Military Targeting. *Naval War College Review* 71 (3): 61–94.
- Elvira Perez, Rob Wortham, and Eugene Miakinkov. 2017. When AI Goes to War: Youth Opinion, Fictional Reality and Autonomous Weapons. ORBIT Journal 1(1) (2017)
- European Union. 2018. European Artificial Intelligence (AI) leadership, the path for an integrated vision. Brussels, Belgium.
- Facial Recognition Is Changing Law Enforcement, Commerce and the Way We Communicate with Each Other. 2018. Technology Wire (Lanham).
- Facial Recognition Tech Sees Global Uptake for Law Enforcement. 2017. *Biometric Technology Today* 2017(9): 12.
- Fioretos, Orfeo, Tulia G. Falleti, Adam Sheingate, and Sven Steinmo. 2016. Historical Institutionalism and Experimental Methods. In *The Oxford Handbook of Historical Institutionalism, The Oxford Handbook of Historical Institutionalism, Chapter 6*. Oxford University Press
- Fishel, Leslie H., and Benjamin Quarles. 1967. *The Negro American; a documentary history*. Glenview, Ill: Scott, Foresman.
- Guterres, António. 2019 Autonomous weapons that kill must be banned, insists UN chief. UN News.
- Guy Smith. 2018. Privacy Law Update: International GDPR Enforcement and Facial Recognition Software. Mondaq Business Briefing, 2018.
- Hannon, Elliot. 2020. Trump Is Now Deploying Unidentified ICE Agents to Arrest Protesters in Democratic-Run Cities. Slate Group. New York, NY.
- Heilweil, Rebecca. 2020. Members of Congress want to know more about law enforcement's surveillance of protesters. New York: Vox.
- Hernandez, Armand P. 1990. Artificial Intelligence and Expert Systems in Law Enforcement: Current and Potential Uses. *Computers, Environment and Urban Systems* 14 (4): 299–306.
- Hoffman, David E. 2018. Dead Hand: Reagan, Gorbachev and the Untold Story of the Cold War Arms Race. [S.l.]: Icon Books Ltd.
- House committee on oversight and government reform hearing on law enforcement facial recognition technology. 2017. *Political Transcript Wire* (Lanham).
- International Committee of the Red Cross (ICRC). 2014. Autonomous weapon systems technical, military, legal and humanitarian aspects. Geneva: Switzerland.
- Jain, Neha. 2016. Autonomous Weapons Systems: New Frameworks for Individual Responsibility. In Autonomous Weapons Systems: Law, Ethics, Policy, 303–24. Cambridge: Cambridge University Press.
- Jennings. 2019. What's going on with TikTok, China, and the US government? New York: Vox.
- Kalmanovitz, Pablo. 2016. Judgment, Liability and the Risks of Riskless Warfare. In Autonomous Weapons Systems: Law, Ethics, Policy, 145–63. Cambridge University Press.
- King, J., Jr., and Darwin. 2015. Behavioral Recognition: Computer Algorithms Alerting Law Enforcement to Suspicious Activity. *Pittsburgh Journal of Technology Law and Policy* 15 (1): 101–114.
- Kraska, Peter. 2007. *Militarization and Policing—Its Relevance to 21st Century Police*. Oxford: Oxford University Press.
- Lawson Jr, Edward (2018), Evidence suggests the militarization of police forces leads to more civilian deaths. London: LSE US Centre.
- Lieblich, Eliav, and Eyal Benvenisti. The Obligation to Exercise Discretion in Warfare: Why Autonomous Weapons Systems Are Unlawful. In Autonomous Weapons Systems: Law, Ethics, Policy, 245–83. Cambridge: Cambridge University Press.

- Liu, Hin-Yan. Refining Responsibility: Differentiating Two Types of Responsibility Issues Raised by Autonomous Weapons Systems. In Autonomous Weapons Systems: Law, Ethics, Policy, 325–44. Cambridge: Cambridge University Press.
- Lochner, Sabrina A. 2013. Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans. Arizona Law Review 55 (1): 201–233.
- Magnuson, Stew. 2012. *Military Training Technology Making Leap to Civilian Use*. National Defense Magazine.
- Magnuson, S. 2008. S. Magnuson. Armed robots sidelined in Iraqi fight, National Defence. www.natio naldefensemagazine.org/archive/2008/May/Pages/Armed2265.aspx.
- NBC Chicago. 2020. Trump Announces 'Surge' of Hundreds of Federal Agents Being Sent to Chicago. Chicago, IL.
- Ormond, D., and Williams, E. (2015). Defense Labs: The Innovation Engine for Sustaining Our Quality Edge. *Defense Acquisition Research Journal* (September-October), 39–43.
- Putin: Leader in Artificial Intelligence will Rule the World. 2017. New York: The Associated Press
- Rogers, James. 2019. The Dark Side of Our Drones Future. Bulletin of Atomic Scientists
- Rogers, James and Michael, Arthur. 2020. Drone Warfare: Distant Targets and Remote Killings. The Palsgrave Encyclopedia of Global Studies.
- Saxon, Dan. 2016. A Human Touch: Autonomous Weapons, DoD Directive 3000.09 and the Interpretation of 'appropriate Levels of Human Judgment over the Use of Force. In Autonomous Weapons Systems: Law, Ethics, Policy, 185–208. Cambridge University Press.
- Sartor, Giovanni, and Andrea Omicini. 2016. The Autonomy of Technological Systems and Responsibilities for Their Use. In Autonomous Weapons Systems: Law, Ethics, Policy, 39–74. Cambridge University Press.
- Schechter, Erik. 2014. In Defense of Killer Robots. New York: Wall Street Journal.
- Schramm, Wilbur, and Donald F. Roberts. 1971. *The process and effects of mass communication*. Urbana: University of Illinois Press. http://catalog.hathitrust.org/api/volumes/oclc/191159.html.
- Sharkey, Amanda. 2019. Autonomous Weapons Systems, Killer Robots and Human Dignity. *Ethics and Information Technology* 21 (2): 75–87.
- Smith, Guy. 2018. Privacy Law Update: International GDPR Enforcement and Facial Recognition Software. Mondaq Business Briefing.
- Tamburrini, Guglielmo. 2016. On Banning Autonomous Weapons Systems: From Deontological to Wide Consequentialist Reasons. In Autonomous Weapons Systems: Law, Ethics, Policy, 122–42. Cambridge: Cambridge University Press.
- United Nations Institute for Disarmament Research. 2014. Framing discussions on the weaponization of increasingly autonomous technologies. http://www.unidir.org/files/publications/pdfs/framing-discu ssions-on-the-weaponization-of-increasingly-autonomous-technologies-en-606.pdf.
- United States Immigration and Customs Enforcement (ICE). 2019. Law Enforcement Information Sharing Initiative. Washington, DC.
- United States Department of Justice. 2019. *Employing Returning Combat Veterans as Law Enforcement Officers*. Supporting the Integration or Re-Integration of Military Personnel into Federal, State, Local, and Tribal Law Enforcement.
- United States Department of State. 2020. Fact Sheet: Military-Civil Fusion and the People's Republic of China. Washington, DC.
- University of Southern Mississippi. 2018. Defense Labs Best Practices in Technology Transfer and Community Engagement. Mississippi, USA.
- US Department of Defense. 2017. Directive 3000.09: Autonomy in Weapons Systems, https://www.esd. whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf
- Wallach, Wendell. 2018. What If the Face Doesn't Fit? The World Today 74 (4): 28-34.
- Weber, Jutta, and Lucy Suchman. 2016. Human–machine Autonomies. In Autonomous Weapons Systems: Law, Ethics, Policy, 75–102. Cambridge: Cambridge University Press.
- Weichselbaum, Simone, and Beth Schwartzapfel. 2017. When Warriors Put on the Badge. New York: The Marshall Project.
- Wakabayashi, Daisuke, and Shane Scott. 2018. Google Will Not Renew Pentagon Contract that Upset Employees. New York: The New York Times.
- Williams, John. 2015. Democracy and Regulating Autonomous Weapons: Biting the Bullet while Missing the Point? Global Policy. https://nls.ldls.org.uk/welcome.html?ark:/81055/vdc\_100026574996. 0x000051.

Wyden, Booker. 2018. Markey Question 39 Federal Law-Enforcement Agencies About Facial Recognition Policies. Congressional Documents and Publications, Washington.

Yin, Robert K. 1994. Applications of case study research. Newbury Park: Sage.

Zimmer, Adrienne. 2019. Makes A Big Impact: License Plate Recognition Technology Can Do Much More than Read License Plates Thanks to Advancements in Artificial Intelligence-and Law Enforcement Reaps the Benefits. *Law Enforcement Technology* 46 (2): 20.

**Publisher's Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.