WHEN ARTIFICIAL INTELLIGENCE RENDERS LAWYERS OBSOLETE:

PROPOSING A LEGAL FRAMEWORK TO GOVERN THE DEPLOYMENT OF AI-ASSISTED UNMANNED AERIAL VEHICLES IN AMERICAN COUNTERTERRORISM

by

Gabriel Boulianne Gobeil*

SYNOPSIS

* Gabriel Boulianne Gobeil is a B.C.L./LL.B. Candidate at the Faculty of Law, McGill University. He obtained a BA from Concordia University, an MA from the University of Ottawa, and an MA from Tel Aviv University. He has worked on Parliament Hill for a Cabinet Minister and more recently as an Intelligence Analyst at a private security firm in Israel. Gabriel would like to thank Richard Janda and the anonymous reviewers for their valuable and generous comments on earlier drafts of this article.

ABSTRACT

Unmanned aerial vehicles (UAVs) are now a central tool of counterterrorism. More specifically, weaponised UAVs have proven highly valuable to the United States (US) military when conducting targeted killings in remote regions of the Middle East and Sub-Saharan Africa. Recent and ongoing progress in the field of artificial intelligence (AI) opens the door to several new military applications, particularly in the assistance of the decision-making process of UAV operators and military lawyers carrying out targeted killings. Among other applications, machine learning, via neural networks and deep learning, may assist in the identification (and perhaps even the selection) of targets. In the US, the 2001 *Authorization for Use of Military Force* and the 1949 Geneva Conventions, which govern the use of force, fail to regulate the various military applications that AI could bring about in counterterrorism operations. This article seeks to fill this gap, drawing from some of the latest regulations in the field of self-driving cars and proposing five guiding principles meant to inform a potential legal framework to govern the deployment of AI-assisted UAVs in American counterterrorism.

RÉSUMÉ

Les drones sont maintenant un outil essentiel pour la lutte contre le terrorisme. Plus spécifiquement, des drones armés se sont révélés extrêmement utiles pour l'armée américaine lors de frappes ciblées au Moyen-Orient et en Afrique subsaharienne. Des progrès récents dans le domaine de l'intelligence artificielle ouvrent la porte à plusieurs nouvelles applications : notamment, lors du processus décisionnel des opérateurs de drones, ainsi que des avocats militaires impliqués lors d'assassinats ciblés. Entre autres applications, l'apprentissage automatique, par le biais de réseaux de neurones artificiels et l'apprentissage profond, pourrait contribuer à l'identification (et peut-être même la sélection) de cibles. L'*Authorization for Use of Military Force*, promulguée en 2001 aux États-Unis, ainsi que les Conventions de Genève de 1949, qui gouvernent l'emploi de la force, ne permettent pas de règlementer les diverses applications militaires de l'intelligence artificielle lors d'opérations de contreterroriste. Cet article cherche à combler ce vide législatif en s'inspirant de certaines réglementations récentes appliquées dans le domaine des voitures autonomes. Il propose cinq principes directeurs visant à guider un éventuel cadre juridique, ayant pour but de réglementer l'utilisation de l'intelligence artificiel lors du déploiement de drones, et ce, dans la lutte contre le terrorisme des États-Unis.

KEYWORDS

Artificial intelligence; AI; Counterterrorism; Deep learning; Machine learning; Military lawyers; Neural networks; Unmanned aerial vehicles; UAVs.

I. INTRODUCTION

Over the last decade and a half, the use of unmanned aerial vehicles (UAVs) has grown rapidly in military circles, with UAVs now at the centre of many States' arsenal. While the largest part of campaigns in which UAVs have been deployed over that period fall under intelligence, surveillance, and reconnaissance (ISR) missions, those which have featured most prominently among scholarly debates have involved the use of lethal force in targeted killing missions. Among the users of this modern technology, one country—the United States (US)—stands out. Armed UAVs are now the US' weapon of predilection in remote war

theatres—such as Pakistan, Somalia, and Yemen—that are not easily accessible by land and thus warrant the projection of force from the air.[1] Of particular appeal to the US, as well as other nations resorting to UAVs, is the ability to "actualize violence from a distance".[2] In other words, one can kill without putting one's boots on the ground. A key operational advantage of this reality is that the lives of UAV operators are not endangered.[3]

At least five main factors explain why UAVs are particularly favoured when it comes to targeted strikes. First, since operators find themselves away from the conventional battlefield and need not fear for their lives, they can hover UAVs above a specific location until their intended target is where it needs to be for a successful lethal strike. More importantly, the lack of a human pilot in the cockpit enables further precision of such strikes because a UAV can be flown at a lower altitude than its manned equivalent. At lower altitudes, conventional pilots are increasingly vulnerable to ground-to-air defence systems,[4] which means that they must either fly rapidly above their target to avoid being shot down should they choose to fly low or remain at a higher altitude and further away from their target. In both cases, a strike taken by a manned plane is likely to be less precise than one by a UAV. Second, not having a pilot in the cockpit also means that UAVs can remain aloft for prolonged periods of time in comparison to manned planes that have to land when their pilots' endurance has been exhausted.[5] For instance, one of the US' most used UAVs—the Predator—can fly up to 35 hours without having to land.[6] This allows multiple operators to take back-to-back shifts and ensure that a target is not lost because a pilot needs to sleep. This also ensures a near-permanent presence in the sky. Third, contemporary laser-guided munitions, with which weaponised UAVs are equipped, now enable a missile to strike its target within a five-foot radius margin of

---

[1] Daniel L Byman, "Why Drones Work: The Case for Washington's Weapon of Choice", (17 June 2013), online: *Brookings Institution* <www.brookings.edu/articles/why-drones-work-the-case-for-washingtons weapon-of-choice/> [perma.cc/Z9YC-W7FP].

[2] James Der Derian, *Virtuous War: Mapping the Military-Industrial-Media-Entertainment-Network* (New York, NY: Routledge, 2009) at xxxi.

[3] Alcides Eduardo dos Reis Peron, "The "Surgical" Legitimacy of Drone Strikes? Issues of Sovereignty and Human Rights in the Use of Unmanned Aerial Systems in Pakistan" (2014) 7:4 Journal of Strategic Security at 81.

[4] Scott Kariya & Paula Kaufman, "New Technology Transforms Tactics in Afghanistan" (2002) 39:4 *IEEE Spectrum* at 33.

[5] Sarah Kreps & John Kaag, "The Use of Unmanned Aerial Vehicles in Contemporary Conflict: A Legal and Ethical Analysis" (2012) 44:2 Polity at 262.

[6] "Predator XP RPA", online: *General Atomics Aeronautical* <www.ga-asi.com/predator-xp> [perma.cc/FN5H-Y8BD].

error.[7] This degree of precision is greater than what would be possible with manned aircraft. This is where the expression to "put warheads on foreheads" takes its full meaning.[8] Fourth, UAVs are far less expensive than their manned equivalent.[9]

A fifth factor, which is the main focus of this article, has the potential to further increase the appeal of UAVs for targeted strikes: artificial intelligence (AI). Ongoing trends in the ways the US wages war, and more particularly its counterterrorism campaigns, strongly suggest that AI will become a central part of UAV warfare.[10] While UAV operators are already away from the conventional battlefield, the military progression toward AI-equipped UAVs further diminishes the involvement of human beings in targeted killings. This eventual delegation of decision-making power to an AI, up to an ultimate point where UAVs become fully autonomous, promises to be highly prized among militaries. However, a wide range of AI-assisted technologies are likely to be deployed well before UAVs become fully autonomous. While short of full autonomy, these technologies are worth exploring as they too raise important questions about the kind of legal framework that should be put in place to govern them. This article explores the legal foundations that may come to form the basis of a regime of governance for the projection of force via AI-assisted UAVs.

II. RESEARCH QUESTION: THE AUMF, MILITARY LAWYERS, AND A VAGUE LEGAL FRAMEWORK

On 23 May 2013, then US President Barack Obama gave a speech at the National Defense University in which he acknowledged having resorted to weaponised UAVs to conduct targeted strikes against high ranking members of al Qaeda and "associated forces". In defending the

---

[7] Robert O Work & Shawn Brimley, *20YY: Preparing for War in the Robotic Age* (Washington, DC: Center for a New American Security, 2014), online (pdf): <s3.amazonaws.com/files.cnas.org/documents/CNAS_20YY_WorkBrimley.pdf> [perma.cc/54G9-2HC5] at 15.

[8] Anna Mulrine quoted in Derek Gregory, "From a View to a Kill: Drones and Late Modern War" (2011) 28:7-8 Theory, Culture & Society 188 at 190.

[9] David Grondin, "The study of drones as object of security: Targeted killing as military strategy", in *Research Methods in Critical Security Studies: An Introduction*, edited by Mark B Salter & Can E Mutlu (New York, NY: Routledge, 2013) at 193; Kreps & Kaag, *supra* note 5.

[10] Gabriel Boulianne Gobeil, "New technology, same old strategy: Why artificial superintelligence represents the logical continuation of the US quest for war virtuousness" (2015) 16:2 Journal of Military and Strategic Studies at 99.

use of UAVs in his administration's counterterrorism campaigns, he noted that "America's actions are legal. We were attacked on 9/11. Within a week, Congress overwhelmingly authorised the use of force".[11] The legal basis Obama was referring to was the Authorization for Use of Military Force (AUMF), a joint resolution that was passed nearly unanimously by both houses of Congress on 18 September 2001. Despite a pending court challenge as to whether Obama violated the 1973 War Powers Resolution when he later resorted to the AUMF to sanction the use of force in Iraq and Syria to fight the Islamic State,[12] the US continues to rely on this decades-old statute when justifying its counterterrorism operations involving UAV-borne targeted killings.[13] Daniel Klaidman notes how important lawyers were in interpreting the text of the AUMF to determine who could ultimately be killed under its authority.[14]

Yet, simply invoking the AUMF does not automatically sanction just any UAV strike. To be sure, UAV operators must follow all applicable laws of war. According to Pratap Chatterjee, military lawyers who assist UAV operators receive a specific training on the Geneva Conventions in which the laws of war are laid out.[15] Hence, before firing a missile, the US relies on these military lawyers to ascertain the legality of each of its targeted strikes.[16]

---

[11] Barack Obama, "Remarks by the President at the National Defense University" (23 May 2013), online: *White House* <obamawhitehouse.archives.gov/the-press-office/2013/05/23/remarks-president-national-defense-university> [perma.cc/J6WY-LTKK].

[12] Sabrina McCubbin, "Smith v. Trump: AUMF Challenge Pretrial Motion Summaries" (23 October 2017), online: *Lawfare* <www.lawfareblog.com/smith-v-trump-aumf-challenge-pretrial-motion-summaries> [perma.cc/6NBZ-C9X2]; Andrew Rudalevige, "The Contemporary Presidency: The Obama Administrative Presidency: Some Late-Term Patterns" (2016) 46:4 Presidential Studies Quarterly 868 at 885.

[13] John Brennan, "Text of John Brennan's Speech on Drone Strikes Today at the Wilson Center" (30 April 2012), online: *Lawfare* <www.lawfareblog.com/text-john-brennans-speech-drone-strikes-today-wilson-center> [perma.cc/P794-Y4WT]; John Kaag & Sarah Kreps, *Drone Warfare* (Malden, MA: Polity, 2014) at 67; Harold Koh, "The Obama Administration and International Law" (25 March 2010), online: *US Department of State* <2009-2017.state.gov/s/l/releases/remarks/139119.htm> [perma.cc/Q3PL-4TLQ]; Shoon Kathleen Murray, *The Terror Authorization: The History and Politics of the 2001 AUMF* (New York, NY: Palgrave Macmillan, 2014) at 68; Shoon Kathleen Murray, "The Contemporary Presidency: Stretching the 2001 AUMF: A History of Two Presidencies" (2015) 45:1 Presidential Studies Quarterly at 193; Rudalevige, *supra* note 12 at 883; Benjamin Wittes, "Not Asking the Girl to Dance" (10 September 2014), online: *Lawfare* <www.lawfareblog.com/not-asking-girl-dance> [perma.cc/TG3N-XGYJ].

[14] Daniel Klaidman, *Kill or Capture: The War on Terror and the Soul of the Obama Presidency* (New York, NY: Houghton Mifflin Harcourt, 2012) at 205-206.

[15] Pratap Chatterjee, "How lawyers sign off on drone attacks", *The Guardian* (15 June 2011), online: *The Guardian* <www.theguardian.com/commentisfree/cifamerica/2011/jun/15/drone-attacks-obama-administration> [perma.cc/S5GW-2SAM].

[16] Spencer Ackerman, "CIA Lawyer: How I Issued Drone 'Death Warrants'" (14 February

While this step is crucial for the US to ensure that its use of force is done in compliance with national and international legal obligations governing the use of armed forces, the presence of a lawyer in the process can be cumbersome due to tactical considerations. As Thomas K. Adams notes, "[k]nowledge is seen as the key to "battlefield dominance," and speed is seen as the key to exploiting that knowledge".[17] Thus, having to consult with a lawyer as to whether any given strike is legal may take several minutes. In some cases, this time-frame can be sufficient for a target to escape or for a civilian to enter the blast radius (as exemplified in *Eye in the Sky*) and warrant that the strike be called off, which can frustrate the military objective of the operation.[18] AI presents a potential solution to this obstacle. Delegating the legal decision-making to an AI-assisted UAV would remove the need for a real lawyer (or at the very least reduce the lawyer's involvement) and would offer a more expeditious process than any human lawyer could achieve. In short, replacing lawyers by AI (or using AI to assist in various aspects of their work) would fulfil a dual-purpose, achieving a balance between battlefield efficiency while ensuring that each targeted strike stands on firm legal foundations.

Delegating a license to kill to an AI-assisted UAV that would grant the weapons system more autonomy presents important military advantages.[19] However, Department of Defense (DoD) Directive 3000.09 restrains the deployment of fully autonomous robots.[20] Section 4(a) states the DoD's general stance on autonomous weapons systems, which warrants "appropriate levels of human judgment over the use of force".[21] Had Directive 3000.09 not expired in 2017, its restrictions would continue to apply to today's most sophisticated UAVs. Yet, military policy documents that preceded Directive 3000.09 also called for weapons systems that would leave at least some level of control to a human

---

2011), online: *Wired* <www.wired.com/2011/02/behind-the-drones-lots-of-bureaucracy/> [perma.cc/3DRQ-NP37]; Chatterjee, *supra* note 15. An accurate and useful depiction of this process is presented in the movie *Eye in the Sky*, Directed by Gavin Hood (Toronto, ON: Entertainment One, 2015).

[17] Thomas K. Adams, "Future Warfare and the Decline of Human Decisionmaking" (2001) 41:4 Parameters 1 at 7.

[18] *Eye in the Sky, supra* note 16.

[19] Noel Sharkey, "Cassandra or False Prophet of Doom: AI Robots and War" (2008) 23:4 IEEE Intelligent Systems 14 at 16.

[20] Heather M. Roff & Peter W. Singer, "The Next President Will Decide the Fate of Killer Robots—and the Future of War", *Wired* (6 August 2016), online: *Wired* <www.wired.com/2016/09/next-president-will-decide-fate-killer-robots-future-war/> [perma.cc/684L-QK82].

[21] *Department of Defense Directive 3000.09* (21 November 2012).

operator.[22] This suggests that the requirement to keep a human in the loop might outlast Directive 3000.09. Thus, even though the current status of the rules governing fully autonomous UAVs is unclear, *semi*-autonomous systems represent a more probable progression of the use of those technologies on the battlefield.[23] According to Peter W. Singer, "[t]he most likely outcome in the near future is for robots to take on the semblance of "war fighter associates"".[24] That is, AI would assist humans rather than replace them completely.

A. RESEARCH QUESTION

The absence of thorough laws of war regulating AI's various military applications combined with the rapid pace of technological progress in AI and machine learning calls upon jurists and policymakers to draft clear and transparent guidelines governing their development and deployment. The main objective of this article is to explore some of the most probable military applications of AI in assisting targeted killings conducted with UAVs so as to devise preliminary guidelines on how these military technologies should be deployed. In so doing, this article asks the following research question: what should the laws of war pertaining to AI-equipped UAVs in operations involving the use of lethal force be? In other words, under what legal framework should AI-assisted UAVs be allowed to operate?

B. ROADMAP OF THE ARTICLE

This article proceeds as follows. Section III briefly looks at what UAVs are as well as the roles they have played in military campaigns and more specifically in counterterrorism operations.[25] This portion also

---

[22] Dan Saxon, "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*, edited by Nehal Bhuta, et al. (Cambridge, UK: Cambridge University Press, 2016) at 193-194.

[23] Despite increasing levels of autonomy, Work and Brimley argue that human operators are likely to remain essential decision-making actors in complex war theatres—at least in the foreseeable future. See Work and Brimley, *supra* note 7 at 24.

[24] Peter W Singer, "War of the Machines" (2010) 303:1 Scientific American 56 at 60.

[25] This article only discusses UAV strikes that are conducted by the DoD, thus leaving aside the more secretive practice of targeted killing carried out by the Central Intelligence Agency (CIA). This is because CIA-led strikes are under a thick veil of secrecy and little to no information is publicly available (see Kaag and Kreps, *supra* note 13 at 26; Geert-Jan Alexander Knoops, "Legal, Political and Ethical Dimensions of Drone Warfare under International Law: A Preliminary Survey" (2012) 12:4 Intl Crim L Rev 697 at 712; Yolandi Meyer, "The legality of targeted-killing operations in Pakistan" (2014) 47:2 Comp & Intl LJS Afr 225 at 244). Moreover, unlike those of the CIA, DoD UAVs operate under a more explicit

presents the strategic context within which UAVs have garnered prevalence—a context which explains some of the incentives of using AI to increase the abilities of UAVs and consequently reduce the involvement of human beings in the decision-making process. Section IV investigates the legal foundation for the use of UAVs in targeted killings, looking at the AUMF in more depth as well as the Geneva Conventions and their Additional Protocols applicable to drone warfare. This section of the article also explores the role of military lawyers whose involvement is key before a strike takes place. Section V looks at AI (and machine learning) and some of its probable military applications when combined with UAV technology to assist operators and military lawyers in carrying out targeted killing missions. Section VI represents the main contribution of this article, presenting five guiding principles aimed at informing an eventual legal framework that could govern the use of AI-assisted UAVs.[26] To sketch out this framework, the article adopts a comparative approach, firstly looking at the regulation scheme of self-driving cars enacted in California and secondly analysing the SELF DRIVE Act, federal legislation pertaining to self-driving cars that is currently under review by the US Senate. Given that the technologies with which self-driving cars are engineered are similar to those employed in UAVs, the aforementioned schemes will be used to inform this article's proposed legal framework for AI-assisted UAVs.

---

and transparent legal framework. Hence, DoD-led strikes offer a fitting starting point to discuss what a legal framework governing the use of AI-assisted UAV strikes should look like.

[26] Although the article focuses on US uses of UAVs, these principles may also guide the drafting of AI-assisted UAV regulation by other actors—State and non-State—who employ military UAVs. Admittedly, the US is unlikely to bind itself to a legal framework that may be more constraining on it than the one it currently has (i.e. the AUMF) if other UAV users do not follow suit. The implementation of these principles by the US therefore depends, at least in part, on whether other actors adopt them as well.

III. UNMANNED AERIAL VEHICLES (UAVs)

A. WHAT ARE UAVs? AND WHY ARE THEY SO VALUABLE IN AMERICAN COUNTERTERRORISM CAMPAIGNS?

UAVs, popularly referred to as drones, are aircraft whose operator is not on-board.[27] Yet, qualifying UAVs as "unmanned" can be somewhat misleading since a human crew is still essential to operate them. In fact, as many as 110 individuals can be employed to operate a single UAV like those deployed in US military campaigns.[28]

The appellation Remotely Piloted Aircraft (RPA) is thus helpful as it indicates that the pilot—or more accurately, the operator—is controlling the aircraft *from a distance*. As former UAV operator Brett Velicovich explains, operators find themselves in a concealed bunker, facing several screens on which they monitor what is in the UAV's field of view and control its every move.[29] The Predator and Reaper, which are the two main UAVs deployed by the US in targeted killing operations, are also equipped with up to two and four air-to-ground (AGM)-114 Hellfire missiles respectively.[30] Being more sophisticated, the Reaper's armament can consist of a combination of other laser-guided missiles.[31] In either case, this makes for a deadly payload that is key in military and counterterrorism operations.

What makes UAVs so appealing in military circles is precisely the absence of a human being in the aircraft and the fact that the humans operating them are sometimes thousands of kilometres away from the actual aircraft. In other words, they are out of harm's way. This

---

[27] "Optionally piloted aircraft" (OPA) represents an exception. OPAs are a type of UAV that can either be controlled by having a pilot physically inside the cockpit or an operator who remains on the ground. For an example, see "Centaur", online: *Aurora* <www.aurora.aero/centaur/> [perma.cc/KZ9S-P9AA].

[28] Yuval Noah Harari, *21 Lessons for the 21st Century* (New York, NY: Penguin Random House, 2018) at 29.

[29] Brett Velicovich, "What it's like to Control a Predator Drone" (2 July 2017), online: *Wired* <www.wired.com/story/control-predator-drone-brett-velicovich/> [perma.cc/ZMF4-7DM2].

[30] "MQ-1B Predator", online: *US Air Force* <www.af.mil/About-Us/Fact-Sheets/Display/Article/104469/mq-1b-predator/> [perma.cc/4LAU-7P8J]; "MQ-9 Reaper", online: *US Air Force* <www.af.mil/About-Us/Fact-Sheets/Display/Article/104470/mq-9-reaper/> [perma.cc/M2A2-TE5Z].

[31] "MQ-9 Reaper", *supra* note 30.

characteristic offers the ability to kill *without risking one's own life*.[32] This main feature has rendered UAVs a highly coveted tool in counterterrorism operations taking place in war theatres that would be extremely dangerous were human soldiers to be deployed. According to proponents of UAV strikes,[33] the projection of lethal force onto an enemy with the knowledge that this enemy simply cannot retaliate directly is what makes UAVs so valuable. Grégoire Chamayou refers to this practice as "*chasse à l'homme*" or "manhunt warfare" whereby the hunter who deploys its UAV is no longer partaking in a Clausewitzian duel in which each side seeks to kill the other; rather, the hunter is facing a helpless enemy, regarded as a "prey", whose only two options to win are fleeing or hiding—just like an animal being hunted.[34]

Chamayou's manhunt warfare is made possible as a result of a state-of-the-art system that is composed of three main parts, namely a command and control centre, a satellite, and an aircraft.[35] The operator's bunker that Velicovich referred to is part of the command and control centre and is the only one of the aforementioned three components with a human presence—except for OPAs.[36] This means that the operator and the rest of the crew must rely on a wide range of technological devices with which UAVs are equipped. These include high-resolution cameras, a Global Positioning System, satellite communication to and from the UAV as well as several other types of sensors. For instance, the Defense Advanced Research Projects Agency (DARPA), the DoD's research and development branch where the most futuristic and top-secret military projects originate,

---

[32] In the midst of the 2011 intervention in Libya, which was authorised by United Nations Security Council Resolution 1973, the Obama administration relied on the projection of force from a distance to argue that the US' actions did not amount to hostilities and that the President was therefore not constrained by the 1973 War Powers Resolution (Fisher, 2012) at 181-2. This example shows how UAVs can be used to evade certain legal structures—pointing to yet another advantage of this technology.

[33] See Brennan, *supra* note 13; Byman, *supra* note 1; Obama, *supra* note 11; Barack Obama, "Statement by the President on ISIL" (10 September 2014), online: *White House* <obamawhitehouse.archives.gov/the-press-office/2014/09/10/statement-president-isil-1> [perma.cc/3P4G-9U6E].

[34] Grégoire Chamayou, *Théorie du drone* (Paris, FR: La Fabrique éditions, 2013) at 51-53.

[35] Gabriel Boulianne Gobeil & Liran Antebi, "The Vulnerable Architecture of Unmanned Aerial Systems: Mapping and Mitigating Cyberattack Threats" (2017) 1:3 Cyber, Intelligence, and Security at 111-112.

[36] Velicovich, *supra* note 29. A fourth component of the system, a launch-and-recovery station from which UAVs can take off and are refueled, repaired, or stored (Boulianne Gobeil & Antebi, *supra* note 35 at 112), represents another site where human operators come into play. This station is not addressed in this article because while it offers important operational support to UAVs, this fourth component plays no role in the decision-making process preceding a targeted strike. Thus, the launch-and-recovery station is not a likely venue for AI technologies to assist human operators and military lawyers.

designed the Gorgon Stare and the ARGUS IS. These two sensors are aimed at enhancing the visual capabilities of UAVs, equipping the aircraft on which they are mounted with 12 and 92 high-resolution cameras respectively.[37] While these sensors expand the visual scope of UAVs, thus offering the operator a more nuanced overview of the battlefield than would be possible with a single camera, they also create a massive amount of video feed that is becoming increasingly too large for humans to process effectively without the assistance of AI.[38]

B. HOW ARE UAVs DEPLOYED IN MILITARY CAMPAIGNS?

The ability to see without being seen and to kill without being killed, which is personified by UAVs, has led them to be tools central to the US' counterterrorism campaigns—especially those operations warranting a high level of secrecy. David Grondin argues that UAVs and the technological systems that support them have grown to become predominant components of what he calls "the *new* American ways of war [emphasis added]".[39] These new ways of war are characterised by the *targeted* projection of violence, which represents a shift from the more conventional approach of sending an army on the enemy's battlefield. Rather than sending "boots on the ground", the US is now able to create circumscribed pockets of violence. That is, it actualises violence only where the enemy—who is often a terrorist or insurgent—is located. As Grondin notes, UAVs have proven flexible, allowing the US to deploy its arsenal in unconventional battlefields, including in urban zones.[40]

Moreover, UAVs enable airpower in a far more focused way than would be possible if the US used a strategy of carpet bombing like that commonly employed during World War II and the Vietnam War. As a result of this tactical precision, advocates of this technology pride themselves on the modest collateral damage that UAVs bring about in comparison to their manned equivalents. As former Director of the CIA John Brennan put it,

---

[37] Matt Frankel, "The ABCs of HVT: Key Lessons from High Value Targeting Campaigns Against Insurgents and Terrorists" (2011) 34:1 Studies in Conflict & Terrorism 17 at 28; Gregory, *supra* note 8 at 193; Noah Shachtman, "Air Force to Unleash 'Gorgon Stare' on Squirting Insurgents" (19 February 2009), online: *Wired* <www.wired.com/2009/02/gorgon-stare/> [perma.cc/UUS9-6LZR].

[38] Boulianne Gobeil, *supra* note 10 at 112.

[39] Grondin, *supra* note 9 at 193.

[40] *Ibid.*

> compared against other options, a pilot operating this aircraft remotely—with the benefit of technology and with the safety of distance—might actually have a clearer picture of the target and its surroundings, including the presence of innocent civilians. It's this surgical precision—the ability, with laser-like focus, to eliminate the cancerous tumor called an al-Qa'ida terrorist while limiting damage to the tissue around it—that makes this counterterrorism tool so essential.[41]

This seemingly humanitarian, yet oxymoronic quality of UAVs—the ability to save lives while taking lives—has prompted the US to deploy its fleet of UAVs in some of the remotest military terrains such as in Pakistan's Federally Administered Tribal Areas (FATA) that border Afghanistan, a mountainous and treacherous region of the Middle Eastern chessboard that makes most ground military operations impracticable. This region harbours members of Al-Qaeda and other non-State actors which the US considers as a threat to its national security.[42] Ian Graham Ronald Shaw and Majed Akhter note that while the US conducted 45 UAV strikes in FATA under George W. Bush's presidency, Obama sanctioned a total of 118 in 2010 alone.[43] These numbers point to the US' increasing dependence on UAVs in removed locations.[44]

Beyond Pakistan, Matt Frankel records that the US resorted to a campaign of "high-value targeting" in Afghanistan, Iraq, Somalia, and Yemen.[45] While the exact numbers of strikes carried out by the US in these States vary depending on the source, they all indicate a sharp increase in the use of UAVs under the Obama administration in comparison to his predecessor.[46] Whereas Obama's focus was on counterterrorism, the emphasis under President Donald J. Trump's administration seems to be on counterinsurgency.[47] Notwithstanding this strategic shift, under the

---

[41] Brennan, *supra* note 13.

[42] *Ibid.*

[43] Ian Graham Ronald Shaw & Majed Akhter, "The Unbearable Humanness of Drone Warfare in FATA, Pakistan" (2012) 44:4 Antipode at 1491.

[44] See Jeffrey Crouch, Mark J Rozell & Mitchel A Sollenberger, "The Law: The Unitary Executive Theory and President Donald J. Trump" (2017) 47:3 Presidential Studies Quarterly at 568; Kaag & Kreps, *supra* note 13 at 28; Kreps & Kaag, *supra* note 5 at 263; Peron, *supra* note 3 at 85.

[45] Frankel, *supra* note 37 at 17-18.

[46] See Geert-Jan Alexander Knoops, "Drones at Trial. State and Individual (Criminal) Liabilities for Drone Attacks" (2014) 14:1 International Criminal Law Review 42 at 43.

[47] Dan De Luce & Seán D Naylor, "The Drones are Back" (26 March 2018), online: *Foreign Policy* <foreignpolicy.com/2018/03/26/the-drones-are-back/> [perma.cc/F4QF-RS5C]. Unlike terrorists who resort to indiscriminate violence against civilians to achieve political

Trump presidency, UAV strikes have intensified in Somalia and Yemen although the US' targeted killing campaign has been more modest in Pakistan. [48] These data point to UAV's ongoing relevance in US counterterrorism.

As part of its broader counterterrorism campaign, the US employs UAVs to conduct two types of strikes: "personality" and "signature" strikes.[49] Where personality strikes denote the killing of specific targets, signature strikes are aimed at individuals whose identity is not known to the US.[50] That is, personality strikes are performed against individuals whose names are on the US' kill list, as was the case of Anwar al-Awlaki who was killed in Yemen in 2011.[51] In contrast, signature strikes are carried out against people whose *behaviour* are associated with that of terrorists—hence their signature label.[52] Signature strikes are therefore preceded by lengthy ISR missions aimed at identifying certain patterns in an individual's daily activities and ultimately determine whether that person poses a threat to the US. ISR missions are also necessary to locate the targets of personality strikes. With respect to manhunt warfare, Chamayou explains that "*La première tâche n'est plus d'immobiliser l'ennemi, mais de l'identifier et de le localiser. Cela implique tout un travail de détection*".[53] The investigative stage that precedes UAV strikes is precisely where technologies like the Gorgon Stare, the ARGUS IS, and other AI-assisted systems become essential. The UAV and its myriad sensors then become the operator's eye in the sky, allowing him to pinpoint terrorists, insurgents, or other targets in otherwise difficult-to-access terrains.

Having fired their weapon from the safety of their bunker, UAV operators must monitor the blast site to ensure that their target was killed. Former UAV operator Brandon Bryant describes the experience of UAV operators who witness the aftermath of a strike and the slow death of their target as follows: "it's really more intimate for us because we see

---

objectives, insurgents focus on the State itself. That is, insurgents oppose State authority but they do not usually attack civilians directly (even though civilians can sometimes be caught in the crossfire). Thus, counterterrorism and counterinsurgency operations focus on two different types of target. Despite this difference, the deployment of UAVs under Obama's presidency resembles that of his successor.

[48] *Ibid.*

[49] Medea Benjamin, *Drone Warfare: Killing by Remote Control* (New York, NY: Verso, 2013) at 131.

[50] *Ibid.*

[51] Murray, "The Contemporary Presidency", *supra* note 13 at 191.

[52] Meyer, *supra* note 25 at 243.

[53] Translation: "The first task is no longer to immobili[s]e the enemy, but to identify and locate it. This involves a process of detection." Chamayou, *supra* note 34 at 53.

everything."[54] The nature of UAV operators' work thus exposes them to disturbing war scenes. This is one factor explaining the high rate of post-traumatic stress disorder and mental health problems with which operators are affected.[55] As Jean Lin Otto puts it, "They [UAV operators] witness the carnage. Manned aircraft pilots don't do that. They get out of there as soon as possible".[56] As I previously argued, the same desire of keeping soldiers out of physical harm's way is likely to prompt the US to increasingly rely on the assistance of AI in its operations involving UAVs so as to reduce operators' role and ultimately remove humans from "*psychological* harm's way".[57] Given this context, AI-assisted technologies are likely to take on increasing functions, tasks that are discussed in more length in Section V below. The next section sets the legal foundation on which US' counterterrorism operations involving UAVs rely.

IV. ON THE LEGAL FOUNDATION FOR THE USE OF UAVs IN TARGETED KILLING OPERATIONS

A. AUTHORIZATION FOR USE OF MILITARY FORCE (AUMF)

As was discussed in the previous section, the US has employed UAVs to carry out targeted killings. Whether these strikes are aimed at known or unknown individuals, both personality and signature strikes involve the killing of specific targets who were systematically identified through ISR missions. However politically contentious it may be, the practice of targeted killing remains lawful, under particular circumstances. According to Cheri Kramer, US domestic law, under the 1989 Parks Memo,[58] permits targeted killings when they take place in the

---

[54] Brandon Bryant, "Ex-drone operator with PTSD: 'We see everything'", *Today* (6 June 2013), online: *Today* <www.today.com/video/ex-drone-operator-with-ptsd-we-see-everything-32665667514> (video).

[55] James Dao, "Drone Pilots Are Found to Get Stress Disorders Much as Those in Combat Do", *The New York Times* (22 February 2013), online: *The New York Times* <www.nytimes.com/2013/02/23/us/drone-pilots-found-to-get-stress-disorders-much-as-those-in-combat-do.html> [perma.cc/NH65-PEV4].

[56] Jean Lin Otto quoted in Dao, *ibid.*

[57] Boulianne Gobeil, *supra* note 10 at 107-108.

[58] The Parks Memo was a memorandum by W. Hays Parks, then Chief, International Law Branch International Affairs Division at the Office of the Judge Advocate General of the Army, which "explore[d] *assassination* in the context of national and international law to provide guidance in revision of U.S. Army Field Manual 27-10, *The Law of Land Warfare*, consistent with Executive Order 12333." Executive Order 12333 reasserted the prohibition on assassination imposed by President Gerald Ford. The memo's full text is available online

context of an armed conflict.[59] While a targeted killing is tactically equivalent to an assassination to the extent that both practices involve the killing of an individual in a secretive manner so as to attain a political objective, the latter was most recently prohibited by President Ronald Reagan's Executive Order 12333.[60] Hence, the presence of an armed conflict is necessary to render an otherwise unlawful assassination a legal targeted killing. The 2001 AUMF provided just that context.

As Shoon Kathleen Murray notes, in the direct aftermath of the terrorist attacks of 11 September 2001, then President Bush set the narrative tone for the AUMF that would be enacted only days later, qualifying the attacks on US soil as "acts of war".[61] Bush's statement was followed by discussions that had been prompted by the White House's desire to obtain more extensive military authority, among other increased powers, to go after the actors that had orchestrated the attacks.[62] After the rejection of a first draft which Congress deemed as granting the President too-great powers, a second version of the AUMF was approved on September 18.[63] The rejected first draft would have given the President the authority not only to wage war against the actors responsible for 9/11, but would have also entitled him to resort to force so as "to deter and pre-empt any future acts of terrorism or aggression against the United States".[64] This part of the text was removed so as to ensure that the exceptional authority granted by the AUMF could only be used against the engineers behind the September 11 attacks.[65] That this language was first included in the preliminary version of the AUMF and subsequently removed from it clearly indicates that Congress did not want to open the

---

(pdf): *University of Pennsylvania Law School* <www.law.upenn.edu/institutes/cerl/conferences/targetedkilling/papers/ParksMemorandum.pdf> [perma.cc/8TMJ-R9J8].

[59] Cheri Kramer, "The Legality of Targeted Drone Attacks as U.S. Policy" (2011) 9:2 Santa Clara Journal of International Law 375 at 381-382. Dawn L Rothe and Victoria E Collins note that the practice of targeting an individual whose name was taken from a list of pre-approved targets is legal since it is tantamount to having met the principle of distinction that is central to the laws of war—provided the intelligence on which the decision to place the target's name on the kill list was reliable (Dawn L Rothe & Victoria E. Collins, "The Normality of Political Administration and State Violence: Casuistry, Law, and Drones" (2014) 22:3 Critical Criminology 373 at 378). This would therefore render personality strikes legal since they are based on such kill lists. However, because the targets of signature strikes are not selected from said lists, the legal status of such strikes is less clear.

[60] Kramer, *supra* note 59 at 381.

[61] Murray, "The Contemporary Presidency", *supra* note 13 at 176.

[62] *Ibid.*

[63] *Ibid* at 177.

[64] *Authorization for Use of Military Force* quoted in Murray, "The Contemporary Presidency", *supra* note 13 at 176.

[65] Murray, "The Contemporary Presidency", *supra* note 13 at 177-178.

door to unlimited presidential powers.

Despite Congress' attempt to curb the powers it was ceding to the executive branch, the adopted text of the AUMF nevertheless grants extensive power. Under Section 2(a) of the document,

> the President is authorized to use all necessary and appropriate force against those nations, organizations, or persons he determines planned, authorized, committed, or aided the terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States *by such nations, organizations or persons* [emphasis added].[66]

While the intent behind the AUMF was to fight the perpetrators of 9/11, the actual text stipulates that the President may also use his authority to stop *future* acts of international terrorism. However, the President may only use force against future perpetrators *if* they also played a role in 9/11—as highlighted by the italicised section above. Despite the requirement that there be a tie to 9/11, critics have noted how broadly worded the AUMF remains.[67] In fact, it leaves it to the President himself to "determine" who is to blame for 9/11, essentially giving him a *carte blanche* as to whose names should be written down on the US kill list. To legitimise the targeting of groups with no apparent connection to 9/11, the US follows the "splinter theory", which it claims allows it to go after organisations who are fragments of the terrorist groups originally covered by the AUMF.[68] The AUMF also assigns to the President the task of gauging what amount of force is necessary and appropriate.[69] Scholars have pointed out that the AUMF—and its subsequent interpretation—represent a strikingly unusual authorisation to the extent that it neither sets geographical nor temporal boundaries on the President's ability to make use of military force.[70] John Kaag and Sarah Kreps contend that the "latitude provided in the AUMF sets a dangerous precedent".[71]

---

[66] *Authorization for Use of Military Force*, 2001, SJ Res 23, 107th Congress [*AUMF*].

[67] Rudalevige, *supra* note 12 at 883.

[68] Sarah Kreps, *Drones: What Everyone Needs to Know* (New York, NY: Oxford University Press, 2016) at 57.

[69] Rudalevige, *supra* note 12 at 883.

[70] Thomas Gregory, "Drones, Targeted Killings, and the Limitations of International Law" (2015) 9:3 International Political Sociology 197 at 202; Kaag & Kreps, *supra* note 13 at 84; Murray, "The Contemporary Presidency", *supra* note 13 at 178.

[71] Kaag & Kreps, *supra* note 13 at 86.

In sum, the AUMF's unspecific language translates into presidential powers that go far beyond the ambit that was initially intended by Congress in 2001—which Chris Edelson attributes to executive branch lawyers who gave the AUMF an overly liberal interpretation.[72] For the aforementioned reasons, it ought to be revised or, as Kaag and Kreps suggest, nullified.[73] The AUMF's drawbacks thus call for the articulation of a new and more circumscribed legal framework to sanction and govern the use of UAVs in counterterrorism campaigns—one which will also take into consideration the ongoing development and application of AI-assisted technologies in targeted killings.

B. ON THE GENEVA CONVENTIONS OF 1949 AND ITS ADDITIONAL PROTOCOLS OF 1977

While the AUMF provides the legal foundation for UAV strikes at the domestic level, the US must still abide by international legal standards when carrying out its targeted killings. As discussed above, targeted killings are legal under the 1989 Parks Memo provided they are conducted within an armed conflict. When that is the case, all laws of armed conflict apply. According to Micah Zenko, the US claims that it remains in a "continuous state of international armed conflict with Al-Qaeda and associated forces".[74] As Obama asserted in his National Defense University speech, "Under domestic law, and international law, the United States is at war with al Qaeda, the Taliban, and their associated forces".[75] In a subsequent speech, Obama noted that despite his administration's success in weakening al Qaeda, the US "continue[d] to face a terrorist threat".[76] This threat, he indicated, stemmed from the Islamic State—an organisation against which the US is still at war in 2019. During his allocution before the Arab Islamic American Summit, President Trump reiterated that the US was still fighting the Islamic State and other terrorist organisations, calling on his Arab counterparts to continue their counterterrorism partnership.[77] These assertions not only indicate that the US is still waging war against several non-State actors

---

[72] Chris Edelson, "The Law: In Service to Power: Legal Scholars as Executive Branch Lawyers in the Obama Administration" (2013) 43:3 Presidential Studies Quarterly 618 at 635.

[73] Kaag & Kreps, *supra* note 13 at 141.

[74] Micah Zenko, *Reforming U.S. Drone Strike Policies* (Special Report 65, Council on Foreign Relations, 2013) at 16.

[75] Obama, *supra* note 11.

[76] Obama, *supra* note 33.

[77] Donald Trump, "President Trump's Speech to the Arab Islamic American Summit" (21 May 2017), online: *White House* <www.whitehouse.gov/briefings-statements/president-trumps-speech-arab-islamic-american-summit/> [perma.cc/L5QN-995K].

deemed as "associated" with al Qaeda, they also set the context (at least discursively) for a state of armed conflict, which thus triggers the application of international humanitarian law (IHL) that governs the use of force during said armed conflicts.

That the US is involved in an armed conflict against al Qaeda was also recognised by the US Supreme Court.[78] Thus, UAV strikes are subject to IHL's principles of distinction, proportionality, necessity, and humanity.[79] The principles of distinction and proportionality are articulated in the four Geneva Conventions of 1949 and their two Additional Protocol of 1977, which codified the bulk of the laws of war. Taken jointly, these two principles also form *jus in bello* that is central to the Just War Tradition—the philosophical foundation of the Geneva Conventions and their Additional Protocols. Finally, the principles of necessity and humanity are values that permeate through the laws of war rather than being explicitly articulated in them.

The principle of (military) necessity demands that force be used only when no other means will achieve a given military objective.[80] Necessity may therefore dictate that the US attempt to capture a target before using lethal force against him or her.[81] This prescription is evidenced by Obama's remarks that "America does not take strikes when we have the ability to capture individual terrorists", and "[a]s a matter of policy, the preference of the United States is to capture terrorist suspects".[82] These two comments suggest that UAV strikes are only carried out when capture is not feasible—although whether that is indeed the case is not clear. The principle of humanity is closely associated with necessity since it "forbids the infliction of all suffering, injury or destruction not necessary for achieving the legitimate purpose of a conflict".[83] That is, if an objective can be achieved by injuring rather than killing a target, killing should be avoided. In this case, killing would also not meet the necessity requirement.

---

[78] Murray, "The Contemporary Presidency", *supra* note 13 at 186.

[79] Zenko, *supra* note 74.

[80] International Committee of the Red Cross, "What is IHL?", online: *ICRC* <www.icrc.org/en/document/what-ihl> [perma.cc/4SAE-6QB5].

[81] Jens David Ohlin, "Is *Jus in Bello* in Crisis?" (2013) 11:1 Journal of International Criminal Justice 27 at 42.

[82] Obama, *supra* note 11.

[83] "What is IHL?", *supra* note 80.

Additional Protocol I pertains to the protection of civilian populations whose lives are endangered by the presence of hostilities.[84] While US counterterrorism operations must comply with all applicable laws of war, Additional Protocol I is the most pertinent document when it comes to UAV strikes as its Articles 48 and 51(5)(b) respectively lay out the principles of distinction and proportionality:

> In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.[85]

> Among others, the following types of attacks are to be considered as indiscriminate: [...] an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[86]

Kaag and Kreps point out that although the US has yet to ratify Additional Protocol I, this document is regarded as customary law and thus imposes legal obligations on US conduct during armed conflicts.[87] The distinction and proportionality principles aim to protect civilians, but, as Jens David Ohlin notes, determining just how many civilians must have been killed before a UAV strike can be deemed disproportionate is not always easy.[88]

C. ON MILITARY LAWYERS AND THE LEGAL PROCESS THAT TAKES PLACE BEFORE A TARGETED STRIKE

In the case of personality strikes, the decision to kill an individual comes once that person's name has made its way onto the US' kill list.[89]

---

[84] ICRC, "The Geneva Conventions of 1949 and their Additional Protocols", online: *ICRC* <www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm> [perma.cc/B69B-W3C8].

[85] *Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)*, 8 June 1977, 1125 UNTS 3, 1991 ATS No 29/ 16 ILM 1391 (1977) (entered into force 7 December 1978) [*Additional Protocol I or API*], art 48.

[86] *Ibid*, art 51(5)(b).

[87] Kaag & Kreps, *supra* note 13 at 174.

[88] Ohlin, *supra* note 81 at 43.

[89] Jaume Saura, "On the Implications of the Use of Drones in International Law" (2016) 12:1

Individuals whose names have been placed on this list are identified by intelligence agencies as posing a threat to the US and sharing ties with Al-Qaeda.[90] According to Jo Becker and Scott Shane, throughout his tenure Obama personally added names to that list, thus turning them into legitimate targets.[91] Obama also approved each strike in Somalia and Yemen.[92] The direct participation of the President in this so-called "nomination" process translates into a pre-approved license to kill, whereby the Commander-in-Chief officially delegates the authority granted him by the AUMF to the US military that is then tasked to go through the list and terminate the individuals whose names are on it. The role of military lawyers then becomes one of ensuring that the military carries out that task in accordance with its IHL obligations—more importantly following the principles laid out under Articles 48 and 51(5)(b) of Additional Protocol I.

In their assessment of whether a strike is legal, military lawyers must therefore look at judicial precedents—that is, court decisions where the principle of proportionality was applied to a targeted killing conducted via UAV. Yet, Ohlin points out that such precedents are nearly non-existent, thus leaving the application of these standards up to military lawyers' interpretation.[93] As he mentions, the notion of intent is narrower in the common law tradition in comparison to the civil law tradition.[94] Thus, common law lawyers are less likely than their civil law counterparts to find cases of *intentional* targeting of civilians. Since the common law represents the main legal tradition in the US, most military lawyers working for the DoD will have been trained in that tradition and will therefore apply the common law notion of intent. In other words, common law lawyers—and, concomitantly, the US—are likely to be more permissive when assessing whether a strike meets the distinction principle.

Unlike operators who must continuously monitor the video feed of UAVs while they are aloft, military lawyers need not be present at all times—although they remain available around the clock in case a targeted

---

Journal of International Law and International Relations 120 at 147.

[90] Kaag & Kreps, *supra* note 13 at 33.

[91] Jo Becker & Scott Shane, "Secret 'Kill List' Proves a Test of Obama's Principles and Will", *The New York Times* (29 May 2012), online: *The New York Times* <www.nytimes.com/2012/05/29/world/obamas-leadership-in-war-on-al-qaeda.html> [perma.cc/XSZ2-5TFG].

[92] Klaidman, *supra* note 14 at 204-205.

[93] Ohlin, *supra* note 81 at 43.

[94] *Ibid* at 44.

strike becomes urgent.[95] Yet, the intelligence gathering abilities of UAVs, as described in Section III above, enable operators and military lawyers to appraise the data as it is being collected and thus follow the progress of any given ISR mission that precedes a targeted killing.[96] According to Robert P. Barnidge, this live oversight could also make the life-and-death decisions of targeted strikes more transparent.[97] Chatterjee maintains that lawyers are able to observe the many screens and sensors inside the command and control centre.[98] They can therefore ascertain the accuracy of any given target and ensure that no civilians find themselves in its vicinity. Once the military lawyer determines that a strike meets all the legal requirements of IHL, they give the UAV operator a green light to fire its weapon.[99] If the target survives and a second strike becomes necessary, the same process is repeated because civilians may have approached the blast site to help the victim(s). The next section delves into AI, exploring some of its likely military application that may assist UAV operators and military lawyers while conducting targeted killings.

V. ON ARTIFICIAL INTELLIGENCE AND HOW IT CAN ASSIST UAV OPERATORS AND MILITARY LAWYERS

A. WHAT IS AI AND WHAT CAN IT DO? ON NEURAL NETWORKS AND DEEP LEARNING

Although he wrote more than 15 years ago, Adams noted that militaries were increasingly relying on technological developments in the field of AI to augment the autonomy of their weapons systems and further improve their battlefield efficiency.[100] Given the current popularity of AI, the trend identified by Adams is likely more pronounced today. Toshinori Munakata describes AI as a form of "advanced computing" that can have a wide range of commercial and industrial applications.[101] One main

---

[95] See Chatterjee, *supra* note 15.

[96] Robert P Barnidge, "A Qualified Defense of American Drone Attacks in Northwest Pakistan Under International Humanitarian Law" (2012) 30:2 Boston University International Law Journal 409 at 413.

[97] *Ibid.*

[98] Chatterjee, *supra* note 15.

[99] *Ibid.*

[100] Adams, *supra* note 17 at 9-10.

[101] Toshinori Munakata, "Commercial and industrial AI" (1994) 37:3 Communications of the ACM 23 at 23. Lee McCauley defines AI as "a broad term typically encompassing any human-made system that performs tasks considered to require some level of intelligence" (Lee McCauley, "AI Armageddon and the Three Laws of Robotics" (2007) 9:2 Ethics and

model of AI—neural networks—is central to machine learning, simulating the way in which humans learn from experience.[102] Neural networks' ability to "learn by themselves from patterns" will likely be key to UAV operations since targeted strikes are inherently repetitive tasks—i.e. the decision-making process preceding them seeks to locate and identify a target, determine the appropriate amount of force to be used, and ensure that all IHL principles are respected.[103] The repetitive nature of targeted strikes thus lends itself well to the way neural networks function.

Yoshua Bengio explains that "[m]achine learning allows computers to learn from examples—to learn from data".[104] He adds that neural networks and "deep learning" represents approaches to "machine learning".[105] A more sophisticated technique, deep learning represents a multi-layered version of a neural network. Like neural networks, this approach learns from the data the machine is presented with, abstracting data in a hierarchical way.[106] For instance, to categorise an image, deep learning does not need to analyse every single pixel; instead, it only needs to abstract the image by looking at the different elements that constitute it and which form its hierarchy, such as its broader shape and contours.[107] This method is similar to how the human brain processes data: one need not look at all the feathers to know that one is looking at a bird. Camera systems in self-driving cars and facial recognition are among some of the recent, practical applications of deep learning.[108] These two uses will likely prove advantageous when combined with UAVs to conduct ISR missions and to identify the target of a strike.

Most of AI's military applications are likely to be seen *before* a targeted strike is carried out—at a moment where human operators must assess a complex battlefield environment that is unique to each mission and strike. This stage requires operators to process a large amount of information and factor in many variables (e.g. the presence of civilians, the size of their payload and its expected blast radius, etc.) while building on the experience they acquired from previous missions. Neural networks

---

Information Technology 153 at 156).

[102] Munakata, *supra* note 101 at 25.

[103] *Ibid.*

[104] Yoshua Bengio, "The Rise of Artificial Intelligence through Deep Learning", *TEDx Talks* (November 2016), online: *Youtube* <www.youtube.com/watch?v=uawLjkSI7Mo> [perma.cc/6XFW-GDGF].

[105] *Ibid.*

[106] Yann LeCun, Yoshua Bengio & Geoffrey Hinton, "Deep learning" (2015) 521:7553 Nature 436 at 436.

[107] *Ibid* at 439.

[108] *Ibid* at 439-440.

might also help perform more kinetic functions. For instance, Peter Trhan shows how neural networks may be used to control the course of a robot navigating within a confined environment.[109] Although applications of neural networks have so far been limited to unmanned *land* vehicles, more sophisticated versions of such neural networks and deep learning will likely be used to allow UAVs to navigate autonomously and avoid colliding with obstacles. Hence, neural networks and deep learning can serve trajectory control functions.

B. ON HOW AI IS LIKELY TO ASSIST UAV OPERATORS AND MILITARY LAWYERS

According to Ty McCormick, as early as October 2013, British military manufacturer BAE Systems was testing a UAV that could "autonomously identify targets"—although the manoeuvres were still overseen by a human.[110] Target identification is different than target selection—with the latter involving a more normative assessment as to whether a person should or should not be killed, which warrants human judgement. Once a target is selected, it must be located and its identity must be ascertained—that is, it must be identified. For instance, if I lose my wallet in a shopping mall, I can go to the lost-and-found, but it would be careless to simply assume that just any wallet there is *my* wallet without first verifying that it indeed contains my ID card. What BAE Systems' UAV enables is to confirm that my ID is in my wallet—or that Anwar al-Awlaki is in fact Anwar al-Awlaki and not just anybody else resembling him. For now, target selection is likely beyond the scope of its capabilities. Yet, as the sophistication of algorithms powering machine learning increases, target selection may become realistic. As Cathy O'Neil warns us, however, algorithms are based on assumptions that reflect the biases of their coders.[111] Challenging the objectivity of algorithms, she argues that "they repeat our past practices, our patterns. They automate the status quo".[112] Thus, if they are based on a pre-conceived notion of what a target looks like—as seems to be the case with signature strikes—the accuracy of algorithms would need to be checked against selection biases via a process O'Neil refers to as an "algorithmic audit".[113]

---

[109] Peter Trhan, "The Application of Spiking Neural Networks in Autonomous Robot Control" (2010) 29:5 Computing and Informatics 823 at 824-825.

[110] Ty McCormick, "Lethal Autonomy: A Short History" (2014) 204 Foreign Policy 18 at 19.

[111] Cathy O'Neil, "The era of blind faith in big data must end", *TED Talk* (April 2017), online: *TED* <www.ted.com/talks/cathy_o_neil_the_era_of_blind_faith_in_big_data_must_end> [perma.cc/533A-GXQT].

[112] *Ibid.*

[113] *Ibid.*

Auditing the algorithms used to select targets so as to prevent such biases might be easier said than done since sensors like the Gorgon Stare and the ARGUS IS produce overwhelming flows of data, as mentioned in Section III above, rendering humans more dependent on powerful algorithms and AI-assisted technology that can overcome this hurdle. According to Adams,

> [a]utomated systems can certainly reduce the pressure of information saturation and eliminate conflicts, but at a price. Essentially, they do so by creating a series of information "filters" that establish priorities and eliminate marginal data, reconcile the remaining information conflicts, and present a consensus picture of the situation. All of this is invisible to the ultimate consumer, out of his or her control, and very likely not well understood. This means that the commander is receiving a picture of the battlefield that is designed to emphasize certain things while de-emphasizing others. Still other factors are omitted entirely.[114]

Current neural networks and deep learning are likely too primitive to allow for such complex filtering of information and present operators and military lawyers with a complete and final picture of the battlefield. According to Sharkey, this may never be achievable since the laws of war do not define the terms civilian and combatant that are central to understanding the battlefield.[115] That said, progress in machine learning may conceivably lead to the type of assistance contemplated by Adams—at which point the line between identifying and selecting targets becomes blurred. In sum, AI systems, such as neural networks and deep learning, are likely to assist operators and military lawyers in the performance of less advanced functions—until new advances in the field of machine learning enable them to take on more complex tasks away from humans. These include target or civilian identification and classification, via facial recognition and object recognition and detection. The next section explores ways in which the use of such technologies in targeted killing could be governed.

---

[114] Adams, *supra* note 17 at 10.

[115] Sharkey, *supra* note 19 at 16.

VI. A TENTATIVE LEGAL FRAMEWORK TO GOVERN AI-ASSISTED UAVs

A. ON THE REGULATION OF SELF-DRIVING CARS BY THE CALIFORNIA DEPARTMENT OF MOTOR VEHICLES

One application of machine learning that has garnered significant public attention is found in self-driving or driverless cars. As mentioned in the previous section, neural networks can serve to orient the course of autonomous land vehicles. Moreover, deep learning methods can be used with camera sensors to enable a machine to recognise different types of objects, thus avoiding crashes when used with self-driving cars. In 2017, the Massachusetts Institute of Technology also started offering a seminar—MIT 6.S094: Deep Learning for Self-Driving Cars—that looks exclusively at the use of deep learning and neural networks in self-driving cars.[116] If anything, this seminar highlights the topicality of AI in self-driving cars. Further pushing the development of self-driving cars is the prospect of witnessing a decreasing number of deadly traffic accidents following the introduction of AI-assisted technologies.[117] This expected benefit is likely to put some pressure on policymakers and legislators to put in place ever more permissive regulations for manufacturers to develop and test self-driving cars.

As is often the case with state-of-the-art technologies, regulating schemes—however tentative—follow their development and deployment, but necessitate some amendments as technologies evolve. While comprehensive rules governing the manufacturing and operation of self-driving cars are still being drafted, the California Department of Motor Vehicles (DMV) has been ahead of other US states, having first articulated its own scheme regulating the testing of autonomous vehicles as early as 2012. Aarian Marshall notes that initial versions of the scheme

---

[116] "MIT 6.S094: Deep Learning for Self-Driving Cars", online: *Massachusetts Institute of Technology* <selfdrivingcars.mit.edu/> [perma.cc/JGX8-FTNH].

[117] Harari, *supra* note 28 at 23-24; Jack Karsten & Darrell West, "The state of self-driving car laws across the U.S." (1 May 2018), online: *Brookings Institution* <www.brookings.edu/blog/techtank/2018/05/01/the-state-of-self-driving-car-laws-across-the-u-s/> [perma.cc/V557-EE5K]; Aarian Marshall, "Congress Unites (Gasp) to Spread Self-Driving Cars Across America" (6 September 2017), online: *Wired* <www.wired.com/story/congress-self-driving-car-law-bill/> [perma.cc/B9P8-PH37]; Jack Stewart, "California's Finally Ready for Truly Driverless Cars" (11 March 2017), online: *Wired* <www.wired.com/2017/03/californias-finally-ready-truly-driverless-cars/> [perma.cc/F8WE-3HLE].

mandated that a driver remain behind the driver's seat at all times when a self-driving car was operating on a public road in California.[118] However, recent changes to the regulations—announced on 26 February 2018 and implemented on 2 April 2018—now enable self-driving cars to circulate without warranting that a human operator be present inside the car and who could take physical control in case of emergency.[119] In July 2018, the Pennsylvania Department of Transportation (PennDOT) released its own guidelines for the oversight of "highly automated vehicles" (HAV).[120] Like the California DMV's earlier and more prudent regulation, PennDOT's new guidance stressed the need for a "safety driver" that could intervene whenever the HAV experiences a glitch.

Despite California's pioneering stance of allowing the safety driver to be *outside* of the self-driving cars, its new regulation clearly states the need for a human in the loop at all times. In fact, Section 227.26(c) forbids a manufacturer from testing an autonomous test vehicle "when an autonomous vehicle test driver is not seated in the vehicle's driver seat and monitoring its operations and *able to take over physical control of the vehicle* in the event of an autonomous technology failure or other emergency [emphasis added]".[121] Moreover, Section 227.32 further prevents testing unless the autonomous vehicle test driver meets several criteria including warranting that she remains in the loop—even if not physically in the car. More specifically, under Section 227.32(a), testing is prohibited unless "[t]he autonomous vehicle test driver is either in immediate physical control of the vehicle *or is actively monitoring the vehicle's operations and capable of taking over immediate physical control* [emphasis added]".[122] The above italicised passages highlight the DMV's concern for a continuous human control over the car.[123] This need for an

---

[118] Aarian Marshall, "Fully Self-Driving Cars Are Really Truly Coming to California" (26 February 2018), online: *Wired* <www.wired.com/story/california-self-driving-car-laws/> [perma.cc/BK45-9949].

[119] *Ibid.* The absence of a human in the car most closely resembles the way UAVs are operated.

[120] "PennDOT Issues Guidance for Increased Safety Oversight of Highly Automated Vehicles", online: *Pennsylvania Department of Transportation* <www.penndot.gov/pages/all-news-details.aspx?newsid=514> [perma.cc/T8CM-NYP8].

[121] "Driverless Testing Regulations. Article 3.7 - Testing of Autonomous Vehicles" (approved 26 February 2018), online (pdf): *California Department of Motor Vehicles* <www.dmv.ca.gov/portal/wcm/connect/a6ea01e0-072f-4f93-aa6c-e12b844443cc/DriverlessAV_Adopted_Regulatory_Text.pdf?MOD=AJPERES> [perma.cc/F9B2-W3D7].

[122] *Ibid.*

[123] PennDOT's guidelines also require that the self-driving car manufacturer "[a]cknowledg[e] that the HAV can safely alert the safety driver, when applicable, that the driver must take back control of the vehicle" in order to test the HAV on Pennsylvania roads.

ongoing supervision is also emphasised in the DMV's definition for an "autonomous test vehicle", stated under Section 227.02(b) of the regulation: "a vehicle that has been equipped with technology that is a combination of both hardware and software that, when engaged, performs the dynamic driving task, *but requires a human test driver or a remote operator to continuously supervise the vehicle's performance of the dynamic driving task* [emphasis added]". [124] The above sections are indicative of a tension in driverless cars, namely lawmakers' desire to keep a human oversight over a technology that is first and foremost aimed at removing the human driver altogether. It might be too early to determine whether humans will stay in the loop or be displaced by AI in the long run, but California's current regulation clearly advocates for a human presence that can act as a fail-safe—which in turn implies that human operators must maintain more than a mere symbolic control over the autonomous vehicle.[125]

B. ON THE REGULATION OF SELF-DRIVING CARS BY THE US CONGRESS

The California DMV's regulation represents the most sophisticated State-level scheme governing the use of self-driving cars to date.[126] Yet, the US Congress is in the process of enacting the SELF DRIVE Act aimed at setting uniform[127] rules across the US, with the House having passed Bill

---

"PennDOT Issues Guidance", *supra* note 120.

[124] "Driverless Testing Regulations", *supra* note 121. According to Marshall (*supra* note 118), current driverless automotive technology can operate somewhat free from human control. However, it has yet to reach a point where manufacturers will feel confident enough to let the machine take full control as doing so comes with the risk of harming their reputation should a fatal error occur (*ibid*). That eventuality would seem to conflict with the DMV's current definition of an "autonomous test vehicle." It is unclear how the DMV would regard a fully autonomous car—that is, one in which absolutely no human control is necessary. Should technological progress render this possible, as current trends suggest it might be, the DMV's definition would have to be revised as its requirement for a human test driver or a remote operator would not be suitable for a vehicle that is entirely autonomous—and thus not requiring a human operator.

[125] In cases involving an autonomous vehicle in which there is no driver, as stipulated under s. 227.38(b)(1), the manufacturer must ensure that "There is a communication link between the vehicle and the remote operator to provide information on the vehicle's location and status" ("Driverless Testing Regulations", *supra* note 118). This section marks the minimum level of control that must be exercised by a human operator who must know where the vehicle is and what manoeuvre(s) it is about to make.

[126] As a point of comparison, the state of Arizona has adopted a laissez-faire approach, having not yet regulated *any* aspects of self-driving cars (Marshall, *supra* note 118).

[127] Manufacturers are also likely to pressure Congress to enact regulation that renders their products marketable. Thus, the implementation of uniform regulation across the US is key because eventual customers are unlikely to purchase a self-driving car unless consistent laws

H.R.3388 unanimously.[128] Under Section 3(1)(b)(1), the SELF DRIVE Act would take precedence over State regulations including the California DMV's—unless it is identical to that of Bill H.R.3388. As Sean O'Kane explains, "states have regulated the safety regarding the operation of vehicles, while the federal government has been in charge of the safety of the vehicle itself".[129] Thus, unlike the California DMV's regulation, the scope of Bill H.R.3388 is somewhat limited to the construction and development of self-driving cars. As a result, Bill H.R.3388 does not legislate on whether the presence of a human driver or operator is a necessary fail-safe of self-driving cars in the same way the California DMV does. Under Section 3(1)(b)(4), states may nonetheless opt to impose "higher performance requirement[s]" or more stringent rules than those proposed in Bill H.R.3388.[130] This means that the California DMV's and PennDOT's requirement for a human presence would remain valid even once Bill H.R.3388 has become law notwithstanding Section 3(1)(b)(1) of the SELF DRIVE Act.

Section 5 of the SELF DRIVE Act, which addresses the possibility that self-driving cars may be the target of cyberattacks, stipulates that a human operator tasked with the mitigation of cybersecurity threats must be designated by the manufacturer of self-driving cars. In fact, Section 5 of Bill H.R.3388 adds Section 30130(a)(2) to Subtitle VI of Title 49, United States Code, which demands that the manufacturer lay out a clear cybersecurity plan that would include "[t]he identification of an officer or other individual of the manufacturer as the point of contact with responsibility for the management of cybersecurity".[131] As Ariel Darvish records, by introducing the SELF DRIVE Act, Congress sought to foster the development and testing of driverless automotive technologies while ensuring that the cybersecurity threats they face do not materialise into

---

are in place that allow the car to drive them to visit their out-of-state relatives.

[128] Sean O'Kane, "The US is speeding toward its first national law for self-driving cars" (6 September 2017), online: *The Verge* <www.theverge.com/2017/9/6/16259170/self-drive-act-autonomous-cars-legislation> [perma.cc/WK3H-VQC9]. Bill H.R.3388 was sent to the Senate on 7 September 2017 and is currently under review by the Committee on Commerce, Science, and Transportation ("H.R.3388 - SELF DRIVE Act", online: *US Congress* <www.congress.gov/bill/115th-congress/house-bill/3388> [perma.cc/8VL5-6L9L]). While the Senate has yet to pass Bill H.R.3388 at the time of writing, I employ the version currently before this Committee as I use this scheme merely to *inform* a legal framework to govern the deployment of AI-assisted UAVs. Thus, that Bill H.R.3388 is subject to change before becoming law does not weaken the legal framework I propose below.

[129] O'Kane, *supra* note 128.

[130] "H.R.3388 - SELF DRIVE Act", *supra* note 128.

[131] *Ibid.*

actual attacks that could have deadly ramifications.[132] In light of this context, Section 5 of Bill H.R.3388 represents an implicit acknowledgement that despite the high level of sophistication of the AI-assisted technologies contained in self-driving cars, vulnerabilities exist and technological progress will likely be accompanied by ever newer cyberthreats.

The nonspecific language pertaining to cybersecurity included in Section 5 of Bill H.R.3388, which leaves it to manufacturers to determine what exact steps must be taken to mitigate the risks of eventual cyberattacks, suggests that lawmakers had in mind the fact that self-driving cars would come with unforeseen vulnerabilities. That is, the Bill's drafters opted for language that enables manufacturers to implement new cybersecurity measures as they become necessary rather than having to amend the law each time a new measure is required.[133] While the current version of the SELF DRIVE Act remains silent on whether a human is needed in the loop, its recognition that self-driving cars can be hacked and the ensuing requirement that a human be tasked with managing the vehicle's cybersecurity does point to Congress' reluctance to let humans completely out of the loop. The Bill's "higher performance requirement" clause further supports this position as Congress gives states the power to enact legislation that would impose a human presence.

C. PROPOSING A LEGAL FRAMEWORK TO GOVERN THE DEPLOYMENT OF AI-ASSISTED UAVs

Having looked at the California DMV's regulation of self-driving cars and the provisional SELF DRIVE Act introduced by Congress, this subsection of the article proposes a tentative legal framework to govern the deployment of AI-assisted UAVs in targeted killing missions. In this section, I refrain from laying out specific rules that should be contained in an eventual legal framework; rather, I lay out general principles that should be regarded as guidelines to inform the drafting of such a document.[134] As Victor Hansen argues, foreign sources are unlikely to

---

[132] Ariel Darvish, "The SELF DRIVE Act: Cybersecurity and Cars on Autopilot" Fordham Journal of Corporate & Financial Law (15 January 2018), online: *Fordham University* <news.law.fordham.edu/jcfl/2018/01/15/the-self-drive-act-cybersecurity-and-cars-on-autopilot/> [perma.cc/R78L-KGYY].

[133] *Ibid.*

[134] As I noted above, these guidelines may serve to inform not only the US, but also other actors who deploy military UAVs. The success of these guiding principles is in part dependent of their application by several states, because individual actors are unlikely to commit to a framework that imposes limits on their ability to use a weapon if other users are not doing so as well.

impose substantive limits on the US' ability to use UAVs; rather, a more promising path to curb US power would have to originate in its domestic institutions, namely its courts and Congress.[135] Yet, Hansen concedes that "courts are institutionally unsuited and incapable of providing appropriate oversight",[136] thus leaving Congress as the most appropriate venue to limit US power to carry out UAV strikes. The principles I propose below represent a starting point for the legislative branch to begin drafting a new legal framework.

The five principles that follow are informed by the current regime governing autonomous cars in the US. They are also guided by the following assumption: given the violent character of warfare, the use of AI in military UAVs requires at least as much human oversight as is currently present in the use of AI in civilian automotive transport. Yet, this assumption may be in conflict with the military imperative of projecting force as swiftly as possible and that ultimately presses military decision-makers in the opposite direction, namely one with less human involvement because keeping an operator or lawyer "in the loop" slows down execution. The following principles resist this temptation, instead embracing the view that the intentional killing of human beings deserves to be conducted under the highest ethical standards. IHL recognises the unfortunate reality that war does take place, but strives to restrict the ways in which it can be carried out once it has started. To construct the following principles in opposition to the military imperative of rapid execution and complete delegation to AI is no doubt a normative stance, but one which seeks to continue the Just War tradition. Having disclosed this ethical assumption, here are the five guiding principles.

Principle 1: When neural networks or deep learning are used to perform primarily kinetic functions that do not involve the use of force, the demand on the operator need not be as high as when a target is selected or a weapon is fired.

Kinetic functions refer to the physical movement of the UAV and what allows the aircraft to remain aloft (i.e. via the motion of its propellers, wings, etc.). This would include functions aimed at stabilising the aircraft during flight as well as those ensuring that it does not stray from its intended course while relying on its Global Positioning System (GPS).

---

[135] Victor Hansen, "Predator Drone Attacks" (2011) 46:27 New England Law Review 27 at 30.

[136] *Ibid* at 36.

As mentioned in Section III above, the US' desire to shield its UAV operators from psychological harm associated with their unique work will likely incentivise further delegation of decision-making power to AI-assisted technologies. However, the increasing reliance on AI and machine learning in UAV operations should follow the California DMV's model. That is, there should be a meaningful (as opposed to a merely symbolic) human oversight of UAV operations wherever the use of deadly force is being contemplated. Unlike self-driving cars that operate on busy public roads and may therefore injure pedestrians or their passengers, the risk of aerial traffic accidents is far more limited when it comes to UAV because they do not transport human passengers.[137]

Moreover, since they operate in the airspace of remote and sparsely populated areas such as Pakistan's Federally Administered Tribal Areas (FATA), UAVs are unlikely to crash into bystanders. However, as technological advances render targeted strikes ever more precise, the possibility of operations being carried out in densely populated areas increases. Thus, imposing a strict requirement for a human oversight when UAVs are not engaged in targeted killings might not be as essential now, but might eventually become so. That said, strikes in urban centres would come with a much higher political risk as even minute errors could result in several civilian casualties. Moreover, a strike in a city centre would be much more accessible for the media (or anyone with a smartphone) to cover than a strike in a desolate location like Pakistan's FATA. Media coverage showing live footage of the blast site in the immediate aftermath of the strike, which is currently impracticable in FATA, would also make it far more difficult for most governments to ignore the public outrage such an incident would likely create. Thus, I argue that the technological advancements that might be achieved in the foreseeable future are unlikely to overcome the chilling effect these factors would create. Thus, Principle 1 assumes that UAV strikes will continue to occur in relatively remote and not densely populated areas.

---

[137] Given the increasing use of UAVs in military campaigns, it is possible to visualise a not-so-distant future in which military UAVs will be transporting human personnel, thereby increasing aerial traffic and warranting the safeguards currently in place for the use of self-driving cars. Amazon's Prime Air, which seeks to implement a large-scale UAV delivery service, indicates that aerial traffic might eventually resemble the streets of a busy metropolis. See "Amazon Prime Air", online: *Amazon* <www.amazon.com/Amazon-Prime-Air/b?ie=UTF8&node=8037720011> [perma.cc/4FQD-EWNU].

Principle 2: When deep learning is used for target identification, UAV operators and military lawyers should actively monitor the process to ensure the accuracy of the target's ID by checking it against other available sources of intelligence. Operators and military lawyers should have the final word.

Principle 2's requirement for a human presence playing an oversight role would be in line with DoD Directive 3000.09, which calls for "appropriate levels of human judgment over the use of force". While target identification does not involve the use of force per se, identifying a target is tantamount to killing him or her since once the UAV operator has obtained a positive ID, the next step will be the termination of the target – provided all IHL requirements are also met. Moreover, a proper level of "active monitoring" would go beyond merely one signing a delivery notice when one receives a package by mail. Instead, it should resemble the more thorough process of opening the package to ensure that it is in good condition and that all the parts have been delivered *before* signing the reception notice.

When machine learning is used to ascertain the identity of a target (*i.e.*, one that has already been selected via a pre-approved kill list), such as when deep learning is applied to facial recognition, the role of the operator and military lawyer should resemble that of the autonomous vehicle test driver under Section 227.32(a) of the California DMV's regulation. That is, they should actively monitor the UAV's target identification process and remain in a position to overrule the algorithm's final conclusion as to who the target is. This could be done by cross-checking the ID of the target in question to ensure that it corresponds to what the operator would expect based on human intelligence (HUMINT) collected by sources on the ground. For instance, if a UAV operating in FATA relies on deep learning technology to identify a target who according to recent intelligence should be in Somalia, the operator should be wary of this conflicting information.

Target identification, which is connected to the principle of distinction, also implies *civilian* identification. Since machine learning simulates the way humans learn from experience, the exposure to large amounts of data obtained during ISR missions should, provided algorithmic audits are properly conducted, enable the UAV to become increasingly efficient at discerning between civilians and non-civilians. Whereas operators should not blindly rely on the identification of a target by the UAV due to the possibility for errors, the identification of a civilian by the UAV should warrant a high degree of deference. That is, operators and military lawyers should assume that the civilian is indeed a civilian

(even though he could be a target). Hence, even when a target has been identified and that the operator has cross-checked the target's identity with alternative sources of intelligence, the identification of a civilian in the target's vicinity should prompt military lawyers' vigilance. In a scenario where killing the target involves a risk of injury or death to a civilian, military lawyers should make the final decision. This process requires an ethical balancing that should not be left to a machine.[138] To be qualified to make these decisions, lawyers should receive a training similar to that of intelligence analysts. Such a training would allow them to understand how the information they are presented with was gathered so that they can approach it analytically rather than uncritically assume its validity.

Judicial review need not be available when military lawyers choose not to strike. In such cases, it would be futile to review the decision on the merits because by the time a reviewing body holds that the strike ought to have been taken, the battlefield circumstances that made the strike possible in the first place would no longer be the same. However, where the lawyer chooses to fire the weapon, judicial review could offer a potential, although insufficient, avenue for the injured civilian (or his family if he was killed) to achieve justice. Future research could determine the exact process through which an applicant would have to go, with particular attention to a prescription period given that it might take time for the applicant to determine who operated the UAV and the jurisdiction where his application for judicial review should be made. That the lawyer relied on information protected by national security considerations would have to be addressed as well as it represents a likely barrier to the judicial review of his decision to strike.

Principle 3: If the mission is not time-sensitive, UAV operators and military lawyers should have a more active role in selecting targets and they should refrain from overly relying on machine learning. The role of UAV operators and military lawyers may be lessened in proportion to the increase in the mission's time-sensitivity.

However broad the AUMF may be, the US continues to rely on this document to legitimise its use of UAVs in counterterrorism operations, as mentioned in Section IV above. Yet, the AUMF only authorises the President to resort to force to fight the perpetrators of 9/11 and, as has been argued following subsequent interpretations of the document, other actors who are splinters of the organisations initially covered under the

[138] This is in line with the ethical assumption I laid out at the beginning of this subsection.

AUMF. Although the authority granted by the AUMF is wide, the selection of targets is still limited to those actors. Furthermore, the principle of distinction laid down in Article 48 of the Additional Protocol I further constrains the US' ability to select targets. Even when a target complies with these legal requirements, Article 51(5)(b) of the Additional Protocol I, which sets out the principle of proportionality, provides a last constraint, preventing the US from using force against an otherwise legitimate target if doing so will cause disproportionate harm to civilian populations. Respect for these legal obligations is of paramount importance as they represent the core of the laws of war. Sensors such as the Gorgon Stare and the ARGUS IS have the potential to patrol and monitor vast war theatres. When they are combined with machine learning that can sort through the large amount of data those sensors gather, it becomes easy, as Adams argues, to let the technology take on a greater role in decision-making.[139] Yet, as O'Neil reminds us, blind reliance on algorithms can have negative repercussions.[140] Thus, operators should refrain from the temptation of letting the machine make decisions on their behalf and should be the ones selecting targets—especially when a given targeted strike is not time-sensitive and operators have sufficient time to make an informed and calculated decision.

The drafters of the Montreal Declaration for a Responsible Development of AI ask a pressing question that is at the core of Principle 3: "Should a human always make the final decision?"[141] Principle 3 will likely be the most difficult principle to implement in an eventual legal framework given the incentives to increase battlefield efficiency by removing humans from the loop completely. Yet, the principle's reference to the level of time-sensitivity of the mission aims to strike a balance between compliance with the laws of war and the reality of the battlefield which sometimes calls for swiftness.

A further risk here is that the person in command could declare a given operation to be "time sensitive", thereby allowing the AI-assisted UAV to override any human operator or lawyer and opening the door to a slippery slope where time sensitivity is invoked all the time. As Principle 5 suggests below, a potential way of preventing, or at least mitigating, the slippery slope problem would be to have a body tasked with overseeing the overall use of UAVs. Should a commander embark on that slippery

---

[139] Adams, *supra* note 17.

[140] O'Neil, *supra* note 111.

[141] "The Declaration", online: *Montreal Declaration for a Responsible Development of AI*, online: *Montreal Declaration Responsible AI* <www.montrealdeclaration-responsibleai.com/the-declaration> [perma.cc/FT9K-JTHW].

slope by declaring all strikes "time-sensitive", the review board discussed in Principle 5 would offer an *ex post* fail-safe. Although the review board may not be able to prevent an individual strike given that it is a mechanism that operates retroactively, it would nonetheless prevent the overall use of UAVs from being deployed by human operators too eager to delegate their decision-making authority to machines.

Getting a clear understanding of Principle 3 requires elaborating on the concept of time-sensitivity. In *Eye in the Sky*, a known terrorist is finally located after months of research.[142] The UAV follows his movements until he meets in a house with a group of individuals, one of whom assembles two vests carrying explosives. Two men then put the vests on themselves, strongly suggesting that they are about to detonate them in a public space. This scene depicts the epitome of what would represent a highly time-sensitive mission. Yet, not all UAV missions involve a similar "ticking time bomb" scenario.

Time-sensitivity is not a binary concept; rather, it should be determined contextually and as representing a spectrum that ranges from not time sensitive to highly time-sensitive. An example of the former would be a routine ISR mission where the intelligence being gathered serves to identify broad trends about a terrorist organisation's activities on a given territory. An ISR mission could also be time-sensitive if, for instance, soldiers are under enemy fire and the UAV gathers intelligence that informs them about the location from which the shots are fired so that they can fire back and thwart the threat against them. A targeted strike could fall on both ends of the time-sensitivity spectrum. Where intelligence indicates that a terrorist whose location is known will remain in the same place for a prolonged period of time and that he does not intend to launch an imminent attack, a targeted strike against him would not be time-sensitive. In an alternative situation, intelligence could suggest that the terrorist has been planning an attack that is about to be launched or that, although it may not be launched for another few days or weeks, the terrorist is about to go into hiding until the attack is ready to be launched at which point it would be too late to prevent it. Such a situation would be highly time sensitive and a targeted strike against the terrorist may be warranted—provided capture is not a viable option.

---

[142] *Eye in the Sky*, *supra* note 16.

Principle 4: To mitigate the risk of cyberattacks against AI-assisted UAVs, human operators should be tasked with the management of cybersecurity and follow a plan that allows for the implementation of new measures as they become necessary.[143]

Even if the aforementioned three principles are followed, the vulnerability of UAVs to cyberattacks must be mitigated. Hackers could otherwise jeopardise all efforts to comply with the laws of war and ensure that AI-assisted UAVs function the way they were designed to. As Liran Antebi and I have argued, UAVs' dependence on computer-based networks makes them particularly vulnerable to a wide range of cyberattacks. [144] The vulnerabilities of autonomous technologies to cyberattacks has also been recognised by Congress, as evidenced by Section 5 of the SELF DRIVE Act, which calls manufacturers of self-driving cars to prepare a detailed cybersecurity plan. Three main steps may be taken to mitigate the risk faced by UAVs: making a realistic assessment of cyber-vulnerabilities, installing a system that would alert the operator when the UAV's cybersecurity has been compromised, and encrypting the data communicated between the UAV and the command and control centre.[145] The management of cybersecurity should be left to a human operator since computer-based systems may be incapable of assessing that they have been compromised. This is exemplified by the Stuxnet malware that infected Iran's Natanz nuclear facilities in 2010. Since Stuxnet had fooled the computers into thinking that everything was operating normally, it took a human to notice the anomalous sound made by the centrifuges that were rotating much faster than normal.[146]

Principle 5: To reduce the risk of moral hazard, the use of AI-assisted UAVs should be overseen by an independent and impartial review board that would be tasked with keeping track of trends pertaining to the use of this technology and offer guidance when it deems it is deployed excessively. Clear, objective, and measurable indicators would also have to be laid out by the review board to assess what qualifies as a "reasonable" or "excessive" use of UAVs.

---

[143] This principle could also be extended to the designing of the algorithms contained in the AI-assisted UAV. Active oversight of the design phase could help ensure that the algorithms themselves are not affected by underlying biases.

[144] Boulianne Gobeil & Antebi, *supra* note 35.

[145] *Ibid* at 123.

[146] See *Zero Days*, Directed by Alex Gibney (New York, NY: Magnolia Pictures, 2016).

This final principle is worth laying out because the military advantages that state-of-the-art technology provides its users with may create a risk of moral hazard.[147] The use of UAVs is particularly prone to such moral hazard. This is because the low political costs of using UAVs to conduct military operations make it more palatable for military and political decision-makers to deploy in areas that would otherwise be inaccessible such as Pakistan's FATA. The ensuing risk is that UAVs will be deployed more including in situations where their user would not have dared venture had UAVs not been an alternative. The moral hazard thus leads to what could be regarded as a military overstretch. To paraphrase the hammer and nail adage, when you have a fleet of AI-assisted UAVs, everything looks like a terrorist. Thus, oversight becomes a crucial component of a legal regime governing the use of this technology.

While a board adds a bureaucratic step, this additional measure is unlikely to slow down the military execution of any given strike because by overseeing the use of UAVs at the macro level, it avoids the impediment of including one more step in the decision-making process *before* the strike is taken. Military swiftness is not impacted by adding a step *after* a military decision has already been taken. Finally, this board could be the forum for an eventual judicial review of a military lawyer's decisions to strike.

VII. CONCLUSION

America's use of UAVs to conduct counterterrorism missions, which has increased in the last decade and a half, makes it unlikely that the technology will disappear anytime soon. The US' reliance on the 2001 AUMF to carry out targeted killings offers a weak and overstretched legal foundation at best. At worst, it sets a dangerous precedent for the kind of legal arguments other States are likely to articulate as they develop the technological might to deploy their own fleets of UAVs. The US therefore stands to benefit from adopting a new legal framework that builds on the above five principles. Admittedly, the US might not want to be bound by a more constraining legal framework unless other actors do so as well. That said, the European Convention on Human Rights, which imposes an "absolute prohibition on the intentional deprivation of life",[148] represents a more restrictive framework than the AUMF. Thus, the use of UAVs by Member States of the Council of Europe, several of whom are US allies, is

---

[147] See Kaag & Kreps, *supra* note 13.

[148] Adam Bodnar & Irmina Pacho, "Targeted Killings (Drone Strikes) and the European Convention on Human Rights" (2012) 32 Polish Yearbook of International Law 189 at 201.

already more restrained than the US is by its own legal framework. Even so, by following this article's principles, the US would set an example for States who may not yet possess UAVs, but that are likely influenced by the way the US currently uses them.[149] Moreover, given the several incentives to remove human beings from the decision-making process that precedes targeted strikes, combined with ongoing progress in the field of machine learning, a framework that would govern the deployment of AI-assisted UAVs in targeted killing missions is becoming more and more pressing.

This article has sought to contribute to the articulation of such a framework, proposing five guiding principles that could inform its eventual drafting. These principles are based on current regulation pertaining to the testing of self-driving cars, vehicles that are in large part equipped with the same technologies that would be contained in AI-assisted UAVs. The above five principles are by no means comprehensive, but seek to begin a conversation about the kind of legal framework under which AI-assisted UAVs should be allowed to operate while keeping in mind the laws of war. More voices need to be brought into this conversation. Policymakers, legislators, and scholars could continue to draw comparisons with the automobile industry, which is an area that is likely to see further legislation as the presence of self-driving cars on public roads becomes increasingly apparent. Once the Senate will have passed the SELF DRIVE Act, or an amended version of it, states are likely to begin enacting (or modify) their own regulations to follow Congress' lead. When this happens, the ground for further research will be fertile. Meanwhile, more research can be done on the possible application of machine learning in UAV missions. The more tangible those applications become, the easier it should be to conceive of the rules that ought to regulate them.

[149] The number of States possessing UAVs that have capabilities equivalent to the Predator and Reaper is quite small relative to the number of States that are likely to acquire comparable technology. The US would be prudent not to use its own UAVs in a way that it might not want to have them used against it. See Sarah Kreps & Micah Zenko, "The Next Drone Wars: Preparing for Proliferation" (2014) 93:2 Foreign Affairs 68 at 68.