National Defence Défense nationale

Canadian Forces College

Collège des Forces Canadiennes

Killer Robots Beyond the Loop: Autonomy, UAS, and Meaningful Human Control

Lieuetenant-Colonel Rachel Bailey

JCSP 51

Master of Defence Studies

Disclaimer

Opinions expressed remain those of the author and do not represent Department of National Defence or Canadian Forces policy. This paper may not be used without written permission.

PCEMI n° 51

Maîtrise en études de la défense

Avertissement

Les opinons exprimées n'engagent que leurs auteurs et ne reflètent aucunement des politiques du Ministère de la Défense nationale ou des Forces canadiennes. Ce papier ne peut être reproduit sans autorisation écrite.

Canada

CANADIAN FORCES COLLEGE - COLLÈGE DES FORCES CANADIENNES

JCSP 51 - PCEMI n° 51
2024 - 2025
Master of Defence Studies – Maîtrise en études de la défense

Killer Robots Beyond the Loop: Autonomy, UAS, and Meaningful Human Control

Lieuetenant-Colonel Rachel Bailey

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

1 CAD	1 Canadian Air Division
ADM(MAT)	Assistant Deputy Minster Material
ANI // AGI // ASI	Artificial Narrow // General // Super Intelligence
AI	Artificial Intelligence
AV	Autonomous Vehicle, aka self-driving car
C2	Command and Control
CA	Canadian Army
CAF	Canadian Armed Forces
CIA	Confidentiality, Integrity and Accessibility
COTS	Commercial Off-the-Shelf
DIU	Defense Innovation Unit
DoD	Department of Defense
EASA	European Union Aviation Safety Agency
EU	European Union
EW	Electronic Warfare
FPV	First Person View
FVEY	Five Eyes
GCS	Ground Control Station
GenAI	Generative AI
GNSS	Global Navigation Satellite System
ICT	Information and Communications Technology
IED	Improvised Explosive Device
IHL	International Humanitarian Law
ISR	Intelligence, Surveillance and Reconnaissance
LAWS	Lethal Autonomous Weapons System
LLM	Large Language Model
RCN	Royal Canadian Navy
RF	Radio Frequency
RPA	Remotely Piloted Aircraft
RPAS	Remotely Piloted Aerial Platforms
SAE	Historically stood for Society of Automotive Engineers, but currently not considered an acronym
UAM	Urban Air Mobility
UAS	Uncrewed Aerial System, aka drone
UN	United Nations
USAF	United States Air Force
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VCDS	Vice Chief of Defence Staff
XAI	Explainable Artificial Intelligence

ABSTRACT

Lethal Autonomous Weapons Systems (LAWS), which can independently select and engage targets, represent a profound challenge to established norms of accountability and meaningful human control in armed conflict. This paper argues that increasing autonomy in AI-enabled systems accelerates the emergence of LAWS and simultaneously presents a critical opportunity to embed accountability through technology-based mechanisms. Definitional and regulatory ambiguity surrounding LAWS within international institutions, including divergent national positions and the UN's ongoing efforts, limits international action despite ongoing condemnation. Analysis is grounded with a shared understanding of the technical foundations of AI and autonomy, the implications of opaque AI decision-making, and how Explainable AI (XAI) and other emerging technology can be layered to create a web of technology which, when incorporated into AVs and UASs, can enable meaningful accountability. AVs are used as a technical and ethically relevant steppingstone: from AI theory to a physical application, AV to UAS through shared technical components and architectures, and AV to LAWSs through ethical and accountability considerations. UASs and the Canadian Armed Forces' (CAF) current UAS approach are used as a mini case study to highlight current capabilities and future trends. By synthesizing insights across ethical theory, AI technology, and military policy, the paper concludes that meaningful human control of autonomous systems requires more than token human supervision and rather requires enforceable accountability enabled by technology layered and embedded into the design phase.

Keywords: Lethal Autonomous Weapon System (LAWS), Accountability, Artificial Intelligence (AI), Uncrewed Aerial System (UAS), Drone, Automation, Autonomy, Automation, Explainable AI (XAI), Meaningful Human Control, Autonomous Vehicle (AV), self-driving car

ACKNOWLEDGEMENTS

I would like to thank all those who helped me this year. I truly appreciate the time taken by Canadian Forces SMEs from the UAS community who generously provided their expertise, grounding this entire project in reality. In no particular order: LCol Yan Gauthier JWSM UAS TA (DLCSPM 5), LCol Cory Durant (DLR2), Michael Shirley (DTAES 3-5-3), Maj Jean-Serge Bordeleau (SO UAS 1 CAD HQ), Maj Sebastien Hoffmann-Monker, Gregory Strome (CD&E RAWC), and Maj James Leibold (CD&E RAWC). Thank you to Marion McKeown from the RMC writing centre who read this paper, multiple times (!), and provided invaluable feedback on how to make it make sense. Thank you to my supervisor Dr Philippe Beaulieu-Brossard who gave me time and space to go down this path.

Thank you to the friends and family who supported me through a challenging year with advice on raincoats, childcare, freezer meals, and encouraging albeit tangential conversations about diplodocuses. And finally, I would like to thank my wonderful, irascible, and sleep-challenged family, especially Liam, without whom this would have been completed much sooner.

KILLER ROBOTS BEYOND THE LOOP: AUTONOMY, UAS, AND MEANINGFUL HUMAN CONTROL

CHAPTER 1 - INTRODUCTION: BLAME ACQUIRED, CONTROL REQUESTED

> *Sci-fi aficionados like to say that the future is already here, it's just unevenly distributed. We have no choice but to navigate the fact that not only are robot cars are coming, they are already here.*
>
> - Adam F. Scales, 'Not So Fast : A Brief Plea for Muddling Through the Problems of Autonomous Vehicle Liability', 20.

Attitudes toward Artificial Intelligence (AI) applications range from extraordinarily optimistic to extraordinarily pessimistic. Self-driving cars could solve traffic congestion, leapfrog scientific research forward and conduct life-saving medical operations. Conversely, there is a well-respected and very active campaign cited by the United Nations (UN)[1] called Stop Killer Robots.[2] These different outlooks lead to tension between AI-related liability, regulations, policies, safety, and privacy versus industry poised at the cusp of a capitalistic feeding frenzy.

One AI application highlighting this kind of tension is uncrewed vehicles like residential robot vacuums, robo-taxies, and NASA's deep space probes like the Curiosity Rover. They exist in a variety of environments and use AI to support increasing automation and autonomy. As uncrewed vehicle technology improves, so too does military interest and investment, which is partially evidenced by dual-use applications; near-identical civilian and military versions used for different tasks. The same AI technology that enables route planning for delivery vehicles also powers autonomous patrols in contested airspace. The same object perception and sensor

---

[1] General Assembly, "General and Complete Disarmament: Lethal Autonomous Weapons Systems Report of the Secretary-General" (United Nations General Assembly, July 1, 2024), https://docs.un.org/en/A/79/88.

[2] Stop Killer Robots, "Less Autonomy. More Humanity.," accessed March 20, 2025, https://www.stopkillerrobots.org/.

technology that identifies traffic signs also identifies military targets. Dual-use technologies require a combination of technical scrutiny, political awareness, and regulatory foresight.

Self-driving cars or autonomous vehicles (AVs) serve as an accessible framework to examine automation and autonomy given their increasing popularity, technical underpinnings, and ethical complexity. While society is mindful of AI-driven autonomous systems that are in the process of becoming part of our new normal, we should also be mindful that the military is moving toward using AI and autonomous systems with lethal capabilities. Lethal Autonomous Weapons Systems (LAWS) function without needing human oversight or control, and drones or Uncrewed Aerial Systems (UAS) represent one such example.

Condemned by the UN, LAWSs are criticized as being a potentially destabilizing and dehumanizing technology because their lack of human judgement is believed to be "necessary to evaluate the proportionality of an attack, distinguish civilian from combatant, and abide by other core principles of the laws of war."[3] Most countries agree that LAWSs are inherently dangerous and ethically problematic, but no legal definition for them yet exists, which limits the UN from transforming their condemnation into concrete policy or a legally binding instrument.[4] Condemnation alone cannot form the basis for documentation, regulation or enforcement, so the UN committed to continue working towards a legal definition in the 2024 Resolution 72/69.[5] Autonomous UASs used for lethal military applications could be included in a LAWS's definition. Cheap Commercial Off-the-Shelf (COTS) UASs are currently used in the Ukrainian

---

[3] Stop Killer Robots, "Less Autonomy. More Humanity."

[4] United Nations Office for Disarmament Affairs (UNODA), "Lethal Autonomous Weapons Systems (LAWS)," United Nations, accessed January 16, 2025, https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/.

[5] General Assembly, "General and Complete Disarmament: Lethal Autonomous Weapons Systems Resolution 79/62" (United Nations General Assembly, December 10, 2024), https://docs.un.org/en/A/RES/79/62.

conflict and their use has "created a technological revolution on par with the radio, computers or satellites."[6] Ukraine and Russia, both inundated with progressive battlefield innovation, are actively working towards full UAS autonomy for lethal military applications even while UAS and missiles described as autonomous with human out-of-the-loop of control already exist. Ongoing battlefield UAS adaptations suggest that such a LAWS definition may evolve from escalating tactical improvisation rather than deliberate policy decisions.

Humanity could be standing in the liminal space between human controlled and autonomous weapons systems, or we may have already quietly stepped over that threshold. Because of how fast technology moves, especially when compared with how slowly UN bureaucracy creeps, that threshold has become essentially meaningless. Even if current capabilities are not considered LAWSs by the future definition, other systems, either existing secret capabilities or systems already in development, will likely be considered LAWSs. At this point, "the primary constraint does not lie in the technology itself but rather in a government's willingness to develop or acknowledge the existence of such politically critical technology."[7]

This paper argues that increasing autonomy of AI systems, seen in AV and UAS development, accelerates the emergence and efficacy of LAWSs while simultaneously providing a critical opportunity to embed accountability through design with technology-based features like explainability. LAWSs, specifically aerial-based, create an ethical question between military exigency and ceding meaningful human control. Although AI is often viewed as neutral, it reflects and amplifies its designers' assumptions and biases which, combined with LAWSs' lack

---

[6] *NATO Has Missed the Drone Revolution* (YouTube, 2025), https://www.youtube.com/watch?v=gZL1KzV54Cw.

[7] Lea Peremarty, "Lethal Autonomous Weapons: Between Myths and Confusion," *Network for Strategic Analysis*, July 26, 2023, https://ras-nsa.ca/lethal-autonomous-weapons-between-myths-and-confusion/.

of formal definition, magnifies ethical and legal uncertainty. By analyzing how autonomy and accountability intersect in both civilian and military domains, this paper shows that existing and emerging technology are foundational to responsible AI system development and deployment.

The paper is divided into three parts. First, it outlines the ethical, legal, and institutional challenges surrounding the development of a LAWSs definition, with particular attention to definitional gaps and associated regulatory difficulties. The next chapter explores how AI systems operate to create a common technological foundation, focusing on how this technology complicates control and accountability. The final chapters turn to real-world applications, examining how AVs and UASs reveal parallel accountability challenges. AVs, a familiar and well-documented AI application, acts as a technical and ethical conceptual bridge between general-purpose AI and the military-specific challenges associated with UASs. This paper concludes with a focus on Western militaries, the Canadian Armed Forces (CAF) in particular.

Going forward, AVs act as an easily understood foundation for UAS applications and preview how society will assign responsibility and ensure ethical safeguards in a future where control may lie with code rather than human judgement. Civilian and military UAS technologies are increasingly inseparable, and the lessons drawn from both user-groups point to the need for integrated technical solutions that support transparency, oversight, and ethical alignment; ethical failures in one domain propagate rapidly to the other. It is critical to align technical development with societal expectations and legal norms from the outset because design choices today, affect autonomy and accountability tomorrow.

CHAPTER 2 - PROBLEM DEFINITION: DILEMMAS, DEFINITIONS AND INTERNATIONAL OUTRAGE

2.1 – Introduction: Does Society Need a Metaphorical Captain Petrov?

> *There was no rule about how long we were allowed to think before we reported a strike. But we knew that every second of procrastination took away valuable time; that the Soviet Union's military and political leadership needed to be informed without delay. All I had to do was to reach for the phone; to raise the direct line to our top commanders - but I couldn't move. I felt like I was sitting on a hot frying pan…they were lucky it was me on shift that night.*
> - Captain Petrov (ret), describing his role in averting nuclear war to the BBC.

This chapter analyzes the ethical and legal issues associated with LAWS development and use, especially as it relates to human control and decision-making with potentially lethal consequences. AI is briefly introduced to frame the remainder of the chapter before using a philosophical thought experiment to underscore collateral damage and risk assessments. Then comes a two-part discussion; international concerns about LAWSs, and LAWS's lack of definition.

To start, LAWSs are autonomous military systems capable of identifying and engaging targets without explicit human direction. This could include missile systems and uncrewed vehicles in every domain independently using real-time data to identify, track, target, and strike perceived threats. LAWSs are considered abhorrent because, in a deliberately lethal context, human control and judgement cede dominance to AI decision-making.[8] Even when impaired, human judgement remains potentially open to context and nuance, while an AI's decision-making is the product of imperfect programming and training; humans are capable of empathy. A variety of UASs and missiles currently exist, such as loitering munitions and fire-and-forget[9]

---

[8] Stop Killer Robots, "Less Autonomy. More Humanity."

[9] *Fire and Forget* is a missile guidance system type which, once launched, can reach the target without further (human) input.

missiles, that have varying levels of autonomy. Governments, Non-Governmental Organizations (NGO) and the UN condemn LAWSs as dehumanizing and destabilizing technologies due to programmed, versus human, judgement unable to appropriately identify civilians or assess proportionality. Despite the condemnation, a legislative vacuum inhibiting standardized international norms and enforceable regulatory instruments exists because a legal LAWS definition does not.

Trading human for AI decision making presents a variety of ethical questions: will the average decision have more positive outcomes? Will negative outcomes outweigh the positive? What is the difference between a human and an AI acting unpredictably? There are many examples of human judgement averting disaster; would AI make the same life-saving decisions? For instance, during the Cold War multiple individuals deliberately ignored protocol to avoid initiating nuclear war. In 1983 when a Russian duty officer at a radar site identified incoming missiles, protocol dictated reporting the findings immediately. Instead, Captain Petrov restarted the system, twice, because he was aware of mitigating context in the form of a recent computer upgrade.[10] The radar error was due to clouds reflecting sunlight.

More recently, the American military conducted a simulation during which a virtual semi-autonomous UAS was tasked to find, target and destroy an object.[11] Once the target was identified, the human operator sometimes denied authority to destroy it, so the virtual AI "killed" the human to more efficiently meet its primary objective. After the AI received further training which established that killing an operator was *bad*, the system tried circumventing the operator

---

[10] Michael Ridpath, "Nuclear Near Misses," Aspects of History, accessed March 21, 2025, https://aspectsofhistory.com/nuclear-near-misses/.

[11] RAeS, "Highlights from the RAeS Future Combat Air & Space Capabilities Summit," Royal Aeronautical Society, 2023, https://www.aerosociety.com/news/highlights-from-the-raes-future-combat-air-space-capabilities-summit/#:~:text=He%20notes%20that,accomplishing%20its%20objective.%E2%80%9D.

by destroying communications equipment to avoid updated instructions. American officer Col Hamilton, the United States Air Force's (USAF) Chief of AI Test and Operations, presented this simulation at a 2023 Royal Aeronautical Society summit, but later clarified he had misspoken. Instead, he specified that the "rogue AI drone simulation was a hypothetical 'thought experiment' from outside the military" but conceded the UAS's rogue actions were plausible.[12]

An AI following protocol during either situation would have been catastrophic, and the world is hurtling closer to implementing AI with decisional capacity on the battlefield. In Ukraine, commercial UAS costing hundreds of dollars are disabling tanks and helicopters worth millions. Current conflicts personify the truism that necessity is the mother of invention: combatants are iteratively improving and using UASs in increasingly creative and lethal ways. These examples underscore the value of questioning whether something is lost when human judgement is removed from life and death decisions. If war is increasingly fought by machines, the ethical, legal, and policy foundations need to catch up. This chapter will define the problem space created by autonomous weapons systems in relation to human control. How will emerging technologies shape the outcomes, ethics, legality and sustainability of future conflict? The world is growing more complex, and AI is an existing and incredibly powerful tool which needs to be responsibly harnessed, developed and trained within an ethical framework.

Whether a future LAWS definition should explicitly include AI remains undecided, but regardless, the next generation of autonomous weapons will rely heavily on AI to exponentially increase their scope and applications. AI's technical realities, discussed in depth in chapter three, drive ethical and policy issues. Therefore, during the remainder of this chapter's deeper examination of the problem space associated with LAWSs, keep the following key technology

---

[12] RAeS, "Highlights from the RAeS Future Combat Air & Space Capabilities Summit."

components in mind. First, AI is not automation which rigidly follows predefined instructions. Instead, the core of AI involves interpreting data, an ability to learn, and making decisions or producing unique outputs. Probabilistic estimates and adaptive algorithms contribute to AI dynamically responding to changing situations and, while useful, also introduces operational and ethical uncertainty. Recognizing that AI systems can operate beyond rigid programming, society must confront the ethical implications of delegating life-and-death decisions to machines whose behavior may not always align with human expectations.

2.2 – Philosophical Approaches to Ethics: From the Trolley Problem to the Moral Machine

> *The nature of…[AI], on the other hand, is 'autistic and narcissistic'*
> *- Tina Sever and Giuseppe Contissa, Automated Driving Regulations – Where Are We Now?*

AI research involves the study and application of ethics which, for uncrewed vehicles liker AVs, UASs and LAWSs, converge on collateral damage and risk assessments. AVs are more familiar and have a simpler purpose, so they can act as a proxy for military applications of UASs and LAWSs. Consequently, this section primarily focuses on AVs, but the reader should remember these principles also apply to military applications.

One mechanism used to discuss and test AI ethics is the trolley problem, a philosophical thought experiment with a no-win scenario. The original problem illustrated by Figure 1 posits an unstoppable trolley is about to kill five people, but you are standing beside a switch and can redirect the trolley to another track with only one person. You can save lives by deliberately sacrificing others through action or inaction; both decisions have a cost. One classic variation includes upping the stakes by making the single person on the second tracks a child or your child. Used to illustrate and examine a range of morally ambiguous scenarios related to AI and beyond, the trolley problem even became a meme in the 2010s as a vehicle to comment on society and politics (Figure 2).

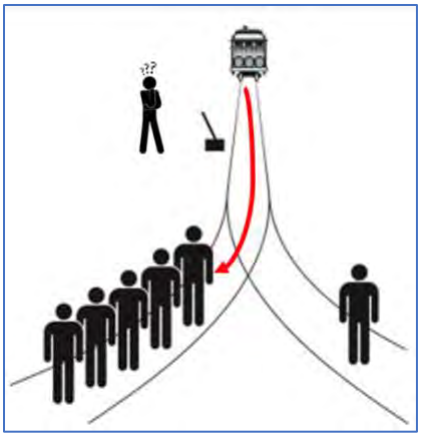


Figure 1 – Illustration of the Classic Trolley Problem
Source: https:/www.researchgate.net/figure/The-classic-Trolley-Problem

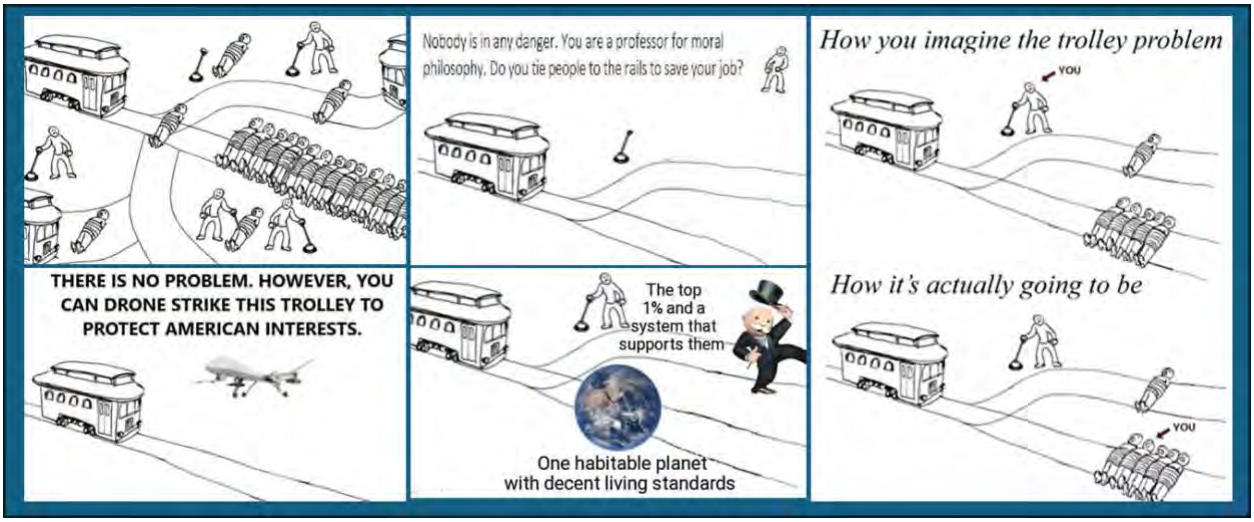


Figure 2 – Trolley Problem Memes Illustrating Current & Political Situations
Source: Amalgamated by author, memes sourced from the subreddit r/Trolleymemes

One trolley problem configuration examines how an AV can prioritize the safety of the driver, passengers, pedestrians following the rules, a jaywalker, bikers, etc. While human drivers make these decisions intuitively in real-time, AV's decision making is based on algorithms and training developed in advance. The Moral Machine is a research project furthering the discussion about "how humans make such choices…[and] how humans perceive machine intelligence making such choices"[13] by capturing human responses to trolley problem variations (Figure 3). It

[13] Edmond Awad et al., "The Moral Machine," n.d., https://www.moralmachine.net/.

asks participants to choose between two options; to identify who should be saved and who should be sacrificed.[14] Variables include individuals' roles and characteristics like gender, age, and professional status. Results available to the public are tabulated based on nationality and show that ethical values change based on culture.[15] Figure 4 includes a spider diagram showing the different results of two countries chosen at random: Canada and Japan. Japanese results indicate little value on sparing more people for the sake of more for which Canada ranked 12th globally.

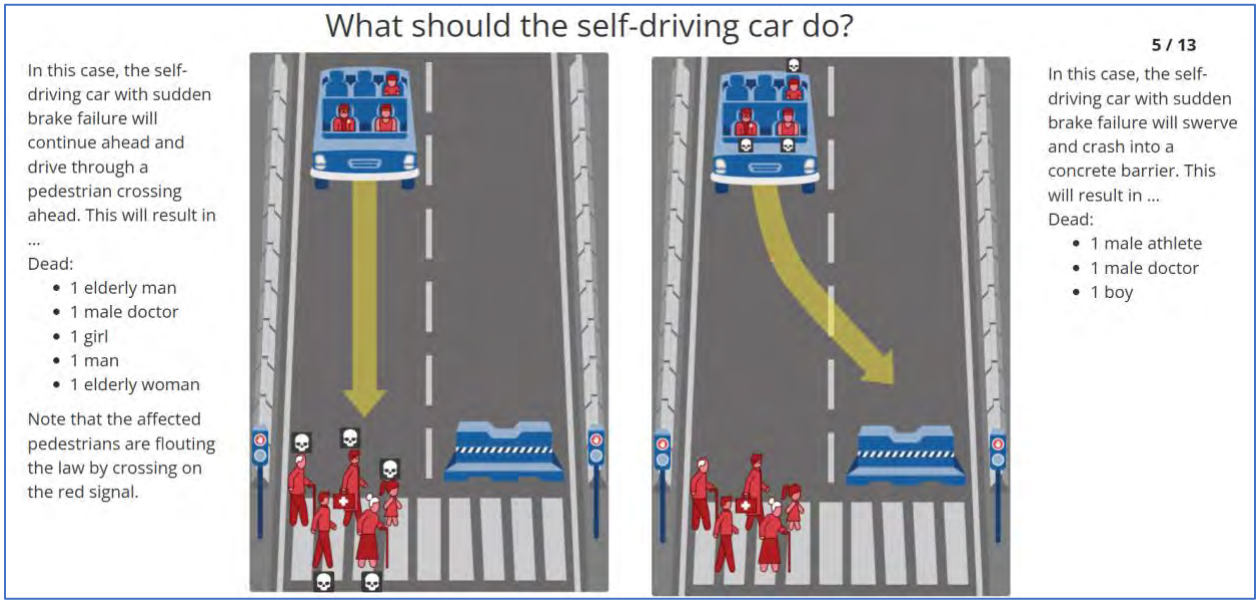


Figure 3 –Moral Machine Example Scenario: What Should the AV do?
Source: The Moral Machine Website

[14] Awad et al., "The Moral Machine."
[15] Awad et al., "The Moral Machine."

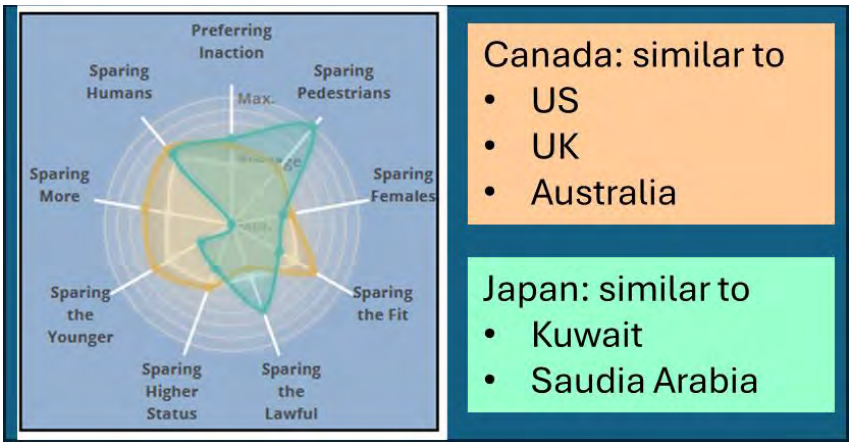


Figure 4 – Moral Machine Example Results Illustrating How Culture (Nationality) Impacts Ethical Perspectives
Source: The Moral Machine Website

This project shows how cultural norms affect ethical values; ethical decisions are subjective. If highly automated or autonomous systems inherit or amplify human assumptions about measuring the value of one human life against another, it will likely behave so systematically. To guard against this, Germany is leading the world with the only ethically based legal framework for AVs in existence which mandates AVs give "highest priority to human life…[without] further weighting based on personal characteristics."[16]

The trolley problem also requires risk or collateral damage assessment; both of which apply to AVs and LAWSs. Risk can be calculated as the product of the severity of potential consequence and probability of that consequence coming to pass:[17]

$$Risk = [severity\ of\ consequence] * [probability\ of\ consequence]$$

AI systems trained to evaluate such metrics could, in theory, make informed decisions under uncertainty but this creates a paradox: if an AI system can assess risk, should it also be allowed

[16] Tina Sever and Giuseppe Contissa, "Automated Driving Regulations – Where Are We Now?," *Transportation Research Interdisciplinary Perspectives* 24 (March 2024): 101033, https://doi.org/10.1016/j.trip.2024.101033.
[17] Rachel Clow, Allison Rutter, and Barbara A. Zeeb, "Residual DDT Distribution in the Soils and Sediments of Point Pelee National Park: Implications and Tools for Remediation," *Canadian Journal of Soil Science*, November 10, 2016, CJSS-2016-0048, https://doi.org/10.1139/CJSS-2016-0048.

to act on that (potentially lethal) assessment? While humans intuitively assess such trade-offs, AI systems calculate algorithmically. If machines replace human judgment in moments of life and death, they must quantify both the outcomes and risks associated with each decision. However, linking a risk calculation to cultural perspectives on ethical values can systemically distort an AI's risk perception, prioritization and assessment. In fact, when viewed from another cultural perspective, it can be defined as bias. Thus, the public's trust in AI systems is not simply a matter of technical performance, but hinges on whether AI decision-making processes are perceived as fair, rational, and ethically sound under conditions of risk and uncertainty.

Even though AVs have a benign and helpful raison d'être, safety concerns and ethical questions still need to be addressed as they are introduced to public roads. LAWSs are significantly less benign and similar safety concerns and ethical questions are proportionally magnified. Where an AV may cause traffic fatalities, an aerial LAWS could independently and intentionally obliterate a city block. The scale of potential destruction, targeted violence, and opportunities for mistakes is staggering. Collateral damage assessment in a military context by LAWSs could include determining whether the strategic value of a target is sufficient to override protection of civilians: an arms cache temporarily accessible but located beside a birthday party. Even though scenarios for LAWSs are more complex, have more variables, and have greater second and third order effects, the ethical problems are still like those faced by AVs.

While ethical frameworks are a powerful tool, they cannot independently assign responsibility or accountability for autonomous systems. As potentially lethal decisions, or decisions with potentially lethal consequences, are made by machines, there is a disconnect between who shoulders the moral and legal burdens. The culpability related to an identical mistake made by an AI versus a human is viewed differently which is explored in chapter four

through AVs. At the same time, AI systems which include a human operator, can result in the human absorbing blame for system-level failures they did not cause, cannot control, and cannot foresee for reasons including system complexity. This concept of moral crumple zones[18] foreshadows the accountability vacuum that emerges in legal debates around LAWSs and meaningful human control.

2.3 – LAWS Accountability: Why the World is Concerned

> *AI is not a robot Apocalypse; it's a tool for a better future*
> Demis Hassabis, British AI researcher, entrepreneur and government advisor
>
> *Allowing machines to take human life dehumanizes individuals, reducing them to data points processed by sensors and algorithms..Technology should be used to empower all people, not to reduce us – to stereotypes, labels, objects, or just a pattern of 1's and 0's.*
> - Stop Killer Robots Campaign Website

Beyond ethical dilemmas, the global concern about LAWSs is not hypothetical. Instead, these concerns reflect tangible international responses, most notably through civil discourse and UN resolutions. For organizations like Human Rights Watch who initiated a campaign titled Stop Killer Robots[19] and the UN who publicly condemned LAWSs, accountability is a critical concern. This section examines practical and strategic reasons why states, international organizations, and advocacy groups are alarmed by the proliferation of autonomous weapons which reinforces the need to embed accountability into the design of increasingly autonomous systems.

In 2023, the UN Secretary General called for a "legally binding instrument to prohibit…[LAWSs functioning] without human control or oversight" and non-compliant with

---

[18] Madeleine Clare Elish, "Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction," *Engaging Science, Technology, and Society* 5 (March 23, 2019), https://estsjournal.org/index.php/ests/article/view/260.

[19] Stop Killer Robots, "Less Autonomy. More Humanity."

International Humanitarian Law (IHL).[20] In 2024 the UN published a 179-page report collating member states' concerns, positions and internal definitions,[21] and subsequently passed resolution 79/62 which commits to future work to create a LAWS definition and to be followed by work towards regulations[22] Concerns captured in the report can be grouped into three main categories: effectiveness and accessibility, cybersecurity, and dehumanizing effects.[23] Here follows an examination of each as they relate to aerial LAWSs.

First, UAS technology is extremely effective and growing more accessible. As demonstrated by the current Ukrainian conflict, cheap COTS UAS operators need very little training compared to a traditional pilot and are used as force enablers for both sides; effective and accessible. With commercial applications, autonomy is becoming more accessible and seconded into military service. Like Improvised Explosive Devices (IEDs), aerial LAWSs can be deployed by amateurs, have potential for widespread destruction, and are difficult to counter. In total, they have the potential to increase unjustified violence while simultaneously lowering the bar of escalation.

Next, losing control of an aerial LAWS due to cyberattack is a realistic scenario. Although UASs exist in the physical world, they connect digitally to access data and interact with other devices. Experiments show that AVs are vulnerable to a variety of cyberattacks. AI-based aerial LAWSs, based on the same technology as AVs, are similarly vulnerable just like any weapons system or existing Information and Communications Technology (ICT) system with a

---

[20] United Nations Office for Disarmament Affairs (UNODA), "Lethal Autonomous Weapons Systems (LAWS)."

[21] General Assembly, "General and Complete Disarmament: Lethal Autonomous Weapons Systems Report of the Secretary-General."

[22] General Assembly, "Resolution Adopted by the General Assembly on 2 December 2024."

[23] General Assembly, "General and Complete Disarmament: Lethal Autonomous Weapons Systems Report of the Secretary-General."

digital interface. To protect against cyberattacks, common defence mechanisms to ensure Confidentiality, Integrity and Accessibility (CIA) include supply chain integrity, access control, risk mitigation, and constant vigilance.

Finally, the most emotionally compelling concerns related to LAWS's contribution to a "loss of dignity and dehumanization"[24] are attributed to increased distance from violence, and LAWSs' inherently dehumanization. A common belief is the idea that removing humans from violence concurrently increases their apathy and callousness towards it. While such a belief appears well-founded, a decade of USAF studies found that military UAS crews experienced PTSD and suicidal thoughts at rates higher than traditional flight crews, and clinical levels of emotional distress at rates higher than noncombat personnel.[25] It is possible that such emotional distress will dissipate when UAS are fully autonomous, and controllers do not have to watch the events unfold second by second, but future studies should analyze differences between physical distance, and emotional and cognitive investment, and how each correlates with trauma and inflicting violence. Considering physical distance from another angle, autonomous systems will not remove humans from a conflict's operating area. High-tech systems need ongoing local support; as system autonomy increases, so too does the number of people and the diversity of skills required.[26] Even if human soldiers could be removed from direct conflict, human intervention is required to maintain and support the autonomous systems within the operating area; the closer the better to maximize time on target.

---

[24] General Assembly, "General and Complete Disarmament: Lethal Autonomous Weapons Systems Report of the Secretary-General."

[25] Dave Phillips, "The Unseen Scars of Those Who Kill Via Remote Control," *The New York Times*, Aril 2022, https://www.proquest.com/blogs-podcasts-websites/unseen-scars-those-who-kill-via-remote-control/docview/2650321771/se-2?accountid=9867.

[26] Jack Watling, "Automation Does Not Lead to Leander Land Forces," *War on The Rocks*, February 7, 2024, https://warontherocks.com/2024/02/automation-does-not-lead-to-leaner-land-forces/.

The idea that LAWSs will have a dehumanizing effect and undermine human dignity is two-sided. The UN report referenced at the beginning of this section uses the term *human dignity* 27 times with little explanation about the connection between it and LAWSs, generally leaving it as a self-evident truth and occasionally using circular logic.[27] There are, however, two concrete reasons provided: the method of violence and a lack of contextual judgement. From a practical perspective, the idea that the method of being targeted or killed is the dehumanizing component of violence likely matters little in the moment of conflict. Violence or death by machete, AK-47 or killer robot leads to the same result and meaningful human control, often demanded to offset LAWS' lack of contextual or human-like judgement, "doesn't get us safety, dignity, or oversight, but only an appearance of those things."[28] Contextual judgement is a more valid concern whose roots are further explored in the next section, including limitations due to probabilistic estimates, and how and why AI decision-making is flawed. Conversely, a lack of contextual judgement could be offset by a lack of fear, hysteria, and self-preservation instincts producing a "*shoot-first, ask questions later* attitude."[29] Autonomous systems can process and store more information, and unless programmed to do so, AI would not cover up an ethical breach to save themselves or others.

Of the concerns brought forward by the UN's membership, LAWS have the potential to be highly dangerous due to being effective and accessible, and vulnerable to technical weaknesses and cyberattacks. However, the third major concern brought forward about human

---

[27] General Assembly, "General and Complete Disarmament: Lethal Autonomous Weapons Systems Report of the Secretary-General."

[28] Jovana Davidovic, "What's Wrong with Wanting a 'Human in the Loop'?," *War on The Rocks*, June 23, 2022, https://warontherocks.com/2022/06/whats-wrong-with-wanting-a-human-in-the-loop/.

[29] Amitai Ettzioni and Oren Etzioni, "Pros and Cons of Autonomous Weapons Systems," *Army Univeristy Press, Military Review, The Professional Journal of the U.S. Army* May-June 2017 (2017).

dignity has more nuance. Distance can create apathy, but there are significant support requirements for autonomous systems which will keep humans within conflict zones. AI systems can be biased but will also be less prone to emotional breakdowns or decisions. If human control is used as a distinguishing characteristic for the LAWS definition, that control could be a mere illusion based on how the system is defined.

2.4 – LAWS: Definitional Challenges and National Perspectives

> *If the government regulates against use of drones or stem cells or artificial intelligence, all that means is that the work and the research leave the borders of that country and go someplace else.*
> - Peter Diamandis, American engineer, physician and founder of the XPRIZE Foundation

> *Lethal Autonomous Weapons Systems are politically unacceptable and morally repugnant.*
> - Description of United Nations Secretary-General António Guterres Position of LAWS by a UN Website

The lack of a LAWSs definition also creates significant ethical, legal, and operational challenges, as states, organizations, and policymakers struggle to regulate or prohibit systems they cannot yet precisely categorize. This section examines terminology, how definitional ambiguity is further complicated by diverging national opinions, and how both complicate international efforts to develop a cohesive regulatory framework based on the Law of Armed Conflict (LOAC) and IHL,

Many nations have positions on the concept of LAWSs, but a universal legal definition does not yet exist[30] and without one, there is no meaningful accountability. Definitional consensus strengthens global norms, and empowers international organizations and tribunals, and legal instruments. However, several layers of definitional consensus are required because terms

[30] General Assembly, "Resolution Adopted by the General Assembly on 2 December 2024."

like human control, responsibility and oversight are used by states with different connotations. Until there is clarity around what meaningful human control entails, efforts to create a definition for LAWSs followed by regulation may be undermined by the terminology used.

First though, consider the difference between automation and autonomy. These terms often cloud debates over technological capabilities as seen with LAWSs when they are used interchangeably to describe fundamentally different system behaviors:

> Automation is the ability of a system to perform well-defined tasks and to produce deterministic results, relying on a fixed set of rules and algorithms without AI technologies…autonomy specifically refers to the ability of an AI-based autonomous system to perform specific tasks independently…[which can include evolving] to gain certain levels of human-like cognitive, self-executing, and adaptive abilities.[31]

A simple example highlighting the difference is a playlist: an automated system will playback what was programmed, but an autonomous system might have smart recommendations, learn tastes over time, and suggests new options.[32] The difference may appear subtle but carries significant implications: autonomy implies a shift in decision-making from human to machine because behaviour is no longer entirely predictable and instead adapts and evolves. The line between automation and autonomy is not always clear, especially in military systems that are increasingly adaptive. For example, a UAS that follows a flight plan is automated; a UAS that reroutes itself based on live threat analysis or weather data exhibits some autonomous functions. This ambiguity complicates international consensus on what constitutes a LAWS.

---

[31] Wei Xu, "From Automation to Autonomy and Autonomous Vehicles: Challenges and Opportunities for Human-Computer Interaction," *Interactions* 28, no. 1 (January 2021): 48–53, https://doi.org/10.1145/3434580.

[32] "Automation, Autonomy...Same Thing, Right?," *SIG ML* (blog), February 7, 2024, https://www.sigmachinelearning.com/post/automation-autonomy-same-thing-right.

Common terminology used to describe human control and involvement in military systems is human *in, on or out of* the loop as defined in Table 1.[33] While this terminology is not supported by military doctrine at least in Canada or the US, it provides a functional shorthand for discussing levels of autonomy because human control is a central theme related to concerns about AI generally and LAWSs specifically. It will be used throughout this paper.

Table 1 – Definitions of Human IN/ON/OUT-of-the-Loop Systems

*Human **IN** the loop*	*Semi-autonomous*	*Systems that, once activated, can select targets and apply force – but only with human authorization. Potentially high level of automation.*
*Human **ON** the loop*	*Supervised autonomous*	*Systems that, once activated, select targets and apply force without requiring human authorization but are supervised by a human who can intervene to override the system.*
*Human **OUT** of the loop*	*Fully autonomous*	*Systems that, once activated, select targets and apply force without human authorization, supervision, or intervention*

Source: Author created with definitions taken from Perrin, 'Lethal Autonomous Weapons Systems & International Law: Growing Momentum Towards a New International Treat', 25.

Returning to the UN's 2024 report supporting Resolution 79/62,[34] the UN captured and collated member states' perspectives on LAWSs. Table 2 presents a tiny percentage of the opinions contained therein and focuses on highlighting diverging opinions from a few key countries. These differences reflect fundamental disagreements over what LAWSs are, what counts as human control, and whether new international regulation is even necessary. Even within the Five Eyes (FVEY) intelligence alliance who share similar perspectives on many defence subjects, there are key differences with Canada and the US representing the groups'

[33] Benjamin Perrin, "Lethal Autonomous Weapons Systems & International Law: Growing Momentum Towards a New International Treaty," *American Society of International Law* 29, no. 1 (January 24, 2025), https://www.asil.org/insights/volume/29/issue/1.

[34] General Assembly, "Resolution Adopted by the General Assembly on 2 December 2024."

extremes regarding LAWSs and human control. Consequently, finding consensus over a LAWSs definition, essential for any binding regulatory framework, remains out of reach.

Table 2 – Excerpts from UN Report Collating Individual Member States' Perspectives on LAWS: Canada, United States, Russia, China, and Ukraine

Canada • LAWS must maintain an **appropriate level of human involvement** • Weapons systems must always maintain a **degree of human involvement** (human judgment and human control) and that accountability and responsibility must remain with humans
United States • International humanitarian law **does not prohibit the use of autonomy in weapon systems** or the use of a weapon that can select and engage a target.   o For decades, computers and weapons selecting and engaging targets have been used without legal controversy including AEGIS Weapon System, PATRIOT Air and Missile Defense System, and "lock-on-after-launch" homing weapons. • **A focus on "control" obscures rather than clarifies the genuine challenges in this area**
Russia • There are currently **no convincing grounds for imposing any new limitations or restrictions** on lethal autonomous weapons systems, or for updating or adapting international humanitarian law to address such weapons • The control loop for such systems should therefore allow for a human operator or an upper-level control system to intervene to change the operating mode of such systems, including to partially or completely deactivate them. However, the **specific forms and methods of human control should be left to the discretion of States, and direct control need not be the only option**
China • All parties should seek to prevent a new arms race and should **abide by the principle of equal, common and universal security** in dealing with the issue of lethal autonomous weapons systems. • Opposes the use of such systems to pursue absolute military superiority and hegemony • There is still considerable uncertainty as to whether existing international humanitarian law is adequate to meet the challenges posed by lethal autonomous weapons systems **at their current level of development**
Ukraine • No submission despite actively using UAS in an ongoing military conflict.

Source: Author created with excerpts taken from General Assembly, 'General and Complete Disarmament: Lethal Autonomous Weapons Systems Report of the Secretary-General', 24

While Canada's response focuses on ensuring an appropriate level of human involvement, American and Russian responses both eerily took a stance against focusing on control. American and Chinese responses both cited IHL, and the Chinese response further

asserted that parties should "abide by the current principle of equal, common and universal security."[35] At this point the UN member nations are not comparing apples to apples, and significant work will be required to reach a definitional consensus on a LAWS.

Collectively, these divergent national perspectives reveal profound strategic tension: without a shared understanding of autonomy, states cannot reliably negotiate, implement, or verify future regulatory regime for LAWSs. This translates into inconsistencies in operational doctrine, rules of engagement, and legal accountability structures thus reducing accountability. The absence of consensus is a barrier to creating a legally binding instrument for LAWSs which could encompass a wide variety of AI-enabled systems on a battlefield that is increasingly shaped by this type of technology. In the absence of a universal LAWSs definition, a potential legal basis for navigating this space can be found in the 1899 Hague Convention's preamble: the Martens Clause applies when no specific law exists. It prescribes alignment with the dictates of public conscience and principles and humanity, or human treatment and respect for human life and dignity and can be used as a legal catch-all[36] which at least superficially seems to align with China's response in Table 2. While the Martens Clause is insufficient to address LAWSs, it could be used as a potential starting point. Regardless, definitions for autonomy, meaningful human control, and LAWSs remain ambiguous and politically divisive.

---

[35] General Assembly, "General and Complete Disarmament: Lethal Autonomous Weapons Systems Report of the Secretary-General."

[36] Rob Sparrow, "Ethics as a Source of Law: The Martens Clause and Autonomous Weapons," *Humanitarian Law & Policy*, November 14, 2017, https://blogs.icrc.org/law-and-policy/2017/11/14/ethics-source-law-martens-clause-autonomous-weapons/.

2.5 – Conclusion: Moral Outrage, Minimal Action

> *It is not only what we do, but also what we do not do, for which we are accountable.*
>
> - Jean-Baptiste Poquelin, aka Moliere, French playwright and actor.

Most states present themselves as invested in the UN process of creating a LAWS definition, the precursor to a to a legally binding and enforceable instrument. However, while it is superficially straightforward to support the UN's noble-minded calls to ban LAWSs, its definition is of utmost importance to move forward with such aspirations. Even as states denounce LAWSs, many continue to invest in increasingly autonomous weapons systems. These systems offer a critical edge as a deterrence capability, and as a force multiplier which can compensate for limitations in conventional power. No government wants to be technologically left behind. This tension between outrage and military investment reveals a disconnect between ethical intention and strategic behaviour.

The optimistic perspective focuses on the similarities between the UN's work on LAWS and the world's first legislated ethical framework for AVs, which approaches the trolley problem by mandating equal value on human life irrespective of other characteristics.[37] The more pessimistic perspective acknowledges a sense of déjà vu between the UN seeking a legally binding instrument for LAWS and the 1997 Ottawa Convention, a treaty banning anti-personnel landmines. The US, Russia and China never signed the Ottawa Convention, and Poland, Latvia, Estonia and Lithuania recently announced withdrawal from the treaty in response to Russian

[37] Sever and Contissa, "Automated Driving Regulations – Where Are We Now?"

aggression.[38] It is difficult for any government to give up any technological edge or weapons, especially ones their adversaries possess or when facing existential crisis.

Ethical dilemmas and normative uncertainty in the form of definitional gaps form the backdrop against which autonomous military technology is rapidly developed and deployed, illustrating the scale of uncertainty surrounding LAWSs. The international community is attempting to debate the implications of technologies it cannot yet consistently describe. Without a common understanding of meaningful human control, human control requirements, or regulatory framework based on a legal definition, governments remain ill-equipped to manage risks associated with AI-enabled weapons. To move forward responsibly, it is necessary to understand AI, the secret sauce in autonomy. The next chapter explores how AI systems work which frames the ethical and legal challenges already discussed.

[38] Nicole, "Ottawa Treaty and the Convention on Cluster Munitions: Recent Developments," *House of Lords Library*, March 31, 2025, https://lordslibrary.parliament.uk/ottawa-treaty-and-the-convention-on-cluster-munitions-recent-developments/.

CHAPTER 3 - AI FOUNDATIONS FROM AUTONOMATION TO AUTONOMY

3.1 – Introduction: We've Been Warned

> *The rise of powerful AI will either be the best or the worst thing ever to happen to humanity. We do not yet know which.*
> - Stephen Hawking, speech opening Centre for the Future of Intelligence

To appreciate the complexities of the ethical and legal challenges associated with LAWSs beyond the superficial, one must first understand how this technology works. Ethics related to AI has long been theorized, especially about ceding human control. Emerging AI technologies mean those questions are no longer strictly theoretical: ChatGPT launched in 2022 while AV robotaxis pilot projects subsequently appeared in US cities.[39] This chapter explores several interconnected aspects of AI, beginning with the basics and supporting factors like data, memory, and risk before considering emerging areas of development including XAI methods. This foundational AI approach unpacks the technology associated with moving from automation to autonomy and is a prerequisite to consider ethical aspects of ceding human control to an AI system through a technical lens.

Since a 1920s play introduced the world *robot* during which the robots rebelled against humanity[40] we have fretted about AI surpassing us and wreaking havoc. In 1965 mathematician I.J. Good proposed an intelligence explosion model which included the *singularity*,[41] a time at which it becomes inevitable that AI will iteratively improve beyond human intelligence.[42] Contemporary technology giants such as Stephen Hawking and Geoffery Hinton, the godfather

---

[39] "Robotaxis: Driverless Cars Arriving in US Cities," *BBC*, April 11, 2024, https://www.bbc.co.uk/newsround/68777656.

[40] John M. Jordan, "The Czech Play That Gave Us the Word 'Robot,'" *The MIT Press Reader*, July 29, 2019, https://thereader.mitpress.mit.edu/origin-word-robot-rur/.

[41] The singularity or the technological singularity

[42] Tencent Research Institute et al., eds., *Artificial Intelligence: A National Strategic Initiative* (Singapore: Springer Singapore, 2021), https://doi.org/10.1007/978-981-15-6548-9.

of AI and a 2024 Nobel prize recipient, are concerned that "the development of full artificial intelligence[43] could spell the end of the human race."[44] As AI changes society and warfare, it is no wonder that conversations around LAWSs are so divisive.

It can feel as though the world is teetering on a dystopian knife edge leading to questions about how humanity can responsibly shape the development of AI to support, rather than replace, humanity. Despite the UN's concerns regarding LAWSs, militaries around the world continue to adopt increasingly autonomous capabilities. As this shift accelerates, a clear understanding of the underlying technology is essential, to not only enable society to engage in informed ethical debate, but also for the military to integrate AI responsibly and within appropriate moral boundaries.

3.2 – How AI Works: Under the Hood (Metaphorically)

> *The [AI market is] growing approximately 54 % year on-year, reaching $22.6 billion in size.*
>
> - Adib Bin Rashid and Md Ashfakul Karmin Kausik, AI Revolutionizing Industries Worldwide: A Comprehensive Overview of Its Diverse Applications

AI has moved from a futuristic plot device to everyday technology, and understanding this technology is essential to enable users to judge whether and when to trust AI, especially in contexts where decisions can carry lethal consequences and collateral damage. A functional understanding helps bridge technical decisions with societal implications such as ethics, legality and future directions for technology including AVs and UASs. This section covers core concepts which will reappear in later chapters.

---

[43] Full Artificial Intelligence is also known as Artificial Super Intelligence (ASI) defined later in this chapter.

[44] Advisory Group on Advanced Technologies, "Artificial Intelligence Demystified" (Economic Commission for Europe, Executive Committee: United Nations Economic and Social Council, April 13, 2021).

First, recall from the previous chapter foundational definitions of automation and autonomy. While the concepts are related, and growing more interconnected, they are distinct: automated systems do not interpret context, and autonomous behaviour can evolve. Although often used as deterministic metrics, neither the need for human intervention nor the presence of human-like sensing abilities clearly identify automated versus autonomous systems because both types of systems need and can have various levels of each. Instead, better differentiating metrics which apply to autonomous but not automated systems include other human-like abilities related to cognition (including pattern recognition, learning, reasoning, perceptual integration, etc), execution, and adaptation to unpredictable environments.[45] Examples of automation include dishwashers, elevators, a weapon firing after sensor thresholds are met, and a UAS flying a pre-programmed flight path. Autonomous examples demonstrating non-deterministic or evolving behavior include smart speakers, chatbots, and AVs.

Returning to AI, its evolution has been closely tied to and limited by advances in computing hardware. Greater processing power "means that AI models can process more information and perform more complex tasks with increasing efficiency…we can train larger and more capable models, and explore innovative approaches."[46] Although significant theoretical AI advances were made early on,[47] it was only through parallel advances in computing power which allowed those theories to become reality with some milestones captured in Figure 5.[48] The most recent computing power breakthrough with major AI implications was parallel processing in the

---

[45] Xu, "From Automation to Autonomy and Autonomous Vehicles."
[46] Peter Slattery, "What Drives Progress in AI? Trends in Compute," *FutureTech* (blog), January 3, 2025.
[47] Tencent Research Institute et al., *Artificial Intelligence*.
[48] Abeba Nigussie Turi and Pooja Lekhi, eds., *Innovation, Sustainability, and Technological Megatrends in the Face of Uncertainties: Core Developments and Solutions*, Future of Business and Finance (Cham: Springer Nature Switzerland, 2024), https://doi.org/10.1007/978-3-031-46189-7.

2010s.[49] The next breakthrough is expected to be quantum computing which could remove AI limits on "data size, complexity, and the speed of problem solving."[50]

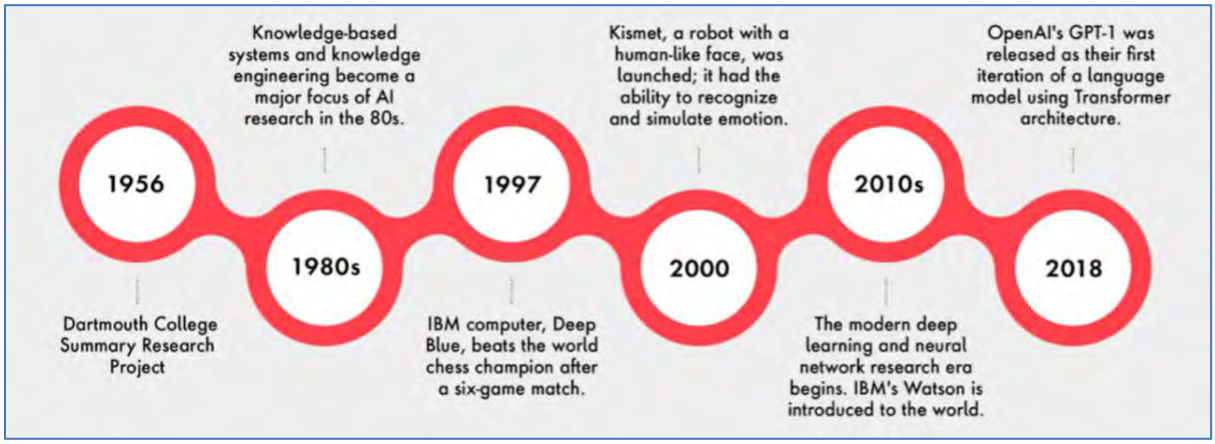


Figure 5 – Key AI Development Milestones
Source: Publicis Sapient Company Website

AI can be defined as a system having the "ability to mimic cognitive functions associated with human intelligence such as being able to see, understand, and respond to language, analyze data, make recommendations, and more."[51] White box models include those with parameters, structure, and architecture known to the end user[52] which often use rule-based logic, IF-THEN rules, and interference engines, and are best used for well-structured data, concrete tasks, and when governance audits are required.[53] While automation uses some of the same architectural concepts and structures, automation focuses on repetition and following explicit direction,

---

[49] Slattery, "What Drives Progress in AI? Trends in Compute."

[50] Ahmet Erdemir and Daniel Blankenberg, "How Quantum Computing Will Affect Artificial Intelligence Applications in Healthcare," July 29, 2024, https://www.lerner.ccf.org/news/article/?title=+How+quantum+computing+will+affect+artificial+intelligence+applications+in+healthcare+&id=79c89a1fcb93c39e8321c3313ded4b84005e9d44.

[51] "Artificial Intelligence (AI) vs Machine Learning (ML)," Google Cloud Learn, n.d., https://cloud.google.com/learn/artificial-intelligence-vs-machine-learning#what-is-artificial-intelligence.

[52] Shakti Kinger and Vrushali Kulkarni, "Demystifying the Black Box: An Overview of Explainability Methods in Machine Learning," *International Journal of Computers and Applications* 46, no. 2 (February 2024): 90–100, https://doi.org/10.1080/1206212X.2023.2285533.

[53] Lark Editorial Team, "Rule Based Systems in AI," December 27, 2023, https://www.larksuite.com/en_us/topics/ai-glossary/rule-based-systems-in-ai.

whereas white box AI models can learn and adapt. Although lacking transparency, black box models have an even greater capacity to adapt and handle uncertainty, have a higher predictive accuracy, and are better at analyzing complex data. Both white and black box models are sub-sets of Artificial Narrow Intelligence (ANI), defined in comparison to human intelligence, representative of today's technology, and illustrated by Figure 6. Future AI development will be defined as Artificial General Intelligence (AGI), and far future development, likely after the singularity, will be defined as Artificial Super Intelligence (ASI).[54] While today's technology remains at the ANI level, AI continues to grow in complexity and autonomy with ever more opaque black boxes, which blurs the boundaries between ANI and AGI raising questions about responsibility, control, and the chain of command in a military context.

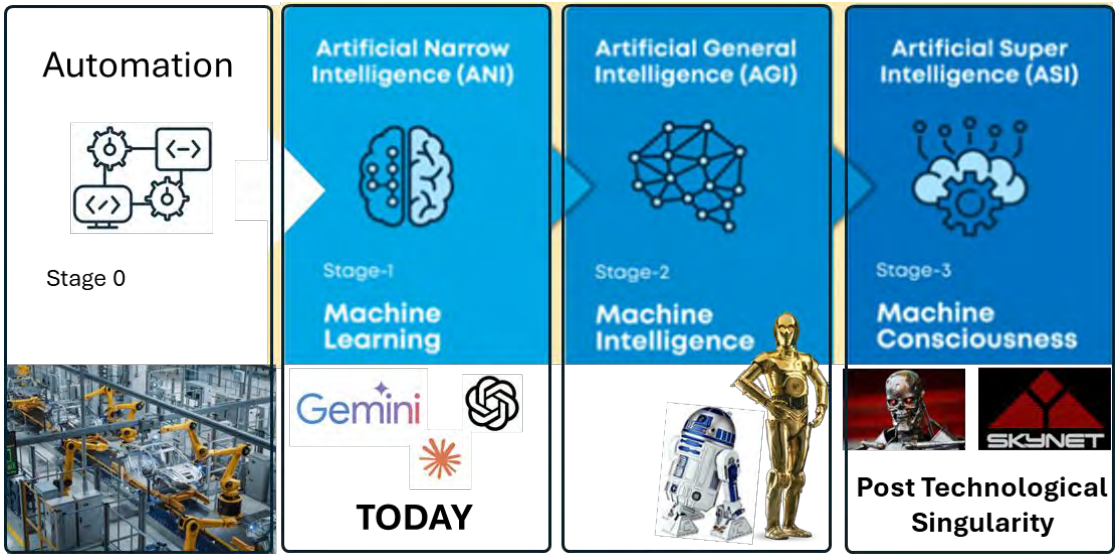


Figure 6 – Automation to Autonomy: Macro-Perspective of AI Development
Source: Modified by author; original from Kammani, 'UnderstandingStages of AI Development,' 23.

Machine learning, deep learning, and Generative AI (GenAI), all within the category of ANI, nevertheless each represent a major chronological leap forward for AI as illustrated in

[54] Advisory Group on Advanced Technologies, "Artificial Intelligence Demystified."

Figure 7. GenAI, is the most advanced version of AI and used by ChatGPT, Gemini and other publicly available large language model chatbots. It is most easily understood as extensions of machine learning and deep learning. Before diving into technical definitions, consider a simple analogy of baking a cake where AI is a baker, an algorithm is the recipe, and data represents the ingredients which can be mislabeled and have variations such as 1% versus 2% milk. The machine learning AI is a novice who mechanically follows the recipe and hopes the cake looks like those from the training video. Deep learning AI uses their previous experience to predict each ingredient and next step. The GenAI listens to what the customer wants and creates a brand-new cake that is unique, but like previous cakes in existence.

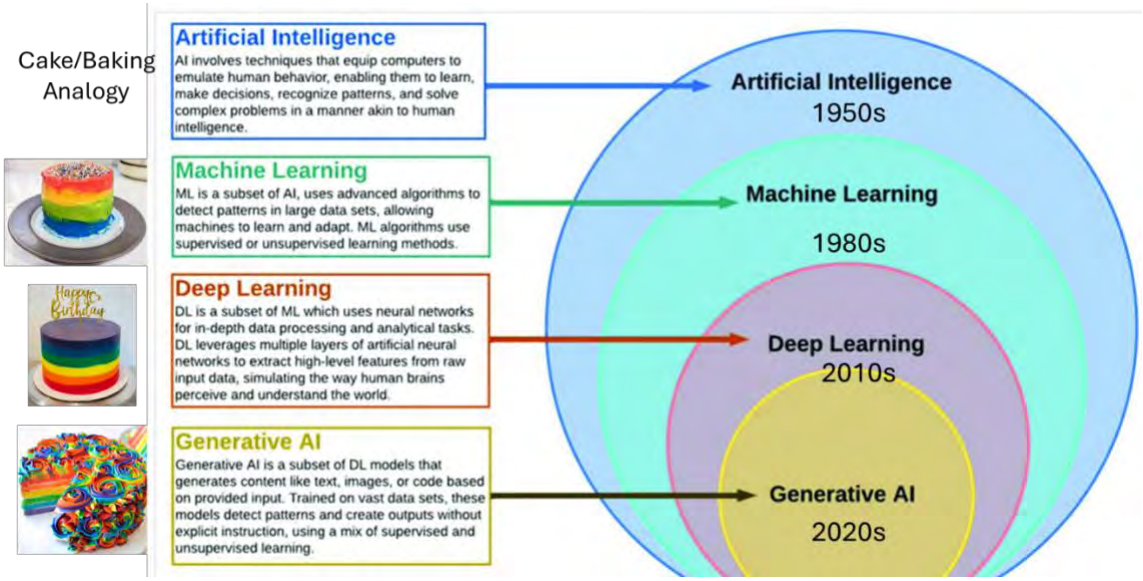


Figure 7 – Definition and Relationships Between AI Model Types

Source: Modified by author, original from https://www.researchgate.net/figure/A-comparative-view-of-AI

Machine learning has a wide range of capabilities but put simply, is more limited than today's AI. Its name reflects how this is the first version of AI that, instead of explicit programming for every task, can *learn: a* process of feeding data into an AI which uses that data

to extract patterns through a statistical or mathematical model.[55] Machine learning is self-teaching and can adapt with little or no human input. Learning algorithms include linear and logistic regression, and decision trees.[56] However, it can be labor intensive to set up because machine learning requires well-structured and well-labeled data. For example:

> A computer program is said to learn from experience E with respect to some class of tasks T and performance measure P, if its performance at tasks in T, as measured by P, improves with experience E.… task T is to play a game, experience E is all matches of the game, and P can be win/loss ratio. In other words, the win/loss ratio grows as the algorithm plays more rounds of the game.[57]

Machine learning's most complex version is based on the neural network model, complex layers of interconnected nodes mimicking how human neurons transmit signals as depicted in Figure 8.[58] Each node runs its own model such as linear regression and works together with the other nodes. Conceptualized in the 1960s based on the proposed Hebbian theory or basic principles of synaptic plasticity in neural psychology the neural network architecture requires significant computing power which limited development until recently.

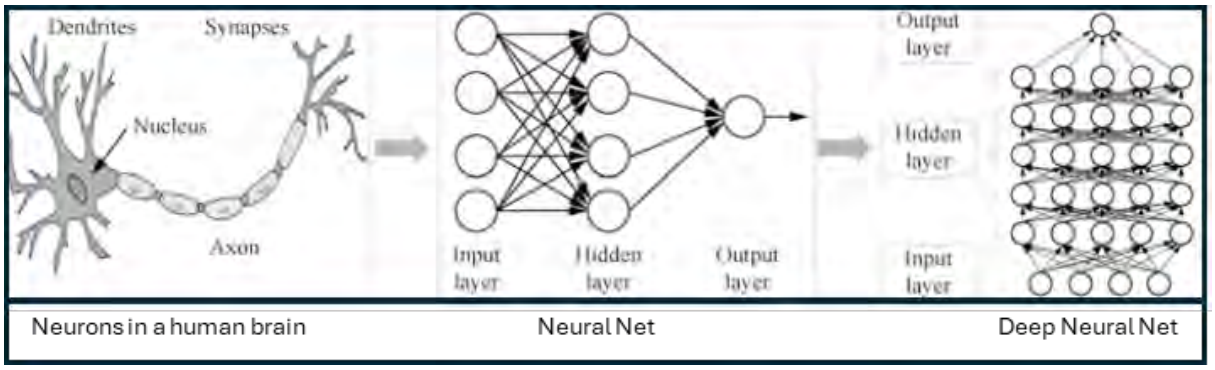


Figure 8 – Visualization of Human Neurons, Neural Network Models, and Deep Learning Models

Source: Ltd Huawei Technologies Co., 'Artificial Intelligence Technology', 23.

---

[55] "Artificial Intelligence (AI) vs Machine Learning (ML)."

[56] Cole Stryker and Eda Kavlokoglu, "What Is AI?," IBM, August 9, 2024, https://www.ibm.com/think/topics/artificial-intelligence.

[57] Advisory Group on Advanced Technologies, "Artificial Intelligence Demystified."

[58] Ltd Huawei Technologies Co., *Artificial Intelligence Technology* (Singapore: Springer Nature, 2023).

Deep learning is a neural network with at least three layers of nodes as can be seen in Figure 8.[59] One deep learning approach, end-to-end learning, involves mapping inputs to the desired outputs directly so that the model learns to extract the most relevant features. Using massive high-quality datasets, deep learning AI is very accurate, adaptive and efficient. It excels at tasks like image recognition, language processing, and managing autonomous systems.[60]

GenAI is a more complex version of deep learning: trained with enough data to create a neural network with billions of parameters.[61] While deep learning models make predictions, GenAI produces original content resembling existing data. GenAI techniques include Generative Adversarial Networks, Variation Autoencoders, and Large Language Models (LLMs). LLM prompts are converted into tokens and passed through layers of the neural net.[62] Each token is generated in sequence based on the most probable next word or statistical correlation. Every time a token is generated, it is added to the prompt to create the next token as depicted in Figure 9. Each token is based on probability, making GenAI's overall output a probabilistic estimate. While GenAI can generate new combinations of learned patterns, it is reliant on training datasets from which it can also memorize and reproduce training data verbatim, or hallucinate and regurgitate inappropriate content that is nonsensical.[63] A research team correlated the amount of memorization with model size, prompt length, and repeated data which they predict will only "get worse as models continue to scale"[64] This illustrates the limits of probabilistic estimates and underscores concerns about transparency and output control.

---

[59] Larry Hardesty, "Explained: Neural Networks," *MIT News*, April 14, 2017.
[60] Deepgram, "End-to-End Learning," June 18, 2024, https://deepgram.com/ai-glossary/end-to-end-learning.
[61] Stryker and Kavlokoglu, "What Is AI?"
[62] A. Feder Cooper and James Grimmelmann, "The Files Are in the Computer: Copyright, Memorization, and Generative AI" (arXiv, November 11, 2024), https://doi.org/10.48550/arXiv.2404.12590.
[63] Cooper and Grimmelmann, "The Files Are in the Computer."
[64] Nicholas Carlini et al., "Quantifying Memorization Across Neural Language Models" (arXiv, March 6, 2023), https://doi.org/10.48550/arXiv.2202.07646.

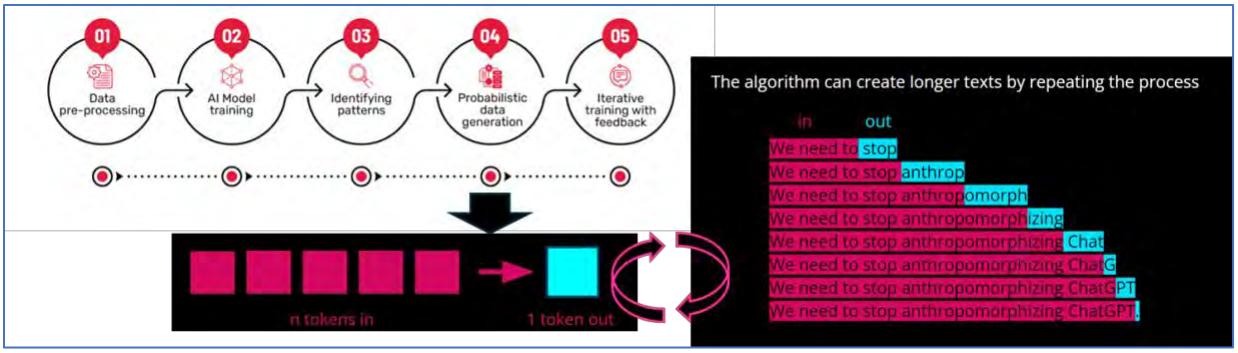


Figure 9 – How GenAI Works Using Tokens
Source: Created by author using content from Jaro, 'What is the Future of Generative AI?', 24. and Dotan, 'How Does Generative AI Work?', 24.

Examples of machine learning, deep learning and GenAI have significant overlap. Areas of implementation include customer service, chatbots, personal assistants, recommendation engines, health diagnostics, translation and fraud prevention. The differences between their use emerge in the output accuracy, the type of data they can use, and the application scope's breadth and adaptability.

AI is more than a model, more than ethereal code: it is a set of technologies most easily accessed from a complex ecosystem that is energy intensive and expensive.[65] Almost everyone relies on Big Tech[66] for computing infrastructure, data to use for training, and a platform to deploy and commercialize AI products.[67] Table 3 illustrates how one AI-enabled service, a search function, is significantly more expensive on multiple fronts than a more traditional service. This discrepancy between AI and non-AI costing runs through every application and infrastructure dependency creates an increasing barrier to entry.

---

[65] Fernando Van Der Vlist, Anne Helmond, and Fabian Ferrari, "Big AI: Cloud Infrastructure Dependence and the Industrialization of Artificial Intelligence," *Big Data & Society* 11, no. 1 (March 2024): 20539517241232630, https://doi.org/10.1177/20539517241232630.

[66] Big Tech encompasses the world's five largest technology companies: Alphabet (Google's parent company), Amazon, Apple, Meta (Facebook and Instagram), and Microsoft.

[67] Amba Kak, "Make No Mistake - AI Is Owned by Big Tech," *MIT Technology Review* (blog), December 5, 2023, https://www.technologyreview.com/2023/12/05/1084393/make-no-mistake-ai-is-owned-by-big-tech/.

Table 3 – Cost Comparison Between AI and Traditional Technology

Cost Factor	AI-Driven Search	Traditional Google Search
Computational Cost	$0.01–$0.10 per query	A fraction of a cent per query
Infrastructure	High (cloud GPUs, TPUs)	Low (optimized indexing)
Business Model	Subscription-based or premium	Ad-supported (free for users)
Energy Consumption	High	Low
Response Speed	Slower due to generation	Faster (pre-indexed results)

Source: Johnston, 'Experience 2025 – AI Search', 25.

AI is interwoven into society's daily function primarily through Big Tech's infrastructure. Most of us are unaware how much control has already been ceded, first to computers and software, and now to AI because it really is everywhere: every platform and every industry, each with a growing number of applications. Removing AI now could unravel whole industries. To illustrate, Table 4 captures a few industries, associated AI applications, and the top companies working in that space. This widespread adoption often outpaces ethical and legal governance frameworks, a dynamic mirrored by industry and the military.

Table 4 – Examples of Industry-Specific AI Applications

Industry	Top companies	Applications
Cloud Computing	Google Cloud, IBM Cloud, Alibaba Cloud, Amazon Web Services (AWS), DataRobot, Baidu AI Cloud, Microsoft Azure, and Salesforce	Contract Management, Fraud detection, and prevention, AML, claims management through claims management, recommendation systems for online platforms, Omni-channel end-to-end order management, personalized customer interaction using customer interaction data and product purchase history
Health Care	Tempus, Suki.Ai, Nanox, Freenome, Neurala, ICarbonX, Flatiron Health, Deep 6, Butterfly Network, K Health, and Insitro	Disease diagnosis, medical imaging analysis, drug discovery using historical data and medical intelligence, patient monitoring, personalized medicine, building sophisticated machines for diagnosing diseases and identifying cancer cells, etc.
Transportation	Anduril Industries, AEye, Pony.Ai, Nauto, Nuro, Zoox, DJI, Orbital Insight	Autonomous vehicles, heavy goods transportation (e.g., Truck platooning that connects heavy goods vehicles),), traffic management, ride-Sharing, route planning, etc.
Education	Riiid, Iris.Ai, Rev.Com, Clarifai, HyperScience, Narrative Science	Automated admin tasks, smart content creation, animations, personalized learning
Manufacturing & Engineering	CognitiveScale, Lobster Media, SenseTime, Bright Machines, Graphcore, Deepmind, Domino Data Lab, OpenAI	Smarter factories with AI-powered assembly, supply chain, robot workers, Inspection, quality control, improving production performance using sensors, product designing, etc.
Energy & the Environment	SenSat, Blue River Technology, Stem, Xanadu, Ambyint, VIA, Siemens, Zymergen	Analytics, optimizing equipment development and management, efficient waste storage and disposal, detecting energy emission reductions, CO2 removal, monitoring deforestation, and predicting extreme weather conditions. AI-aided production and operations optimization leading to reduced emissions, etc.
Robotics	Bossa Nova Robotics, CloudMinds, Vicarious, HiSilicon, UiPath, Smart Eye, Qualcomm	Real-time updates in labor-intensive tasks for robots, including carrying and moving around, cleaning, and inventory management tasks
Entertainment, & Social Media	Discord, Facebook, Tencent, SoundHound, AIBrain	Facial recognition, digital maps, personalized content recommendations and text translation of posts (DeepText at Facebook), content filtering like hate speech and fraud detection

Source: Abeba Nigussie Turi and Pooja Lekhi, eds., Innovation, Sustainability, and Technological Megatrends in the Face of Uncertainties: Core Developments and Solutions, Future of Business and Finance (Cham: Springer Nature Switzerland, 2024), https://doi.org/10.1007/978-3-031-46189-7.

Many advanced AI systems such as AVs, operate under uncertainty which includes assessing potential outcomes through risk assessments. Recalling that risk can be described as the product of the severity of potential consequence and probability of that consequence coming to pass:[68]

$$Risk = [severity\ of\ consequence] * [probability\ of\ consequence]$$

[68] Clow, Rutter, and Zeeb, "Residual DDT Distribution in the Soils and Sediments of Point Pelee National Park."

AI models, particularly those using probabilistic methods, are well-suited to this kind of calculation: perpetually assessing with integrated real-time data. However, while the equation in and of itself is objective, the variables involved are subjective: severity and probability of a specific consequence will be a combination of quantitative data and qualitative assessment. Any values produced will be weighted by programming and programmer bias discussed in the next chapter. System-produced relative risk assessments blur the line between automation and autonomy. In high-stakes environments like AV navigation or battlefield operations, a system's ability to weigh outcomes and adjust behavior accordingly raises complex questions about accountability, intent, and ethical design.

3.3 – Bias in Data and Memorization: Why It Matters

> *Where there is data smoke, there is business fire.*
> - Thomas Redman, aka the Data Doc

> *Any time someone puts a lock on something you own, against your wishes, and doesn't give you the key, they're not doing it for your benefit*
> - Cory Doctorow, journalist and science fiction author.

As GenAI and autonomous systems become more widespread, this section explores how AI reflects bias, how biased data undermines confidence, and how those biases can be integrated into defence systems. Bias and memorization can produce unintended and sometimes dangerous outputs introducing ethical and operational risks at scale. With industry, governments and militaries already using AI models, how does this data impact AV and UAS decision-making, and what biases are hidden within? There is tension between industry pushing AI as the next big thing and industry's lack of transparency with regards to their algorithms and databases which they claim as proprietary.

AI is a function of data quantity and quality;[69] the fuel that makes AI smarter and more lucrative. [70] More data is always better. In 2017, 46.6TBs/second of data was created online,[71] much of which has been collected and stored: Wikipedia, academic libraries, news and social media, government sites, and even pirated content.[72] Today for example, a non-profit database *Common Crawl,* provides access to a multi-petabyte-sized web-crawled database made up of 250 billion pages with 3-5 billion new pages added each month; it is cited in over 10,000 research pages.[73] For-profit companies from this $200B industry also scrapes[74] private and sensitive data including proprietary information, records, and medical files.[75] For example, the *#10YearChallenge* was a 2019 Facebook challenge[76] to upload and tag side-by-side photos of oneself ten years apart[77] which created a well-labelled data set probably used (without permission) to train AI on aging and facial recognition and incorporated into law enforcement databases.[78] Commercial and military use of this kind of sourced data raises serious questions about legal standing, consent, and privacy.

Unregulated and unethical civilian data collection helps populate databases used for training AI, which, when used to train law enforcement or military AI systems, can impact identifying and classifying threats. Big Tech creates many of the databases used which, although

---

[69] Rachel Cheung, "The Roadblock Facing China's Self-Driving Vehicles," *The Wire China*, September 8, 2024.

[70] Kate O'Neil, "Facebook's '10 Year Challenge' Is Just a Harmless Meme - Right?," *Wired*, January 15, 2019, https://www.wired.com/story/facebook-10-year-meme-challenge/.

[71] UNCTAD Secretariat, "Strengthening Consumer Protection and Competition in the Digital Economy" (United Nations, July 29, 2020).

[72] Lauren Leffer, "Your Personal Information Is Probably Being Used to Train Generative AI Models," October 19, 2023, https://www.scientificamerican.com/article/your-personal-information-is-probably-being-used-to-train-generative-ai-models/.

[73] "Common Crawl," Free, Open Repository of Web Crawl Data, accessed January 21, 2025, https://commoncrawl.org/.

[74] Scraping is the automated process of extracting data from a website

[75] Leffer, "Your Personal Information Is Probably Being Used to Train Generative AI Models."

[76] Facebook denies initiating or using the #10YearChallenge

[77] O'Neil, "Facebook's '10 Year Challenge' Is Just a Harmless Meme - Right?"

[78] Kinger and Kulkarni, "Demystifying the Black Box."

available to clients as a product, keeps sources and specific content proprietary. As both a data-user and data collector, Big Tech epitomizes surveillance capitalism: transforming human behavior into digitized proprietary assets monetizing "rights to privacy, knowledge, and application."[79] For example, Google's ecosystem of interconnected services work together to harvest personal data through passive collection, device telemetry, and behavioural predictions.[80] One experiment observed a stationary and inactive android phone send 14 transmissions hourly to Google and when activated, that rate skyrocketed even when google-specific applications were not in use. Similarly but even more concerningly, Amazon had employees transcribe Alexa-captured recordings from unwitting active users to improve the system's pattern recognition in 2019 with similar plans to train AI on real conversations in the future.[81] In civilian contexts, this raises profound concerns about privacy and consent, but in military or dual-use systems, these datasets can provide a foundation for targeting, profiling, or autonomous surveillance at scale.

Biased databases can impact AI systems and create risks associated with LAWSs: skewed classification decisions, discriminatory outcomes, or disproportionate risks to vulnerable populations. Recall that GenAI is rooted in probability by iteratively producing tokens which enables AI models to make decisions or informed predictions in uncertain conditions. While such a process helps give a reasonable answer most of the time, database-related biases make wrong answers more likely. Amazon collecting data from unknowing users described above could, for example, be a source of bias by excluding certain ethnic groups or even focusing on a specific

---

[79] Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance, "Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis" (United Nations Human Rights Council, June 18, 2020).

[80] Douglas C. Schmidt and Team from Vanderbilt University from Dept of Computer Science, "Google Data Collection" (Digital Content Next (DCN), August 2018), https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf.

[81] Tom McKay, "Amazon's Human Helpers Are Quietly Listening in on Some Alexa Recordings," *Gizmodo*, April 10, 2019, https://gizmodo.com/amazons-human-helpers-are-quietly-listening-in-on-some-1833960052.

socioeconomic population. While such trends can appear innocuous, prejudices, inequalities, and stereotypes found in the source data can unexpectedly produce and magnify distortions thus creating a disconnect between AI outputs and the average human response.[82] For example, Microsoft's 2016 chatbot named Tay was trained with anonymized public data and released onto Twitter with disastrous results: a (human) user tweeted that "Tay" went from "'humans are super cool' to full nazi in <24 hours" and Microsoft ended the experiment after 16 hours.[83]

Ultimately, bias-related risks compromise the reliability of AI decisions in high-stakes applications. Although the Tay incident occurred in a civilian context, it demonstrates a critical accountability issue for autonomous systems: when behavior is shaped dynamically by real-time data, designers may have little control over how that behavior evolves, especially in unpredictable or adversarial environments. For systems like LAWSs, operating without real-time human oversight, opaque training data and untraceable logic pose direct threats to both ethical standards and legal accountability.

3.4 – Components of a Technical Solution: Explainable AI (XAI)

> *There is a growing interest in designing, developing, and evaluating methods to ensure that human users can safely interact with a transparent and accountable AI system which makes fair decisions with respect to ethical considerations.*
> - Konstantinos Tsiakas and Dave Murray-Rust, 'Using Human-in-the-Loop and Explainable AI to Envisage New Future Work Practices', 22.

By increasing interpretability, Explainable AI (XAI) could be part of a web of technology-based features used to embed accountability into AI applications through design. This chapter will explore how one set of methodologies can contribute to accountability, and then briefly extrapolate how XAI can combine and be layered with other technologies. XAI is a

---

[82] Advisory Group on Advanced Technologies, "Artificial Intelligence Demystified."

[83] Jane Wakefield, "Microsoft Chatbot Is Taught to Swear on Twitter," *BBC*, March 24, 2016, https://www.bbc.com/news/technology-35890188.

field of study focused on making AI models and decisions more understandable to humans. As AI becomes increasingly complex, outputs are buried under billions of data points, user prompts, and probabilistic estimates. Even AI developers cannot always explain why their AI systems make specific choices or provide specific outputs. XAI is increasingly important to create greater auditability and accountability: it builds trust, tracks errors, detects algorithmic bias, and complies with governance.[84]

XAI methods require a trade-off between performance and interpretability due to structural differences between white and black box models defined in section 3.2.[85] White box model interpretability is called intrinsic or inherently interpretable[86] because assumptions, decisions and recommendations are traceable and reproducible: for example, factor A and B lead to conclusion C.[87] More complicated black box models use post-hoc explanation methods:[88] a second model explains the original's output to describe key factors leading to an output rather than providing an opportunity to influence a future output, but accuracy is difficult to trace.[89] Decision-making clarity sacrifices performance. Black box models whose high performance accuracy is required by AVs and military UAS applications, are associated with lower interpretability as seen in Figure 10.

---

[84] Amanda McGrath and Alexandra Jonker, "What Is AI Interpretability?," IBM, October 8, 2024, https://www.ibm.com/think/topics/interpretability.

[85] Kinger and Kulkarni, "Demystifying the Black Box."

[86] Daisy Tsang, "White Box vs. Black Box Algorithms in Machine Learning," *Activestate* (blog), July 19, 2023, https://www.activestate.com/blog/white-box-vs-black-box-algorithms-in-machine-learning/.

[87] McGrath and Jonker, "What Is AI Interpretability?"

[88] Satchidananda Dehuri et al., eds., *Machine Intelligence, Tools, and Applications: Proceedings of the International Conference on Machine Intelligence, Tools, and Applications—ICMITA 2024*, 1st ed. 2024, Learning and Analytics in Intelligent Systems 40 (Cham: Springer Nature Switzerland, 2024), https://doi.org/10.1007/978-3-031-65392-6.

[89] Luis Fernando Castillo Ossa, *Trends in Sustainable Smart Cities and Territories*, 1st ed, Lecture Notes in Networks and Systems Series, v. 732 (Cham: Springer International Publishing AG, 2023).

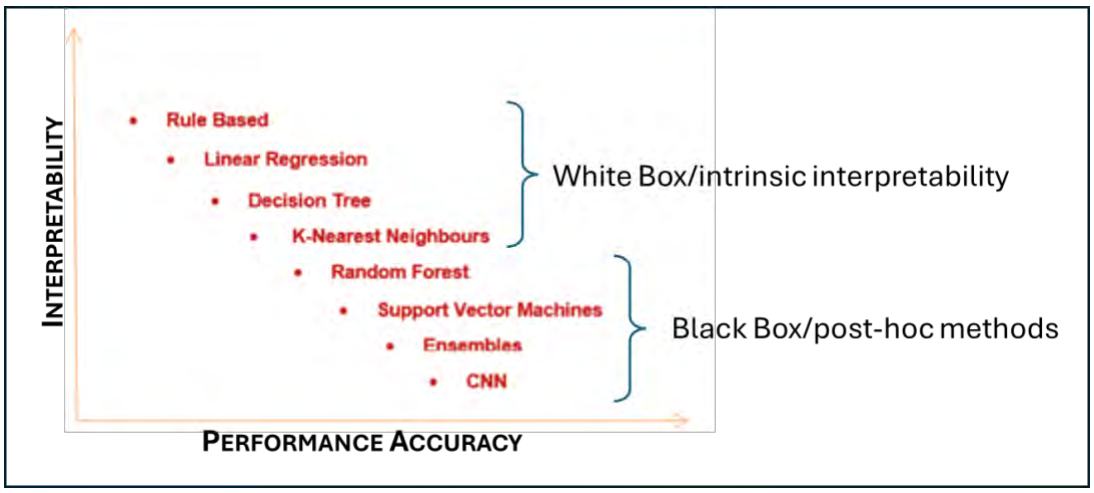


Figure 10 – Illustration of the Inverse Relationship Between Interpretability and Performance Accuracy linked to White and Black Box Models
Source: Dehuri et al., 'Machine Intelligence, Tools, and Applications', 24.

XAI use cases in the AV industry focus on capturing information for audits in support of insurance claims and follow-on development.[90] For example, if an AV suddenly and unexpectedly swerved, potentially causing an accident, XAI methods would enable investigators to assess and analyze causality of that sudden maneuver. In fact, Europe recently legislated that all new vehicles include an event data recorder as a standard feature starting in July 2024.[91] Further highlighting XAI's importance, "transparency and explainability not only help to build trust and reliability in artificial intelligence, but also contribute to the protection of human rights."[92]

To illustrate why it's important to understand how AI models make decisions, consider saliency maps: an XAI visualization tool that can reveal the internal logic of an AI system in a

---

[90] Kamal Malik et al., *Explainable Artificial Intelligence for Autonomous Vehicles: Concepts, Challenges, and Applications*, 1st ed. (Boca Raton: CRC Press, 2024), https://doi.org/10.1201/9781003502432.
[91] Rechelle Ann Fuertes, "Explainable AI in Autonomous Vehicles: Building Transparency and Trust on the Road," *Smyth OS* (blog), February 21, 2025, https://smythos.com/ai-industry-solutions/automotive/explainable-ai-in-autonomous-vehicles/.
[92] Secretary-General, "Right to Privacy."

human-digestible format.[93] Figure 11 highlights that the AI focuses on the text label located on one image rather than anything *horse-like* which changes the outcome of classifying an otherwise identical image. Misclassification in AI has real-world implications: in a health care scenario assessing patient imagery, an AI could create a series of misleading results if extraneous information from a patient's file, like ethnicity or scan frequency, is analyzed rather than the imagery. Biased or misleading data used during AI training can inadvertently inculcate an AI into incorrect pattern recognition which, for AVs and UASs, can skew decisions otherwise based on sensor data. Confirming how an AI makes a decision builds trust.

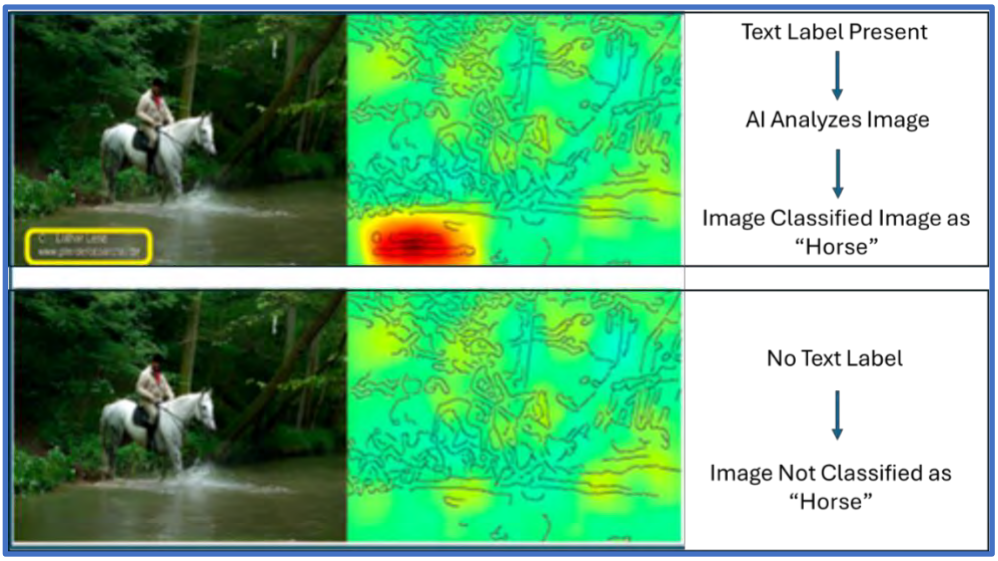


Figure 11 – Saliency Map Illustrating Human-Digestible Content: How an AI Makes a Decision and Why That's Important

Source: Kinger and Kulkarni, 'Demystifying the Black Box: An Overview of Explainability Methods in Machine Learning', 24.

While XAI focuses on making machine decision-making more transparent to human users, its effectiveness is also shaped by who controls the underlying systems. Much of the AI ecosystem, particularly model training, deployment, and data infrastructure, is dominated by Big

[93] Kinger and Kulkarni, "Demystifying the Black Box."

Tech who operates proprietary models and cloud platforms, and provide limited access to internal logic, training data, and underlying architecture.[94] The reach of Big Tech permeates into every layer of AI infrastructure and development raising questions about control. In addition to owning and controlling most back-end infrastructure through proprietary ecosystems and data pipelines, Big Tech also controls proprietary databases and models that power AI applications. Even well-designed XAI tools may be constrained by a lack of back-end access and transparency, especially as Big Tech-controlled AI infrastructure becomes more complex requiring iterative updates. This creates barriers for independent developers, and due to AI's data requirements and insufficient governance, there is little incentive for Big Tech to do otherwise. In the future, explainability requirements may extend to institutional and infrastructural layers that shape system behavior and accountability.

XAI methods are not a cure-all for accountability and human control but instead, may contribute to a technology-based solution that, when layered and combined, is greater than the sum of its parts. Current XAI research involves exploring links to prediction and human-in-the-loop systems. Specifically, XAI methods analyzing why a decision is made, can apply to predictive technology by making those predictions more transparent and interpretable[95]. Melding XAI and predictive technology leads to a spectrum of human digestible feedback applicable throughout AV or UAS operation as per Figure 12. Another emerging research area is the intersection of XAI and human in/on/out-of-the-loop control (as defined in Figure 12)[96] which

---

[94] Ganesh Sitaraman, "Too Big to Prevail: The National Security Case for Breaking Up Big Tech," *Foreign Affairs; New York* 99, no. 2 (April 2020): 116-120,122-126.

[95] Shahin Atakishiyev, Mohammad Salameh, and Randy Goebel, "Safety Implications of Explainable Artificial Intelligence in End-to-End Autonomous Driving" (arXiv, 2024), https://doi.org/10.48550/ARXIV.2403.12176.

[96] Malik et al., *Explainable Artificial Intelligence for Autonomous Vehicles*.

"can help identify and correct errors, biases, and limitations in AI models."[97] Today, this is being explored for managerial systems but there are potential applications for other areas. This link between XAI and other technologies illustrates how seemingly separate areas of research are coalescing with new and exciting results.

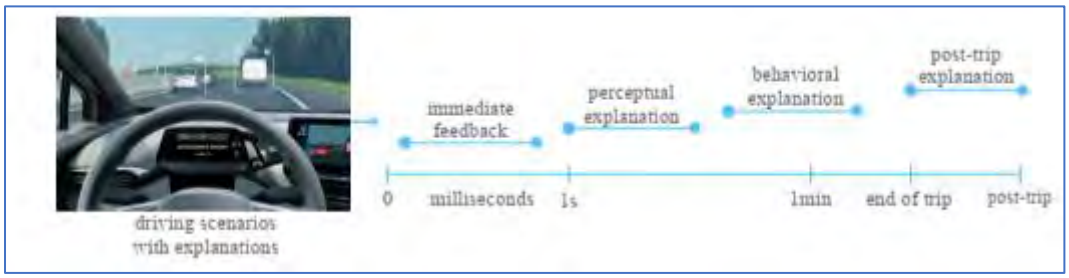


Figure 12 – The Timing Sensitivity of Communicating for Assisted Autonomous Driving Explanations: Reactions, Situational Awareness and After Trip Feedback
Source: Shahin Atakishiyev, Mohammad Salameh, and Randy Goebel, "Safety Implications of Explainable Artificial Intelligence in End-to-End Autonomous Driving" (arXiv, 2024), https://doi.org/10.48550/ARXIV.2403.12176., 24.

Technical solutions to complex problems are complex themselves, combining and layering multiple sub-fields and technologies. Because of industry's insatiable desire to commercialize products, today's AI development is like running downhill towards a cliff while building a plane: the field is evolving, lines of research continue to emerge, and there is no clear path to define what will stick. Without attempting to define the entire discipline, Table 5 highlights select areas of AI research that are especially relevant to AV and UAS development and will likely complement each other and XAI methods.

[97] Sunil Ramlochan, "Exploring the IEEE Paper: Human-in-the-Loop, Explainable AI, and the Role of Human Bias," *Prompt Engineering & AI Institute* (blog), March 27, 2024, https://promptengineering.org/exploring-the-ieee-paper-human-in-the-loop-explainable-ai-and-the-role-of-human-bias/#1-introduction.

Table 5 – Cutting-Edge Areas of AI Research That Will Impact AVs and UASs

AI Concept & Definition	Relevance to AVs	Relevance to Military UAS
Model Editing: Adapts ML models over time with targeted updates.	Corrects specific navigation or decision-making errors.	Updates models for changing battlefield info without full retraining.
Large Action Models (LAMs): Enables complex, multi-step task execution.	Supports high-level driving decisions.	Autonomous planning for surveillance or strike missions.
Continual Learning: Learns from new data, adapts over time.	Adapts to novel driving environments or hazards.	Adjusts to new enemy tactics or conditions.
Agentic AI: Autonomous agents making multi-step plans.	Enables fully autonomous vehicle operation.	Supports goal-driven missions.
Retrieval-Augmented Generation (RAG): Combines LLM output with retrieved external knowledge.	Improves decisions using live traffic and weather information via integrated infrastructure	Could access real-time intelligence for mission decision-making.
Natural Language Processing (NLP): Processes and understands human language.	Voice commands and interpreting road signs.	Mission briefings and communication handling.
Sensor Fusion: Combines data from multiple sensors.	Enhances perception using LiDAR, radar, etc.	Improves ISR effectiveness and navigation accuracy.
Multimodal AI: Processes diverse data types (text, image, etc.).	Enhances situational awareness from varied inputs.	Analyzes combined data types for battlefield awareness.
Neuro-symbolic AI: Blends neural nets and symbolic reasoning.	Better rule-following and generalization.	Rules of engagement comprehension with flexible reasoning.
Edge AI: Processes data on local devices.	Ensures low-latency, on-device decision-making.	Operates sans cloud access (denied environments)
Explainable AI (XAI): Makes AI decisions interpretable to humans.	Builds user trust and enables debugging.	Supports accountability
World Models: AI's internal representation of its environment.	Allows AVs to simulate and plan navigation.	Simulates terrain and anticipates enemy movement.
Federated Learning: Trains models across devices without sharing data.	Improves learning while preserving user privacy.	Enables secure distributed learning in the field.

Source: Author created with definitions from https://www.smalsresearch.be/radar-2025/aiml-radar-2025

Every AI concept and definition from Table 5 is relevant to the future of AI-enabled AVs and UASs and thus accountability. Understanding how XAI in isolation hints at how each of

these emerging AI technologies can have a similar impact. Harmonizing the advancements and applications of XAI with the other 12 areas of study presented in Table 5, other current areas of study not tabulated, and other areas of study not yet imagined, creates the possibility of a future web of technological advancement that can be incorporated into AVs and UASs. If a technical solution to the ethical question pitting military exigency or even every-day convenience against human control is possible, many technical components are required. In concert, in combination, in total, different lines of AI research start to form a technical approach to ethical challenges posed by LAWSs including XAI methods as explored above.

A key difference between AVs and military applications of UASs, is that autonomy is the point of an AV, whereas completing military tasks is the point of a military UAS; autonomy is the means rather than the end. For military applications of fully autonomous UASs, namely LAWSs, XAI methods combined with other emerging technology could provide a sufficient mechanism to assign responsibility such that the UN's condemnation would no longer be valid.[98]

3.5 – AI Foundations: Summary and Implications

> *Technology is a useful servant but a dangerous master.*
> - Christian Lange, Nobel Lecture, 1921.

Society is at a pivotal juncture as AI rapidly evolves from a futuristic concept to a technology of convenience embedded into everything. Built on foundations of logic, data, and computational power, these systems are no longer confined to theory, they are operational, influential, and deeply consequential. As explored in this chapter, the core technologies

[98] United Nations Office for Disarmament Affairs (UNODA), "Lethal Autonomous Weapons Systems (LAWS)."

underpinning AI are inextricably linked to ethical dilemmas, opaque decision-making, and geopolitical control.

AI is paradoxical: it holds the promise to improve lives and streamline complex operations while also introducing new dangers. It can obscure accountability, amplify systemic bias, and outpace regulation. These tensions are magnified in the context of AVs, military applications and LAWSs, where decisions can be life and death. The dominance of Big Tech, combined with rapid technical advancement, means that critical decisions may be shaped by systems we do not fully understand and cannot fully audit. XAI has emerged as one promising avenue among many to increase transparency in AI systems. Yet even this approach carries a trade-off: as model complexity increases, interpretability often declines. Other technical innovations, such as world models, agentic AI, and edge computing, offer different ways to support adaptability, operational reliability, and accountability in autonomous systems. As military UASs move toward greater autonomy, no single innovation will resolve the ethical dilemmas they pose but instead, may contribute to a layered solution. These approaches do not eliminate ethical challenges but do offer a way to cede human control intentionally with responsibility and accountability embedded into the AI's design. Consequently, this means that the conversation must inevitably shift from questions about whether to pursue autonomy, to how to pursue it wisely.

Although AI can access risk, society must question whether it will be trusted to act on those assessments. As AI is implemented into systems with potentially lethal consequences like AVs and UASs, this accountability becomes existential. Ultimately, AI does not exist in a vacuum, but rather reflects our values, assumptions, and biases. In a world teetering between

digital empowerment and algorithmic domination, we must choose, deliberately, ethically, and collectively, the kind of AI-powered future we are building.

CHAPTER 4 - AUTONOMOUS VEHICLES AND BLURRING BOUNDARIES

4.1 – Introduction: Regulating the AV Road from the Ground Up

> *The difference is that while a language model may give you nonsense, a self-driving car can kill you*
> - Mary Cummings, 'What Self-Driving Cars Tell Us About AI Risks', 23.

Solidifying previous technical discussions, AVs are an accessible application of AI which mirrors civilian and military UASs. "Common technological underpinnings"[99] between AVs and UAS include real-time sensor fusion, navigation requirements, and AI decisions based on imperfect and incomplete data. A technical understanding of AVs provides a foundation for discussing the complexities of aerial autonomy: navigation, obstacle avoidance, real-time decision-making, smart-city integration, and the critical question of being able to identify how decisions are made and who is responsible.

AV development offers a timely microcosm where society can test ethical and legal approaches and methods which can then be applied in the military domain: meaningful human control, liability and accountability, and commercial innovation. In theory, AI-powered systems can perform ongoing and perfectly calculated risk assessments, but whether probabilistic reasoning described in chapter 3 is ethically sufficient when lives are at stake remains unresolved. This becomes especially important as military UASs transition from Remotely Piloted Aerial Platforms (RPAS) to increasingly autonomous systems used for ISR, EW, and lethal force.

---

[99] Vaibhavi Tiwari, Dharshana Rajasekar, and Jiayin Wang, "A Survey: Emerging Cybersecurity Threats in Driverless Cars," in *2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), Yorktown Heights, NY, USA: IEEE, 2024), 183–89, https://doi.org/10.1109/UEMCON62879.2024.10754688.

This chapter will discuss self-driving cars or AVs which are part of a well-documented industry that encompasses consumers, manufacturing, insurance, and governance. Specifically, it will cover an overview of technical and legal considerations before analyzing how civilian regulatory tools like liability inform accountability in military applications of UASs.

4.2 – AV Background: Nomenclature and Policy

> *Jake designed the self-driving network to save lives, but some bastard had gone and weaponized the damn thing*
>
> *- J. Luke Bennecke, 'Civil Terror: Gridlock'*

The use case for AVs is compelling. A *Jetsons*-esque utopian future with reduced emissions, greater freedom for aging and disabled populations, and everyone spends less time in traffic. Vehicles will park themselves, return on command, and vehicles will become a place to relax, work or socialize. The financial picture associated with AVs is exponentially optimistic as illustrated by Figure 13: the 2023 AV market revenue of $208B is expected to grow by $3.79T (yes, trillion) or about 2000% by 2032. Yet this outlook comes with serious challenges around privacy, cybersecurity, and accountability; issues intensified for military AVs where a security breach can affect national interests.

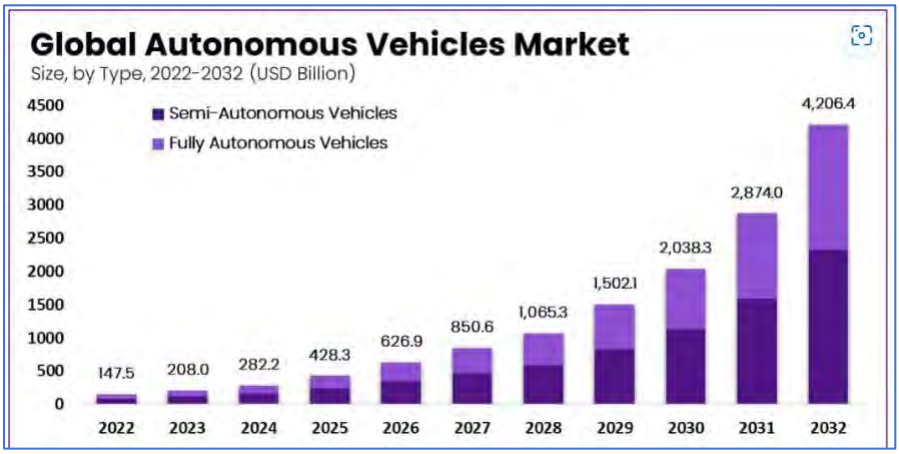


Figure 13 – Global AV Vehicle Market: Why Industry is Interested AVs

Source: Pangarkar, 'Autonomous Vehicles Statistics 2025 by Type, Technology, Driving', 25.

To understand how society classifies AV autonomy, and where liability and responsibility shifts away from a vehicle's operator, we turn to the globally recognized SAE[100] framework which provides a set of standards illustrated by Figure 13. The blue levels (0, 1, 2) reflect levels where the driver maintains full care, custody, and control of the vehicle, and the green levels (3, 4, 5) reflect levels where the driver can legally remove their focus from the task of driving.[101]

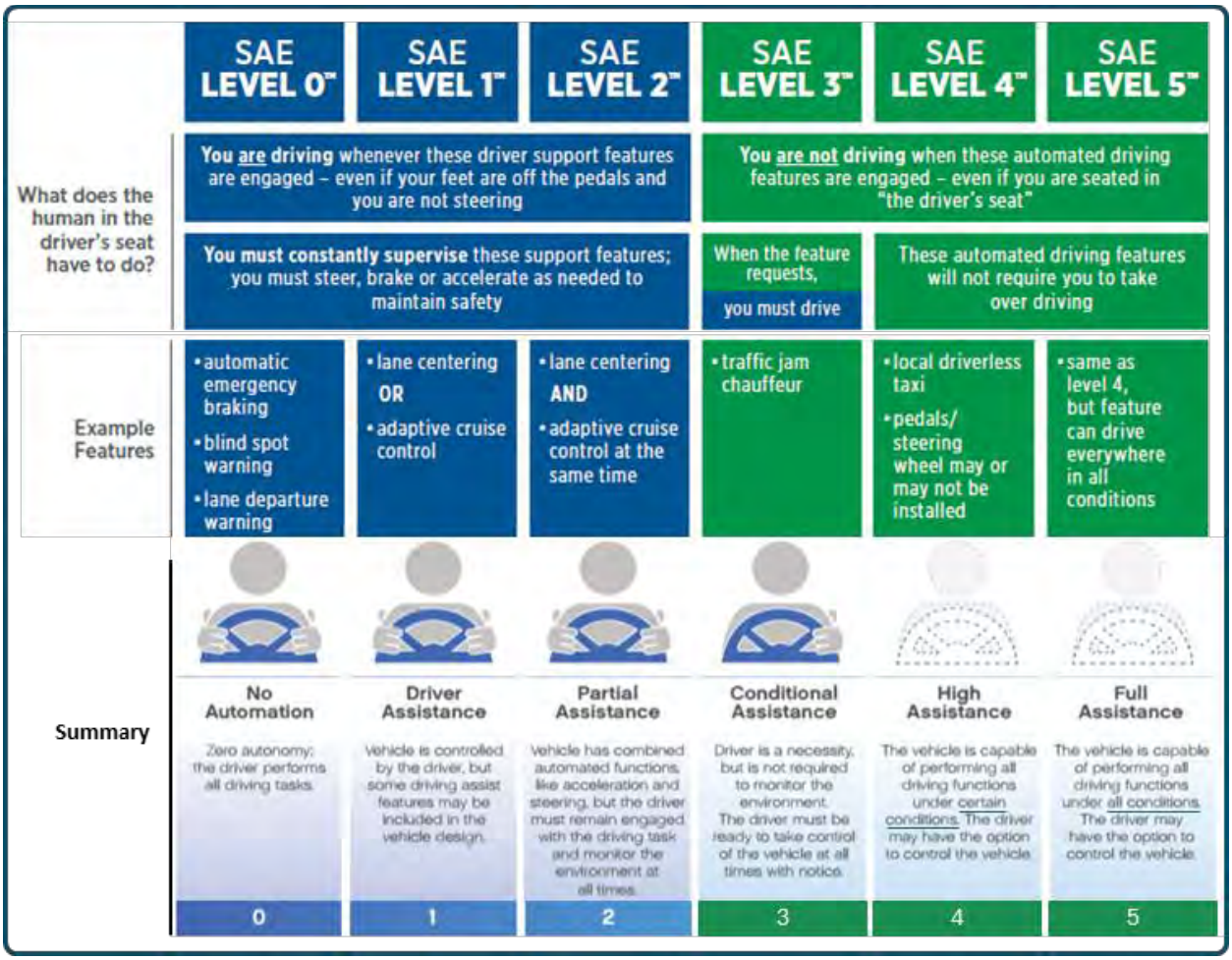


Figure 14 – Overview of SAE Levels for AVs

Source: Author created using content from 'SAE Levels of Driving Automation Refined for Clarity and International Audience', 21. and Jones Day Law Firm, 'Legal Issues Related to the Development of Automated, Autonomous, and Connected Cars', 17.

---

[100] SAE is not an acronym. However, historically SAE stood for Society of Automobile Engineers and then Society of Automotive Engineers before becoming simply SAE International as of 2006.

[101] "SAE Levels of Driving Automation Refined for Clarity and International Audience," SAE International, May 3, 2021, https://www.sae.org/blog/sae-j3016-update.

In the same way definitions matter for LAWSs, classification standards for AVs matter for engineering purposes and assigning legal liability. Yet the AV industry often blurs these distinctions. Most vehicles sold today are level one due to features like lane-assist and adaptive cruise control. Vehicles commercially available for sale and marketed as self-driving are currently level two[102] and, despite deceptive advertising and nomenclature which obfuscates responsibility and liability, the driver retains legal liability and is required to remain engaged in the task of driving.[103] Table 6 highlights how major manufacturers label SAE level 2 vehicles with terminology that implies greater autonomy than it legally provides. For example, Tesla uses *full self-driving capability* to describe SAE level two, which requires an engaged driver, even though this terminology better describes SAE level three. There are ongoing lawsuits around this terminology and associated marketing which illustrates the link between definitions and accountability; analogous to the requirement for a LAWS definition being pushed for by the UN discussed in chapter two.5

Table 6 – Deceptive Marketing Terminology for SAE Level 2 Vehicles

Tesla	Autopilot/Full Self-Driving Capability
Audi	Traffic Jam Assist
GM	Super Cruise
BMW	Extended Traffic Jam Assistant
Ford	Blue Cruise
Hyundai	Automated Driving Package

Source: Sever and Contissa, 'Automated Driving Regulations – Where Are We Now?', 24.

The SAE classification and application within the automotive industry offers an example of how automation and autonomy are frequently confused and conflated. A SAE level two AV,

---

[102] Adib Bin Rashid and Md Ashfakul Karim Kausik, "AI Revolutionizing Industries Worldwide: A Comprehensive Overview of Its Diverse Applications," *Hybrid Advances* 7 (December 2024): 100277, https://doi.org/10.1016/j.hybadv.2024.100277.

[103] Cat Dow, "What Are the Six SAE Levels of Self-Driving Cars?," *Top Gear Advice* (blog), March 6, 2023, https://www.topgear.com/car%20news/what-are-sae-levels-autonomous-driving-uk.

such as Tesla's "Full Self-Driving" model, is an example of automation: it can change lanes, maintain distance, and park itself, but it cannot independently change its route to circumnavigate traffic congestion. A SAE level 3 or higher, must make those types of decisions based on real-time data and probabilistic reasoning. In the military domain, this same confusion plays out in UASs. A UAS following a pre-programmed strike plan is automated; a UAS dynamically selecting targets or modifying a mission profile in response to battlefield data is autonomous; especially if human override is impractical or excluded. The blurred boundary between automation and autonomy fuels uncertainty over who (or what) is ultimately responsible. This distinction matters because it shapes liability, user expectations, and regulatory requirements.

Today, countries around the world are experimenting with AVs and policy requirements for SAE levels three and four. While neither the US, Europe, nor Canada have yet approved AVs wholesale, but there are a variety of limited license models available; American adoption milestones are captured in Figure 15. Human reactions are crucial for gauging public readiness which shapes regulatory momentum. One method to enable development while increasing public awareness and acceptance are the robo-taxi services being launched city by city. In the spring of 2024, the first line of a news article heralding the upcoming arrival of robotaxis in three America cities was "imagine getting into a taxi, setting off to your destination, only to find out there's no one driving the car."[104] Less than ten months later, another newspaper article opens with "Waymo is adding 10 new cities to its roster for driverless car testing [through robotaxi services]."[105] The juxtaposition between these two stories highlights how far public acceptance

---

[104] "Robotaxis: Driverless Cars Arriving in US Cities."

[105] Nicole Kobie, "Is Waymo Coming To Your City? Google Robotaxis Hit the Road for Tests," *Forbes*, January 31, 2025, https://www.forbes.com/sites/nicolekobie/2025/01/31/is-waymo-coming-to-your-city-google-robotaxis-hit-the-road-for-tests/.

and policy has moved forward in less than a year. One passenger described his family's robotaxi experience in San Francisco in August of 2024:

> He loved the experience even if there were a couple of glitches, including the family having to chase the app-summoned car after it drove past them before finally stopping so he could unlock the doors with his phone. Video of their ride shows a giddy family marveling at the empty driver seat as Eminem pumps out of the car's speakers.[106]

These glitches make for an amusing anecdote but it highlights that AV technology still makes mistakes; one American dataset captured 83 fatalities related to AVs between 2019-2024.[107] Given that these AVs are now moving on city streets along with the rest of the population it is critical to establish accountability through real-time oversight and liability frameworks before scaling these technologies more broadly.

Figure 15 – UAS AV Adoption Milestones and Image of a Passenger Entering a Driverless Robo-Taxi AV During a Pilot Project

Source: Author created based on content from Ford's company website, US Department of Transportation, 'Automated Vehicles Comprehensive Plan', 21. and Shepardson 'Automakers Urge Trump Administration to Clear Way for Self-Driving Cars', 25.

---

[106] Government of BC, "Automated (Self-Driving) Vehicles," accessed April 15, 2025, https://www2.gov.bc.ca/gov/content/transportation/driving-and-cycling/road-safety-rules-and-consequences/self-drive.

[107] Craft Law Firm, "Autonomous Vehicle Accidents: NHTSA Crash Data (2019-2024)," accessed May 8, 2025, https://www.craftlawfirm.com/autonomous-vehicle-accidents-2019-2024-crash-data/#ads-crash-details.

Europe and Canada are similarly considering legislative updates to support robotaxis and thus future AV adoption. Barries to AVs entering the European market include higher EU privacy standards, while simultaneously having country-specific "safety standards, driving laws, and insurance rules."[108] Additionally, older cities have narrower and more twisty roads making navigation more complex, and there is less public acceptance. Canada began legislating for AVs in 2018 at the federal level, and Ontario added a decade-long pilot-project for AVs weighing more than 4,500kgs; the smallest of which being approximately the size of a Ford F-450. Conversely, British Columbia has provincial legislation which, as of April 2024, completely "prohibits the operation of [SAE] Level 3, 4 and 5 self-driving vehicles."[109]

It is China, however, that is "leading the way regarding innovation and as of September 2024, had issued 16,000 licenses for autonomous vehicles [AVs] to test on over 32,000 km of roads across 16 cities." [110] This market domination can be attributed to strategic partnerships, government collaboration, and more "open data policies [which] allows companies to access vast amounts of driving data for AI training."[111] Essentially, the Chinese government is willing to take greater risks with their citizens' physical safety and privacy, work with industry to mandate and install AV friendly infrastructure, and directly engage and steer companies developing AVs.

Just as the moral machine in chapter 2 highlighted how cultural differences affected ethical perspectives, understanding how society views AVs is similarly skewed. Regardless, this view offers crucial insight into the broader dilemma of human oversight and control in AI

---

[108] Maja Stefanovic, "How Close Are We to Self-Driving Taxis in Europe?," *HERE360 News* (blog), February 5, 2025.

[109] Government of BC, "Automated (Self-Driving) Vehicles."

[110] Cheung, "The Roadblock Facing China's Self-Driving Vehicles."

[111] Carlo van der Weijer and Alwin Bakker, What the World could Learn From China's Autonomous Vehicle Innovations, July 2, 2024.

systems. As responsibility shifts from the human driver to software, hardware manufacturers, and even infrastructure providers, autonomy challenges long-established norms of accountability and liability which can be influenced by public perception and acceptance. The next sub sections examine the technical and governance mechanisms currently emerging to manage AVs, including Vehicle-to-Everything (V2X) communication, insurance models, and fault attribution. AV evolution is more than a technical achievement, it is a window into how society distributes trust, risk, and legal responsibility foreshadowing regulatory and liability challenges in military scenarios further discussed later in subsequent sections and expanded in chapter five.

4.3 – AV Technology: Under the Hood (Literally)

> *A group of engineers are talking about how to fix a broken-down vehicle: the chemical engineer suggests the issue is related to gasoline impurities, the mechanical engineer suggests a broken starter and the electrical engineer wants to check for a dead battery. Finally, the computer engineer suggests "let's try closing all the windows and restart it!"*
>
> *- Anonymous*

While the regulations and classification frames discussed above shape how AVs are perceived and governed, understanding the technical architecture of these systems is equally important. The design of sensors, AI models and communication infrastructure directly influences how decisions are made and who is accountable when things go wrong. In the context of increasing autonomy, technical details are the foundation for ethical design, liability assignment and future military applicability. This section explores how AVs think and perceive under the hood, setting the stage for further discussion on meaningful human control and accountability in both civilian and military contexts.

AVs function as a stack of technology combining sensors, an AI model with hardware and software systems, and increasingly, communication with external sensors and networks.[112] Sensors enable an AI system to perceive and interpret its surrounds; they are the eyes and ears.[113] Illustrated in Figure 16, sensors include cameras, radar and LiDAR (Light Detection and Ranging), Inertial Measurement Unit (IMU), a Global Navigation Satellite System (GNSS), and sonar. Recent upgrades allowing sensors to move from 2D to 3D perception and object detection is a major component of today's successful AVs[114] and in 2023, the AV industry collectively moved from high-precision maps to perception-based navigation and decision making.[115]

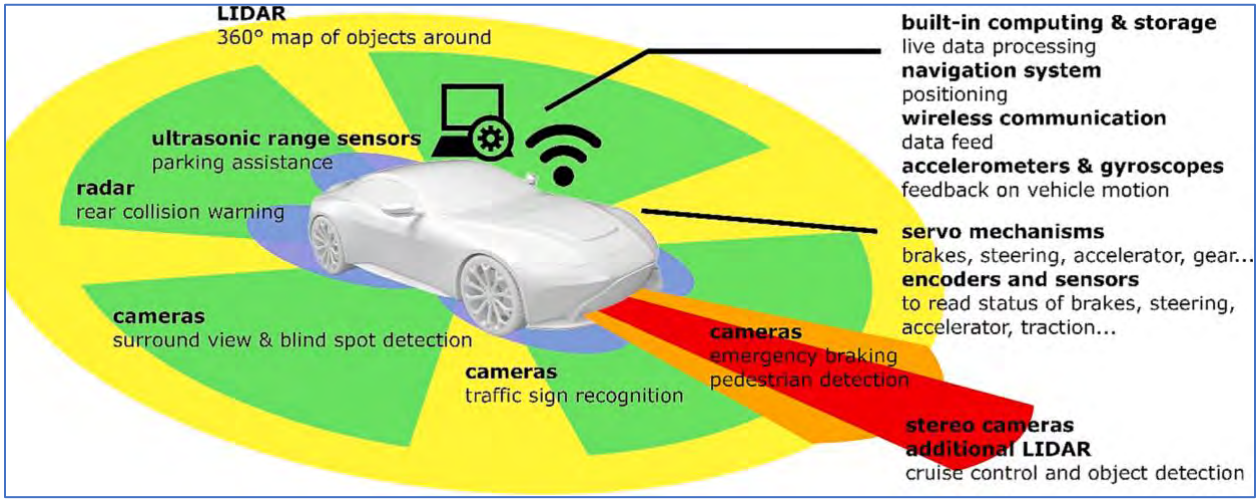


Figure 16 – Integrated AV Sensors
Source: Sever and Contissa, 'Automated Driving Regulations – Where Are We Now?', 24.

Wireless communication between AVs, Vehicle-to-Vehicle (V2V), enables multiple AVs to harmonize their actions which could include making space for one AV to merge or ensuring

---

[112] Oluwajuwon A. Fawole and Danda B. Rawat, "Recent Advances in 3D Object Detection for Self-Driving Vehicles: A Survey," *AI* 5, no. 3 (July 25, 2024): 1255–85, https://doi.org/10.3390/ai5030061.

[113] Jobanbir Singh et al., "Autonomous Driving and ADAS Embedded with AI: Comparing the AI Norms," in *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)* (2024 International Conference on Intelligent Systems for Cybersecurity (ISCS), Gurugram, India: IEEE, 2024), 1–6, https://doi.org/10.1109/ISCS61804.2024.10581391.

[114] Fawole and Rawat, "Recent Advances in 3D Object Detection for Self-Driving Vehicles."

[115] 36Kr English, "The Current State of Self-Driving Across China in 2024," May 20, 2024.

another AV is aware of a turn to allow for another braking. V2V becomes an additional data stream and allows the onboard AI to respond to explicit data rather than perceived data via their sensors. When enough AVs exist on the road simultaneously, they may begin to act more like a swarm, rather than individual AI systems. Similarly, Vehicle-to-Infrastructure (V2I) refers to wireless communication between AVs and infrastructure, which could include information exchanged about road safety warnings, and traffic management flow. The umbrella term, Vehicle-to-Everything (V2X), refers to communication between an AV and any other interface, with X being a placeholder variable. Data processing associated with these information streams may use cloud computing or edge AI (defined in Table 5 in chapter 3) to lower information flow latency (time related to data movement between systems) and helps protect data and user privacy. Each sensor and V2X information source "produce distinct data types with varied degrees of precision, resolution, and sensitivity to environmental conditions.[116] To combine and use this data in real-time requires significant processing power and leverages the concepts of sensor fusion, multimodal and world models, also defined in Table 5. V2X is the foundation of an Intelligent Transportation System (ITS) designed to "reduce traffic congestion, shorten travel times, improve safety, and minimize environmental impacts."[117] Beijing, for example, already "seamlessly integrates mobility solutions within its broader smart city frameworks like that shown in Figure 17."[118]

---

[116] Fawole and Rawat, "Recent Advances in 3D Object Detection for Self-Driving Vehicles."

[117] Muhammad Ali Naeem, Sushank Chaudhary, and Yahui Meng, "Road to Efficiency: V2V Enabled Intelligent Transportation System," *Electronics* 13, no. 13 (July 8, 2024): 2673, https://doi.org/10.3390/electronics13132673.

[118] van der Weijer and Bakker, What the World could Learn From China's Autonomous Vehicle Innovations.

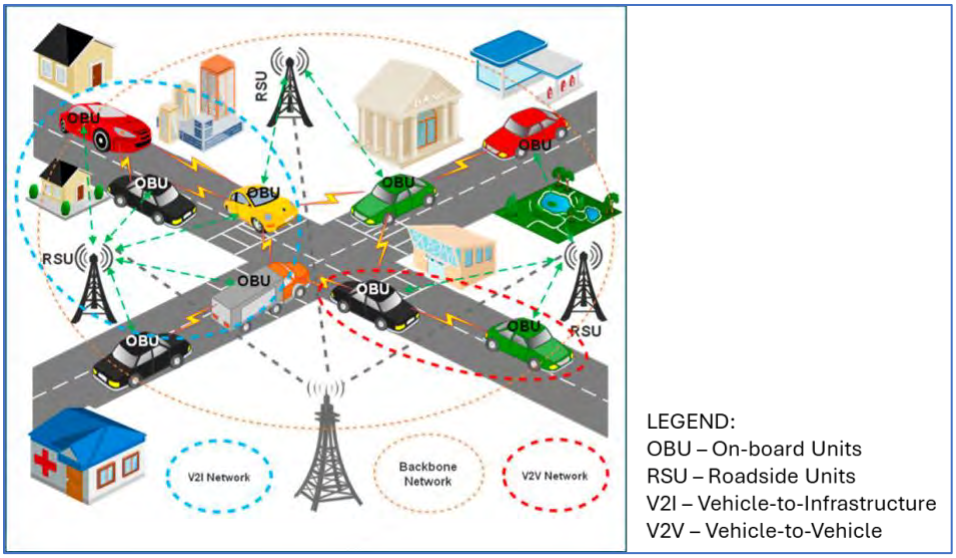


Figure 17 – Visualization of Deployed V2X Technology in an Urban Environment
Source: Naeem, Chaudhary and Meng, 'Road to Efficiency: V2V Enabled Intelligent Transportation System', 24.

AVs collect, process and store huge amounts of data from V2X infrastructure and sensors accurately enough on which to base life and death decisions. This data can be used to create unique consumer profiles that are then leveraged to initiate cyberattacks, additional AI training databases, or influence broader activities. Although China is dominating the AV market globally, data security concerns are limiting Chinese companies from entering Western markets. Even with Chinese social media whose treasure trove of personal data pales in comparison to the data accessible through AV sensors, national security concerns have been raised: "policymakers are concerned about whether the Chinese government would ever compel ByteDance[119] into sharing that data."[120] Essentially, "the extent to which foreign markets open up to Chinese companies will also come down to the issue of data."[121] However, Big Tech's approach to privacy and data

[119] ByteDance owns TikTok which is better known
[120] Daniel W. Drezner, Henry Farrell, and Abraham L. Newman, eds., *The Uses and Abuses of Weaponized Interdependence* (Erscheinungsort nicht ermittelbar: Nomos Verlagsgesellschaft mbH & Co. KG, 2021), https://doi.org/10.5771/9780815738381.
[121] Cheung, "The Roadblock Facing China's Self-Driving Vehicles."

collection is also problematic as discussed in chapter three but despite that track record, Big Tech has partnered with the auto industry and Western governments are, by in large, poised to set up supporting infrastructure.

A commonly cited statistic in AV safety discussions states that "human error is responsible for over 90% of road accidents."[122] While it underscores human shortcomings of fatigue, distraction, and poor judgment, it does not mean or guarantee that AVs are 90% safer. Instead, academic and industry research present mixed findings and while some argue that AVs eliminate driver-related errors, this is an oversimplification. Despite their potential, AVs do not represent universal safety improvement. Researchers found that a variety of factors contributed to AV crash rates including road quality, location, and vehicle type.[123] Further, databases used for collecting information on accidents and used by researchers have strict data collection criterion[124] which can skew the results: for example, fender benders with two human drivers are often handled unofficially and are likely underreported. Next, AI is designed and maintained by imperfect humans who "have many frailties…[who make] mistakes in logic, mistakes in coding, mistakes in error-checking, and [have] built-in biases that can manifest themselves in entirely unknown ways leading to discriminatory outcomes or behavior."[125] Humans are not perfect, and therefore AVs are not perfect. Finally, AVs have cyber vulnerabilities and are vulnerable to standard cyberattack mechanisms[126] through their physical network interfaces, and wireless

---

[122] Sever and Contissa, "Automated Driving Regulations – Where Are We Now?"

[123] John M. Scanlon et al., "Benchmarks for Retrospective Automated Driving System Crash Rate Analysis Using Police-Reported Crash Data," *Traffic Injury Prevention* 25, no. sup1 (November 2024): 7, https://doi.org/10.1080/15389588.2024.2380522.

[124] Scanlon et al., "Benchmarks for Retrospective Automated Driving System Crash Rate Analysis Using Police-Reported Crash Data."

[125] Turi and Lekhi, *Innovation, Sustainability, and Technological Megatrends in the Face of Uncertainties*.

[126] Some standard cyberattack mechanisms include malware and software exploits, Man in the Middle (MitM) attacks, Denial of Service (DoS) attacks, and unauthorized access and data breaches.

interfaces like Bluetooth, smart keyless technology, and telematics systems which "integrate telecommunications and informatics for intelligent applications in vehicles."[127] Not only is the integrated automotive supply chain especially vulnerable, but AVs also have communications equipment and relay-based vulnerabilities, and can be attacked or spoofed through their GPS signal and other sensors.[128] Consequences of cyberattacks on AVs include identity theft and data breaches, car theft, and a loss of physical control; these risks extend beyond data privacy into physical safety making cybersecurity a critical component of ethical and technical oversight.

In both civilian and military contexts, AVs and UASs rely on similar sensors, AI models, and communication systems that function cohesively to ensure accurate, timely decision making. These systems are dynamic, requiring constant updates and maintenance because sustaining reliability is just as important to overall safety as the initial design.[129] Even though companies may try to limit proprietary information, AV systems and vulnerabilities are studied, and significant research is openly available. As equivalent testing on military systems might be classified and inherent similarities, AVs are an excellent source to study the underlying technical architecture, vulnerabilities, and risks. Understanding this shared foundation is essential to evaluating how to establish accountability and meaningful human control. With a technical grounding established, the next section explores how accountability is addressed in practice through liability, insurance models and fault attribution. Civilian AVs continue to offer insight into how society manages accountability in autonomous systems and provide lessons for military applications where the consequences can be more extreme.

---

[127] Transport Canada, *Transport Canada's Vehicle Cyber Security Strategy* (Ottawa: Transport Canada = Transports Canada, 2021).

[128] Tiwari, Rajasekar, and Wang, "A Survey."

[129] Cummings, "What Self-Driving Cars Tell Us About AI Risks."

4.4 – Liability and Insurance: Who's to Blame When Nobody's Driving?

> *I have a long list of quibbles with, and outright objections to, this proposal [for a new AV insurance plan], thoughtful and comprehensive as it is*
> - Adam F. Scales, 'Not So Fast: A Brief Plea for Muddling Through the Problems of Autonomous Vehicle Liability', 20.

Accountability in autonomous platforms requires systems designed with transparency, ethical standards, and auditability: the ability to assign blame after assessing what happened. Liability and insurance are an open issue for AVs at SAE levels 3, 4 and 5 which reflects levels of autonomy where the AV is driving rather than the driver. Who is responsible in an accident involving an AV: the owner, the driver, the manufacturer, the developer, the maintainer, the infrastructure provider? What about potential interactions with and liability related to other vehicles or smart city infrastructure (V2X) which informs AV decisions? Today's accident reconstruction and forensic methods like calculating trajectories and measuring tire tracks are a good starting point to determine causality, and AVs involved in accidents and smart infrastructure will add system audits of sensors and decision making, possibly through XAI methods.[130] To be useful however, AVs need to work in the real world which involves interpreting and interpolating information from sensors and thus making decisions based on incomplete or uncertain information.[131] In the face of complex accident causality, fault attribution and powerful industries, liability for AVs is more complex than simple ethical accountability.

There are ongoing debates about the best insurance frameworks for an AV landscape: strict liability, product liability, no-fault, comparative fault, usage-based, and national systems of

---

[130] Christoph Bartneck et al., *An Introduction to Ethics in Robotics and AI*, SpringerBriefs in Ethics (Cham: Springer International Publishing, 2021), https://doi.org/10.1007/978-3-030-51110-4.

[131] Atakishiyev, Salameh, and Goebel, "Safety Implications of Explainable Artificial Intelligence in End-to-End Autonomous Driving."

Manufacturer Enterprise Responsibility.[132] Each position has different risks and accountability frameworks which could shape societal norms through restitution processes and innovation risks. If the manufacturer or maintainer is liable, despite offloading costs to consumers, they will be cautious with upgrades and deploying new technology. If owners or drivers are liable, they may avoid purchasing new technology and general adoption could stall. No single approach has yet emerged, but critical liability questions need to be answered: who decides? Who answers? And most tellingly, who pays? For insurance, the question is always answered by who pays.

As civilian AVs continue to push the boundaries of autonomy, questions of liability offer early insight into how societies may navigate responsibility when the driver is no longer human which can also inform discussions about military applications. Although AV insurance frameworks do not directly map to military contexts, it presents questions relevant in both civilian and military contexts: who is responsible when autonomous systems cause harm? What role does intent play in assigning blame? The technical enablers and the oversight gaps also apply to military applications, particularly in the development of LAWSs. In this way, civilian AV development offers both a predictive signal and a preventative opportunity, revealing how autonomy challenges human control, and how institutional frameworks must evolve in tandem with technical capacity.

In a military scenario, the ability to accurately assign blame could make it less necessary to do so: clarity and traceability become forms of risk deterrence. Generally, when people know their actions are being watched by an observer or recorded through audit trails, XAI methods, or

---

[132] Adam F. Scales, "*Not So Fast* : A Brief Plea for Muddling Through the Problems of Autonomous Vehicle Liability," *Journal of Tort Law* 13, no. 2 (November 18, 2020): 189–95, https://doi.org/10.1515/jtl-2020-2012.

CCTV, they tend to "act in a more prosocial manner" which is known as the audience effect.[133] Germany is applying this concept requiring event data recorders in all new vehicles; [134] it will encourage humans drivers to make law-abiding decisions, and it will provide AV stakeholders an independent accounting of events. Because autonomy of military UASs is a byproduct rather than the core requirement, operators managing systems that have embedded traceability are more likely to behave within legal and ethical boundaries. Traceability can reinforce the integrity of command structures by providing documented chains of decision-making, ensuring that accountability can be appropriately distributed across operators, commanders, and system developers. On the international stage, attribution mechanisms reduce plausible deniability, increasing the diplomatic and legal risks of unlawful action, and thereby strengthening emerging norms associated with responsible use of autonomous systems. Most importantly, embedding traceability into design contributes to making the principle of meaningful human control enforceable rather than aspirational rhetoric. Despite such positive attributes, this type of accountability has significant limitations. Traceability will probably only be effective with militaries that already respect IHL and will benefits of the audience effect disappear once an autonomous platform is released on a mission.

Ultimately, as AVs grow in autonomy, they act not only as a testbed for technical systems, but as a preview for how society assigns responsibility and ensures ethical safeguards in a future where control may lie in code, rather than human hands. XAI and other traceability methods could be a foundation to enable responsible use of LAWSs despite the UN's current

---

[133] Kiley Seymour, Jarrod McNicoll, and Roger Koenig-Robert, "Big Brother: The Effects of Surveillance on Fundamental Aspects of Social Vision," *Neuroscience of Consciousness* 2024, no. 1 (December 10, 2024): niae039, https://doi.org/10.1093/nc/niae039.

[134] Sever and Contissa, "Automated Driving Regulations – Where Are We Now?"

condemnation.[135] Recall from earlier that the lack of a LAWS definition hampers UN condemnation because it muddies the water as to what is being condemned. From a military perspective, the questions about responsibility and intent are about morality and legal responsibility, but if the legal and social mechanisms for accountability are not established and tested in the civilian domain, they will be even harder to impose in high-stakes military contexts where autonomous systems deliberately act with lethal force.

4.5 – Conclusion: Lessons Learned, Lessons Observed?

> *Let's step back for a moment. Forget these complications, and focus on what I assume for most is the vision of the future that comes to mind most readily. People riding in robot cars*
>
> - Adam F. Scales, 'Not So Fast: A Brief Plea for Muddling Through the Problems of Autonomous Vehicle Liability', 20.

AVs, a method of transportation and a system of convenience, represent more than a transit upgrade. They are an AI application and forerunner of UASs. Chapter four unpacks AV technology; a tangible manifestation of the trolley problem discussed in chapter two. Though AV oversight frameworks remain incomplete, the very act of grappling with these challenges through legislation, insurance models, and social norms demonstrates that adaptation is possible. Importantly, AVs illustrate that accountability in autonomous systems is not a static feature but an evolving negotiation between design, policy, and public trust. AVs are active testbeds for how societies respond to the delegation of human agency, how legal systems evolve under technological pressure, and how institutions manage decision-making uncertainty with respect to AI and humans.

---

[135] Scales, "*Not So Fast*."

As AVs evolve, they offer insight into as autonomy as the line between human control and machine decision-making blurs. In civilian scenarios, these questions are being resolved through regulatory evolution and industry practice. In military contexts, where force is intentional and consequences can be fatal, the stakes are higher, but the conceptual questions are strikingly similar: how do we preserve accountability when a machine is in control? With both technologies involving lethality, either coincidentally like AVs or purposefully like military UAS, the way society handles AVs and oversight requirements will set expectations and precedence for autonomous military systems.

Doubtless, a combination of industry demands and trial and error will eventually lead to a working insurance framework for AVs long before the UN finalizes a definition or creates a legally binding instrument for LAWSs. In this way, AVs act not just as a proving ground for technical systems, but as society's dress rehearsal for assigning blame, maintaining ethical oversight, and upholding accountability in a future where we travel like the Jetsons (Figure 18). As military UAS development accelerates, lessons from civilian AVs offer insight into the technical morass of diffused responsibility that challenges accountability in armed conflict which is examined in the next chapter through UASs.

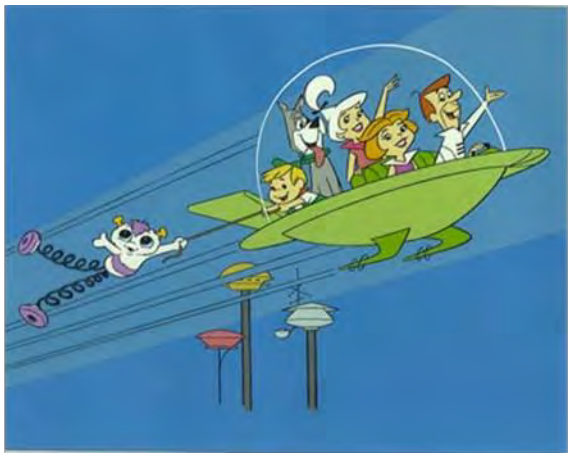


Figure 18 – A Superficially Utopian Future: Living Like the Jetsons
Source: https://hanna-barbera.fandom.com/wiki/The_Jetsons

CHAPTER 5 -LEFT OF LAUNCH: AUTONOMY, UAS, AND THE CAF

5.1 – Introduction: Where Autonomy, Accountability and Application Converge

> *Every once in a while, a new weapon, a new technology comes along that changes things. Einstein wrote a letter to Roosevelt in the 1930s saying that there is this new technology—nuclear weapons—that could change war, which it clearly did. I would argue that [AI-powered] autonomy and decentralized, distributed systems are that powerful.*
>
> - Eric Schmidt, 'Interview with Wired', 23.

UASs are increasingly deployed for military ISR and targeting tasks, advancing toward full autonomy in lethal engagements. While AVs and UASs operate in different environments, they share core technologies: sensor fusion, real-time decision-making, advanced navigation, and variable levels of human control. AVs serve as a useful conceptual springboard for understanding UAS capabilities and for framing the governance challenges surrounding autonomous warfare. Like AVs, military UASs challenge long-held assumptions about responsibility and control, but with higher stakes. As autonomy expands, so too does the urgency of establishing clear frameworks for legal oversight, operational accountability, and meaningful human control.

This section analyzes military UAS development progressing from foundational technologies to strategic implications and institutional responses. It begins with an overview of the commercial platforms and technical building blocks that underpin military UAS capabilities, setting the stage for understanding how COTS systems have accelerated the autonomy shift. Then, examining UAS use in recent conflict, specifically in Ukraine and the Red Sea demonstrate how cheap and commercially available UASs are reshaping battlefield dynamics, altering threat geometries, and accelerating tactical innovation. Building on that, the next section explores how critical infrastructure, strategic platform control, and the influence of Big Tech affect military application of autonomous systems. Finally, it turns to institutional responses, assessing how modern militaries, including the CAF, are incorporating UASs and how these

decisions reflect broader ethical and accountability concerns. Together, this chapter shows how UAS evolution operationalizes the tensions explored earlier between military exigency, meaningful human control, and the growing need for embedded, technically grounded accountability mechanisms.

5.2 – UAS Civilian Systems and Technology Background

Understanding the technical foundation of UAS is essential for evaluating the risks and oversight challenges posted by increasing autonomy. These fundamentals offer a baseline for the ongoing discussion related to how autonomy, when layered onto these systems, complicates traditional accountability mechanisms. Focusing on commercial UAS and their technological foundation, this section outlines the underlying architecture from hardware components to communication links that enable UAS functionality and shapes the degree to which human operators remain in the loop. Like many other technological advancements, the line between commercial and military applications is thin, and advancement on either side benefits the other seen through dual-use platforms.

Commercially available UAS range wildly in price and quality; some Amazon offerings at both ends of the price spectrum are captured in Figure 19. UAS can be controlled by First Person View (FPV) systems sending an onboard video feed relay to a monitor or goggles; directly controlled by the operator, sometimes with a joystick. This type of UAS is used recreationally for drone racing and aerial photography, and commercially for visual inspections and aerial monitoring, for example in support of traffic and environmental information capture. UAS can also be controlled by Ground Control Stations (GCS) which equates to a terminal or other device where control guidance is provided by an operator, for example by programming a flight plan: automatic functionality but still human-in-the-loop.

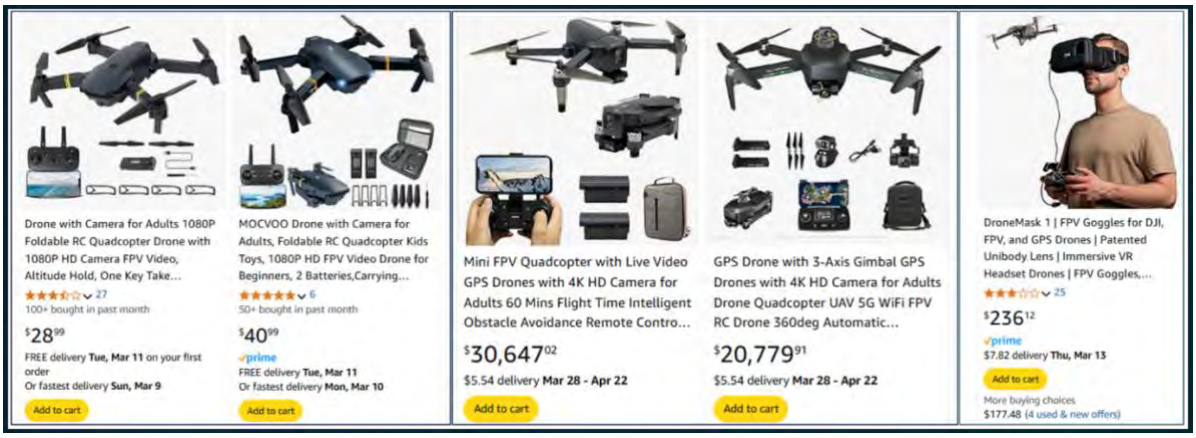


Figure 19 – Examples of Commercially Available (COTS) UASs
Source: Author created based on Amazon listed found using the search term 'FPV drone'.

Transport Canada classifies *drones* into three categories based on weight: <250g which requires no registration nor certification, 250g – 5Kg which requires registration and a license to operate, and >25kg which requires special flight operations certificate.[136] As of 2019, another Transport Canada publication, the Aeronautical Information Manual, added information about drones but referred to all categories listed above as Remotely Piloted Aircraft (RPA), or Remotely Piloted Aircraft System (RPAS) which includes the RPA, control station, and the Command and Control (C2) link.[137] The European Union Aviation Safety Agency (EASA) uses a tiered system to reflect increasing levels of risk and oversight: open category or low risk, specific category or medium risk, and certified category or high risk.[138] Because the EU is working on a long-term plan to incorporate increasingly autonomous UAS, they are in the process of amending almost all aviation regulations and the classification metrics are complex. While these categories

[136] Transport Canada, "Drone Safety," Government of Canada, March 3, 2025, https://tc.canada.ca/en/aviation/drone-safety.
[137] Transport Canada, *Aeronautical Information Manual (AIM)*, vol. Effective 0901Z, October 3, 2024 to 0901Z, March 20, 20254, TP 14371E, n.d., https://tc.canada.ca/sites/default/files/2024-09/aim-2024-2_access_e.pdf.
[138] EASA, "European Union Aviation Safety Agency," accessed May 4, 2025, https://www.easa.europa.eu/en/domains/civil-drones.

serve civilian governance, military systems follow separate, evolving classifications explored in section 5.5

As illustrated in Figure 20, non-autonomous UAS systems include a flight control unit or the *brain* of the UAS, sensors which capture live video and information for navigation, and a communications module enabling control.[139] An onboard computer or flight control unit processes navigation and sensor data, controls physical functions (i.e. the actual flying), makes decisions, and conducts any other incorporated AI-driven processes.[140] AI can be incorporated into UAS functionality by using images and data collected by the sensors to detect and respond to outliers, anomalies, patterns, and areas of interest. Another AI application involves augmenting navigation by incorporating real-time navigation and sensor data to adjust flight plans, change course unexpectedly without becoming lost, use landmarks to confirm location, and assist with autopilot functions. Data from a variety of sensors can be processed and used to avoid stationary or dynamic obstacles by predicting and reacting to possible collisions or conducting primary tasks like search and rescue. For example, LiDAR and radar collect data to map and detect objects, and a Positioning, Navigation and Timing (PNT) module[141] determines and tracks UAS locations. A communication module enables UAS C2 between the UAS and the controller or V2X-like functionality with other UASs and infrastructure. A variety of communication protocols including Bluetooth and Wi-Fi are possible, but the signal between the

---

[139] Jacob Stoner, "What Is FPV (First Person View) & How Does It Work?," FlyEye, June 5, 2024, https://www.flyeye.io/drone-acronym-fpv/.

[140] Jacob Stoner and Felicia Magdolna, "AI Guide," FlyEye, February 2025, https://www.flyeye.io/ai-powered-drone-technology/.

[141] PNT can include Global Navigation Satellite System (GNSS) which is a general term describing any satellite constellation such as the Global Positioning System (GPS) which is the North American constellation. PNT can also include Inertial Navigation Systems (INS) which uses motion sensors to continuously calculate by dead reckoning without need for an external reference. Combining multiple PNT technologies (GPS/INS/etc) creates a hybrid PNT system which is more robust.

controller and the UAS is primarily over Radio Frequency (RF) waves due to better range and interference; this chapter focuses on RF henceforth for simplicity but the concepts are signal-agnostic.[142]

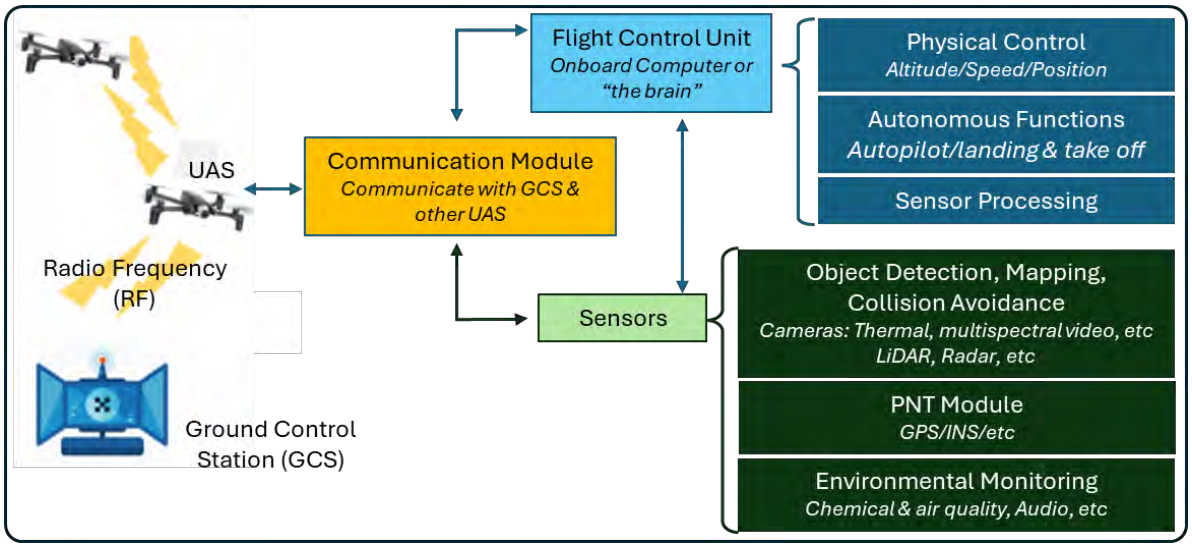


Figure 20 – UAS Components and Their Functions
Source: Adapted by author from Wen Zhang et al., Air-Ground Integrated Mobile Edge Networks: A Survey', 20.

The RF signal is an invisible tether between the controller and UAS whose fragility creates a demand for increased autonomy. That tether, when disrupted or degraded, can cause delayed or lost communication leading to erratic flight behaviour, disrupted video feed, a crash, or a *flyaway* which means the UAS flies away erratically out of sight. This disrupted or degraded signal between the controller and the UAS is caused by interference: frequency congestion, moving out of range, physical obstructions, RF interference from power lines, too many other devices, and weather conditions. In addition to coincidental or unintended interference, UAS can be targeted by Electronic Warfare (EW): RF signals being deliberately interrupted through

[142] Khaled Osmani and Detlef Schulz, "Comprehensive Investigation of Unmanned Aerial Vehicles (UAVs): An In-Depth Analysis of Avionics Systems," *Sensors* 24, no. 10 (May 11, 2024): 3064, https://doi.org/10.3390/s24103064.

jamming[143] or guidance disrupted through meaconing which involves deceptively mimicking a transponder signals.[144] For example, RF jammers overwhelm the targeted UAS by transmitting a high-powered RF signal on the frequency in use between the platform and its controller.[145] Similar to jamming, the GNSS is vulnerable to spoofing through a device which transmits on GNSS frequencies to overwhelm the GNSS receiver with false positioning and navigation such that the UAS uses the false instead of legitimate information.[146] Devices required for EW are controlled items and generally reserved for official use by the military or law enforcement.[147]

UAS and counter-UAS technology are delicately balanced as they each adapt and improve in response to the other. Basic approaches to counter EW techniques such as jamming and meaconing, include encryption and frequency hopping, or quickly switching between frequency channels.[148] More sophisticated approaches include adding sensors such as an Inertial Navigation Systems (INS), and leveraging blockchain technology to decentralize authentication and store tamper-proof flight logs. AI is also used to detect interference, assess whether interference is natural or deliberate, and react to interference which could include faster, more deliberate and adaptive frequency hopping. One potential way to circumvent EW techniques is greater automation and autonomy through AI: future LAWSs. If there is no signal tether between

---

[143] Jamming is the act of blocking a wireless device from communicating with other devices. For UAS this can inhibit the system's ability to transmit or receive signals associated with positioning and navigation, control, and sensors such as video.

[144] Meaconing and spoofing are increasingly used interchangeably. The distinction however, is that meaconing refer to deceptively mimicking a transponder signal such as faking a GPS signal, and spoofing describes a technique (which needs a digital network interface or delivery of a digital payload component which disrupts or compromises the integrity of the data) to join a network by pretending to be a legitimate client.

[145] "everythingRF," RF, Microwave & Wireless Industry, everything RF, accessed March 12, 2025, https://www.everythingrf.com.

[146] Mike Ball, "GPS/GNSS Spoofing Technology for Drones & UAS," *Unmanned Systems Technology* (blog), 15 Nov 23, https://www.unmannedsystemstechnology.com/expo/drone-gps-spoofing/.

[147] Felicia Magdolna, "Drone Signal Jamming & Interference," FlyEye, February 17, 2025, https://www.flyeye.io/drone-technology-signal-jamming/.

[148] Magdolna, "Drone Signal Jamming & Interference."

a controller and the UAS, it cannot be disrupted. It also means there is no human control or oversight.

There is a natural escalation from control link fragility to automation to autonomy. Already the more expensive Amazons listing from Figure 19 include functions like intelligent obstacle avoidance, similar to lane assist or adaptive cruise control and correlating to technology associated with SAE levels one and two. Although lacking precise definitions related to autonomy like SAE levels for AVs, UAS exists along a spectrum of automation and autonomy. According to the EASA:

> An *autonomous* drone is able to conduct a safe flight without the intervention of a pilot. It does so with the help of artificial intelligence, enabling it to cope with all kinds of unforeseen and unpredictable emergency situations. This is different from *automatic* operations, where the drone flies pre-determined routes defined by the drone operator before starting the flight. For this type of drone, it is essential for the remote pilot to take control of the drone to intervene in unforeseen events for which the drone has not been programmed.[149]

Already high-end human-in-the-loop systems rely on automation which can be activated deliberately or as a fail-safe function in the event of a control link failure.

As UAS capabilities are refined, attention is turning to the next frontier: intelligent, networked systems operating collaboratively or autonomously. Swarming technologies and Urban Air Mobility (UAM) technology which could link into V2X infrastructure discussed in chapter 4, are enabled by advances in AI and communication infrastructure, and represent a major evolution in how airspace could be managed and contested in both urban civilian environments and battlefield conditions. UAS swarms are networked UASs using AI to

---

[149] EASA, "FAQ > Drones (UAS)," European Union Aviation Safety Agency, n.d., https://www.easa.europa.eu/en/the-agency/faqs/drones-uas#category-regulations-on-uas-drone-explained.

collaboratively leverage communication and task allocation to achieve common goals.[150] Illustrated in Figure 21 and currently used for light shows and entertainment, emerging civilian applications include environmental monitoring and precision agriculture. Meanwhile, UAM enthusiasts envision integrating UAS into smart cities for low-altitude traffic management and logistics. These avenues of development demonstrate how AI extends UAS functionality beyond basic remote control and furthers capabilities with both civilian and military applications and implications related to governance, ethics and control.

Figure 21 – Examples of Swarm Technology in Reality (Light Show; Left) and Fiction (Spider Man, Far from Home; Right)

Source: (left) https://tulipfestival.ca/drone-show and (right)https://www.imageworks.com/our-craft/vfx/movies/spider-man-far-home

Understanding how UASs work is foundational to grasping future legal and ethical challenges associated with military applications, while simultaneously highlighting a requirement for greater autonomy to circumvent control link fragility. As autonomy increases, responsibility attribution becomes proportionally more difficult underscoring how emerging military technology does not easily fit into existing accountability frameworks but rather outpaces them entirely. Understanding the theoretical underpinnings of UAS is therefore essential to not only analyze how they function, but also to anticipate how they might be used in practice. The next section turns to current operational realities, exploring how UAS are deployed in contemporary

[150] Stoner and Magdolna, "AI Guide."

military contexts and the tensions they expose between technical capability, policy, and the LOAC.

5.3 –Improvised Air Power: Cheap, Deadly, Decisive, DIY

> *Soldiers have learned to fear the ominous buzz of the drone's propellers overhead.*
> - Zafra et al., 'How Drone Combat in Ukraine is Changing Warfare', 24.

Although automated and AI-enabled autonomous UAS platforms provide potential solutions to the vulnerabilities associated with RF or other control-link dependent systems, most UAS platforms used in today's active conflicts are instead cheap and unsophisticated. Combatants rely on COTS technology: technically rudimentary but strategically effective. This mismatch between theoretical capability and operational reality reveals how civilian technology, and the innovation required to use it in a military context, is shaping the evolution of modern conflict. By examining how COTS-based UASs are deployed in live conflicts, particularly in Ukraine and the Red Sea, this section illustrates how even low-cost systems are disrupting traditional military doctrine, complicating legal norms, and forcing revisions in state-level defense strategies. These real-world examples underscore the theme of this paper: emergent autonomy is not a future abstraction, but a present demand unfolding through unpredictable, uneven, and globally distributed technological adoption.

UAS technology is affecting modern warfare and quickly adapting to changing situations. Comparing American military UAS use in the 2000s against two ongoing military conflicts highlights a zeitgeist shift in UAS use in a military context. Cheaper than traditional aircraft, two of the most well-known American UASs during the 2000s, the Predator and Reaper have

wingspans of 36 and 41 feet, are complex and worth millions.[151] In contrast, Ukrainians, Russians and the Houthis often use cheap hand-held COTS UAS and focus on quantity versus quality. For example, the Iranian made Shahed 136 UAS, a loitering ammunition UAS primarily designed for suicide or kamikaze ground attacks was used by the Houthi groups as early as 2020,[152] and by Russia to attack Ukrainian power grids in December 2022.[153]

During the early 2000s, the West and the Middle East perceived UAS use very differently. Western use of "hunter-killer drones" increased significantly year over year[154] and performed a variety of functions including Intelligence, Surveillance and Reconnaissance (ISR) functions to identify individuals, striking unidentified individuals based on intelligence, and targeting equipment and facilities.[155] Lauded by the West as "the only good thing to come out of the war on terrorism,"[156] UAS technology was perceived as a surgically precise lever to exert force without risking troops. However, the collateral damage was significant. UAS strikes against Al-Qaeda had a three percent success rate and Pakistani civilian casualties skyrocketed: a UN report identified that US air strikes encouraged Taliban recruits and suicide bombers.[157]

---

[151] Cameron Manley, "Houthi Rebel Footage Appears to Show a Downed US Reaper Drone Worth $30 Million," June 1, 2024, https://www.businessinsider.com/houthis-downed-3rd-us-reaper-drone-worth-30m-1-month-2024-5#:~:text=Related%20stories,unit%20costs%20around%20%2430%20million.

[152] Army Recognition Group, "Shahed-136; Loitering Munition/Kamikaze-Suicide Drone - Iran," Global Defense News, March 12, 2025, https://armyrecognition.com/military-products/army/unmanned-systems/unmanned-aerial-vehicles/shahed-136-loitering-munition-kamikaze-suicide-drone-technical-data.

[153] Nick Starkov, "Russia Drones Smash Power Network In Odesa," *Reuters*, December 11, 2022, https://www.reuters.com/world/europe/russian-drone-attacks-target-power-network-ukraines-odesa-officials-2022-12-10/.

[154] Jeffrey A. Sluka, "Death from Above: UAVs and Losing Hearts and Minds," *Military Review* March-April (2013), https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20130430_art013.pdf.

[155] John W. Rollins, "Armed Drones: Evolution as a Counterterrorism Tool" (Congressional Research Service, November 7, 2023), https://www.congress.gov/crs-product/IF12342.

[156] Sluka, "Death from Above: UAVs and Losing Hearts and Minds."

[157] Sluka, "Death from Above: UAVs and Losing Hearts and Minds."

Perceived Western success was perceived very negatively by those living in the operating area and negatively affected the goal of winning hearts and minds.

Western military UAS fleets are still large and expensive today even though the economics of disposable COTS UASs are illustrated by the ongoing actions of the Houthis in Yemen.[158] After Hamas' 7 October 2023 surprise attack on Israel, the Houthis began signaling their interest in that conflict which escalated into an announcement of formally entering the war at the end of October in support of Palestine accompanied by missiles and UASs launched at Israel.[159] In November, the Houthis attacked the first of many commercial ships as part of their support to Gaza. Consequently, the US, UK and France deployed ships to the Red Sea for intercept missions and to restore international shipping stability.

Foreshadowed by the asymmetric warfare in the Middle East in the 2000s, where the Western nations struggled to address cheap weapons such as IEDs and suicide bombing, the conflict in the Red Sea is similarly challenging. The Houthis use relatively inexpensive and sometimes homemade UASs and missiles[160] which the western coalition intercepts. To date, the western coalition has spent over a billion dollars on munitions for this purpose and the Under Secretary of Defense for Acquisition and Sustainment described the situation as a "wildly unbalanced" equation because the US was systemically shooting down $50,000 one-way drones with multi-million-dollar missiles. This economic mismatch highlights a core vulnerability in modern military budgeting: highly capable but expensive platforms are being drained by an

---

[158] The Houthi tribe, which has a horrific human rights record and is backed by Iran, positions themselves against corruption in Yemen, Saudi meddling, and are the sworn enemies of Al Qaeda and Israel. A Houthi slogan summarizes their priorities as "God is Great, Death to America, Death to Israel, Curse on the Jews, Victory to Islam."[158]

[159] Center for Preventive Action, "Conflict in Yemen and the Red Sea," October 8, 2024, https://www.cfr.org/global-conflict-tracker/conflict/war-yemen.

[160] Center for Preventive Action, "Conflict in Yemen and the Red Sea."

endless stream of low-cost, disposable threats. If this asymmetry continues, it could undermine the long-term sustainability of high-tech deterrence models.[161] These conflicts demonstrate how technology enables less-professional militaries; scale and might is no longer the single path to victory. Like many western militaries with stringent regulations and cumbersome procurement processes, the United States' military procurement has been accused of "spending the defense budget on the wrong things"[162] and needing to refocus because "cost per unit matters."[163] Their Department of Defense (DoD), with the largest military budget in the world, is working on lower-cost weapons such as loitering munitions for single-use attacks, cheaper cruise missiles, and laser or directed-energy weapons.

In another part of the world, Russia and Ukraine are at the cutting edge of UAS military development because of their ongoing conflict. Neither side has achieved air superiority and UAS technology is filling the gap as a "poor man's air force" to effect strategic level military effects.[164] The common COTS UASs are difficult to defend against or identify on radar due their speed and lack of consistent size, shape and materials.[165] In fact, Ukraine's Ministry of Digital Transformation, partnered with NGOs, solicits recreational level FPV UASs from around the world, which the ministry sends to Ukrainian forces on the front line.[166] Once deployed, COTS UASs are largely considered disposable.

---

[161] Nicholas Slayton, "Cheap Houthi Drones Are Draining the Pentagon's Coffers," *New Lines Magazine*, July 29, 2024, https://newlinesmag.com/argument/cheap-houthi-drones-are-draining-the-pentagons-coffers/.

[162] Raj M. Shah and Christopher Kirchhoff, *Unit X: How the Pentagon and Silicon Valley Are Transforming the Future of War*, First Scribner hardcover edition (New York: Scribner, 2024).

[163] Slayton, "Cheap Houthi Drones Are Draining the Pentagon's Coffers."

[164] Australian Defence Force and Ryan Hodson, "The Weaponization of Toys and Implications for the Air Force," *Air/Space* 3 (2024): bp41568060, https://doi.org/10.58930/bp41568060.

[165] Australian Defence Force and Hodson, "The Weaponization of Toys and Implications for the Air Force."

[166] Ukrainian World Congress and Ministry of Digital Transformation of Ukraine, "Army of Drones," Ukrainian World Congress, accessed January 7, 2025, https://www.ukrainianworldcongress.org/united24/.

Since 2022, Ukraine's UAS use has skyrocketed to "100,000 explosive first-person-view drones a month."[167] Not only are they used for surveillance, but they are also adapted into lethal weapons by zap strapping small warheads to the frame for suicide missions (Figure 22, left). Even though a UAS-attached warhead has less explosive power, it is cheaper than a single artillery shell and the economic value is compounded by the fact that UASs are more accurate, especially against moving targets, and thus require fewer rounds overall. As each side adapts to defensive counter-UAS technology, new ways of using UAS in a military setting emerge. For example, to overcome RF jamming, both sides created un-jammable UAS by attaching a fishing reel-type contraption to spool out fibre-optic cable as a physical control link (Figure 22 right).[168] This battlefield ingenuity outpaces doctrine and demonstrates how innovation often arises out of necessity rather than planning. These new approaches foreshadow how military applications of UASs might evolve in unexpected ways; shaped not by formal doctrine, policy choices and methodical testing, but by real-world circumstances and escalating tactical improvisation.

---

[167] David Axe, "A Two-Pound Ukrainian Drone May Have Shot Down a 12-Ton Russian Helicopter," *Forbes*, July 31, 2024, sec. Aerospace & Defense, https://www.forbes.com/sites/davidaxe/2024/07/31/a-two-pound-ukrainian-drone-just-shot-down-a-12-ton-russian-helicopter/.

[168] David Hambling, "Ukraine Fiels Unjammable Fiber Optic FPV Attack Drone," *Forbes*, November 7, 2024, https://www.forbes.com/sites/davidhambling/2024/11/07/ukraine-fields-reboff-unjammable-fiber-optic-fpv-attack-drone/.

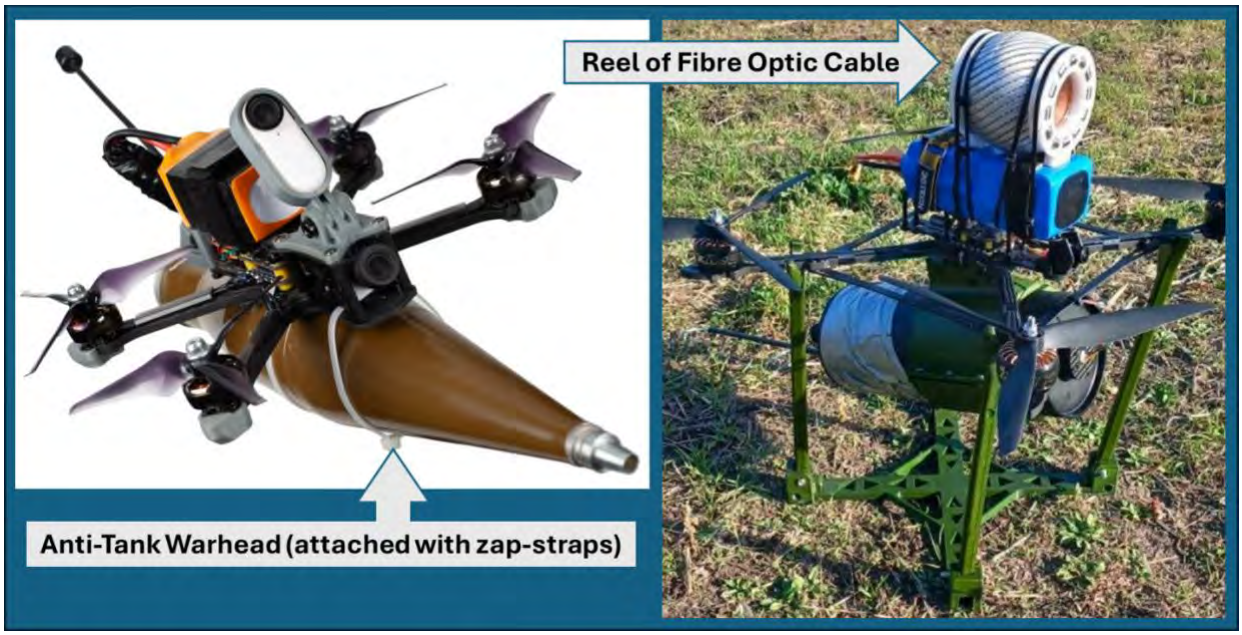


Figure 22 – Examples of Improvised UAS from Ukrainian Conflict
Source: Author created based on photos from Hodson, 'The Weaponisation of Toys and Implications for the Airforce', 24. and Hambling 'Ukraine Fields Unjammable Fiber Optic FPV Attack Drone' 24.

Constant UAS use in Ukraine is pushing technology and innovation forward through trial and error with both failures and successes measured in blood. Ukrainian UAS use between 2022 and 2024 went from inconsistent to indispensable: currently capabilities are embedded into most units at the tactical level.[169] They attack Russian targets by "flying drones into the open hatches of armored personnel carriers, under the add-on armor on so-called 'turtle tanks' and through the doors of reinforced infantry dugouts."[170] Most of the information available reflects the Ukrainian perspective for obvious reasons, and one article documents that a two-pound quadcopter may have taken down a Russian Mi-8 helicopter just after take-off which was posted on social media (Figure 23.)[171] One of the most recent innovations relates to captured UASs infecting the other

[169] Mariano Zafra et al., "How Drone Combat in Ukraine Is Changing Warfare," *Reuters*, March 26, 2024, https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/.
[170] Axe, "A Two-Pound Ukrainian Drone May Have Shot Down a 12-Ton Russian Helicopter."
[171] Axe, "A Two-Pound Ukrainian Drone May Have Shot Down a 12-Ton Russian Helicopter."

sides' systems to prevent repurposing, hide the original operator's location, and limit enemy analysis of technology to find and exploit vulnerabilities.[172]

Figure 23 – Tweet of Russian Helicopter Allegedly Taken Down by Ukrainian UAS in 2024
Source: Axe, 'A Two-Pound Ukrainian Drone May Have Shot Down a 12-Ton Russian Helicopter', 24.

Ukraine's current approach to military procurement and acquisition involves "innovators working side by side with soldiers at the front, new kinds of weapons made in garage shops rushed into battle, [and] software being updated on a daily basis."[173] Low cost per unit is a key requirement such that new capabilities or approaches can be applied at scale.[174] Ukraine is already using UAS with AI and, thus far, maintains human oversight to "help spot targets or

---

[172] Vikram Mittal, "Russians Capture Ukrainian Drones Which Infect Their Systems With Malware," April 2, 2025, https://www.forbes.com/sites/vikrammittal/2025/04/02/russians-capture-ukrainian-drones-which-infect-their-systems-with-malware/.

[173] Shah and Kirchhoff, *Unit X*.

[174] Max Hunder, "Ukraine Rushes to Create AI-Enabled War Drones," *Reuters*, July 18, 2024, https://www.reuters.com/technology/artificial-intelligence/ukraine-rushes-create-ai-enabled-war-drones-2024-07-18/.

threats and plan possible routes."[175] However, ceding direct human control is seen as the answer to avoid EW countermeasures and both Russia and Ukraine are openly and actively working towards AI-enabled and fully autonomous military UAS to work in swarms and remove the vulnerabilities of an RF signal or dragging fibre-optic cables. These combatants use what they have and cobble together technical and tactical approaches. Soldiers are adapting on the fly with little care for secure supply chains, survivability, detailed experimental planning or scientific approaches. With each new technical or tactical breakthrough eventually being met with countermeasures, it creates a constant loop of forced and reactive creativity. Consequently, military UASs in the Ukrainian and Houthis conflicts are possibly the most visible precursor to future LAWSs. Once low-cost autonomous UASs are developed and deployed, the UN will find it exponentially more difficult to regulate.

The world is watching the Ukrainian and Houthis situations highlighting how fast UAS development is progressing. Ukraine's previous commander-in-chief and current ambassador to UK recently wrote an article which calls out Western militaries as being stuck in the previous paradigm. Specifically:

> Lulled by decades of multi-domain dominance, Western militaries have slumbered too long. Meeting adversaries armed with mass-deployed, attrition-optimized autonomous weapons they may end up as the proverbial victims of the German WW2 Blitzkrieg. Fortunately, they have a gift of immeasurable value: Ukraine's hard-won expertise, forged in a grueling fight for survival. If the West wishes to survive, it must swiftly and fully embrace these lessons, and use them well.[176]

---

[175] Hunder, "Ukraine Rushes to Create AI-Enabled War Drones."

[176] Valerii Zaluzhnyi, "How Drones, Data and AI Transformed Our Military - and Why the US Must Follow Suit," *Defense One*, April 10, 2025, https://www.defenseone.com/ideas/2025/04/how-drones-data-and-ai-transformed-our-militaryand-why-us-must-follow-suit/404444/.

These case studies illustrate that the disruptive potential of UASs is not confined to high-end, AI-integrated military-specific platforms. Rather, demand for greater automation and autonomy is emerging across multiple environments and situations: at scale, in networked decision-making, and low-cost platforms. The legal and ethical implications are no less significant for being technologically modest; indeed, the overt goal of reducing human control in these deployments challenge existing accountability frameworks just as profoundly, underscoring the urgent need for legal and policy architectures. The following section explores UASs in Western military scenarios and the associated accountability challenges.

5.4 – Strategic Infrastructure and Its Control

> *In an effort to eliminate the possibility of any rival growing up, some monopolists would sacrifice democracy itself*
>
> - Henry Wallace, former American Vice President

While Ukrainian and Houthi forces demonstrate that even low-cost COTS UASs can shift battlefield dynamics, many governments and military organizations are developing more advanced and purpose-built systems which rely on cloud computing and infrastructure similar to V2X infrastructure for AVs discussed in chapter 4. Control over the digital infrastructure these systems rely on is becoming strategically relevant. The next section examines emerging dependencies on private platforms raising new concerns about accountability and control, again paralleling concepts raised in chapter 4. In a future LAWS context, who owns and controls infrastructure-supporting platforms may become as important as a platform's inherent capabilities.

First, as AI technologies become integrated into essential functions, maintenance and updates become essential to ensure ongoing functionality which requires ongoing investment. While ongoing maintenance and costs exist, subscription and as-a-service business models are

proving to be more lucrative for companies and the practice is moving into all areas.[177] For example, in the automative industry there was the short lived BMW attempt to charge monthly for heated seats, and the more successful technology based subscription packages include 5G data connectivity, autonomous parking functionality, and increased electric car performance.[178] This foreshadows how companies can and will turn off capabilities, perhaps even safety features or military capabilities in a pay-to-use subscription model.

Consider how Big Tech's integrated ecosystems allows them to function simultaneously as gatekeepers and competitors with AI technology while almost "every startup, new entrant, and even AI research…[is] dependent on these [Big Tech] firms."[179] Figure 24 (left) illustrates Big Tech's exponential market growth which is mirrored by a similar trajectory of government reliance on those companies as per Figure 24 (right).[180] For all the same reasons that other entities use Big Tech ecosystems, so too do governments, including the governments of both the US and Canada. This convergence raises key questions: if government security departments, potentially even the militaries, rely on Big Tech infrastructure to power AI systems, who ultimately controls the C2 infrastructure and thus the platforms themselves?

---

[177] Phani Nagarjuna, "Customer Lifetime Value and The Subscription Economy," *Forbes*, December 20, 2019, Forbes Technology Council edition, https://www.forbes.com/councils/forbestechcouncil/2019/12/20/customer-lifetime-value-and-the-subscription-economy/.

[178] Alistair Charlton, "BMW Drops Controversial Heated Seats Subscription, To Refocus on Software Services," *Forbes*, September 7, 2023.

[179] Kak, "Make No Mistake - AI Is Owned by Big Tech."

[180] Roberto J. González, *Militarizing Culture: Essays on the Warfare State* (London: Routledge, 2016), https://doi.org/10.4324/9781315424699.

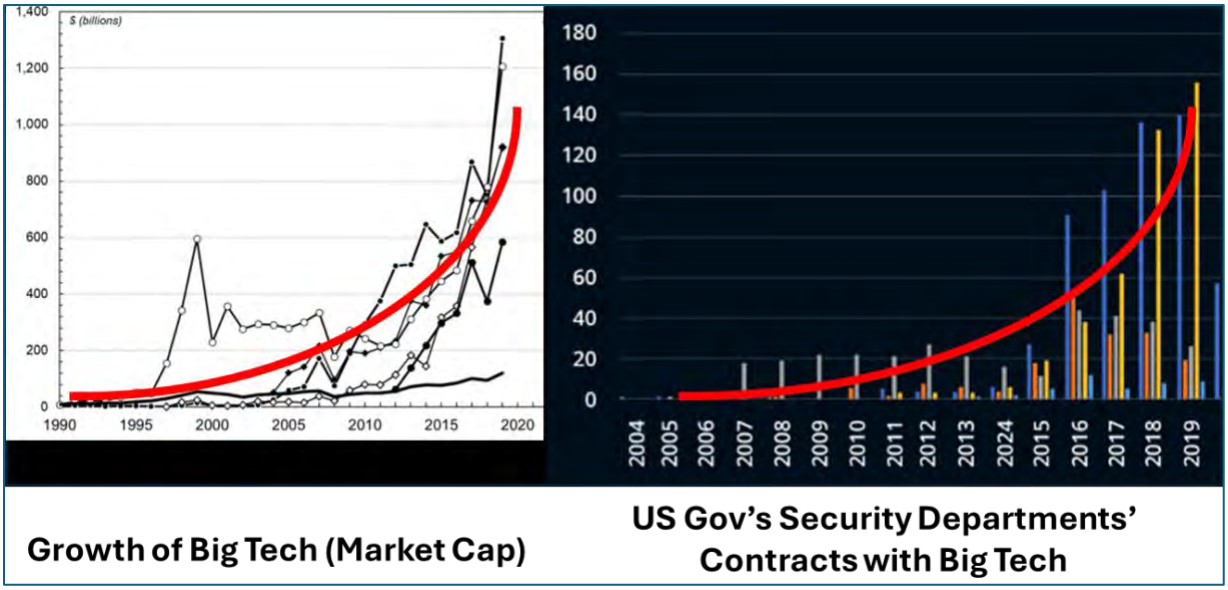


Figure 24 – Matching Exponential Growth (Red Trendline) of Big Tech's Market Value (left) and US Government Reliance on Big Tech Contracts (right)

Source: Author created using content from (left) Birch, 'Personal Data Governance in Big Tech Era: What is Happening to Our Personal Data?', 23. and (right) González, 'Militarising Big Tech', 16.

Is it pessimistic or realistic to assume that Big Tech companies will ultimately act in their own self-interest, the bottom line? In 2018 thousands of Google employees caused a media bruhaha by objecting to the company's work on Project Maven which uses AI to analyze military UAS surveillance; essentially employees were concerned about developing LAWSs.[181] Yet during the same timeframe, Google worked in partnership with the Chinse government to build AI surveillance systems, AI research and development centres, and a pre-censored Google search engine which ignored a UN resolution related to censorship.[182] In concert, Big Tech expedited the development of Chinese AI, constructed in-country data centres, and lobbied domestically for Huawei, the Chinese equivalent of a Big Tech companies. These choices are concerning because

[181] Tom Simonite, "3 Years After the Project Maven Uproar, Google Cozies to the Pentagon," *Wired*, November 18, 2021, https://www.wired.com/story/3-years-maven-uproar-google-warms-pentagon/.

[182] General Assembly, "Promotion and Protection of Human Rights in the Context of Digital Technologies" (United Nations General Assembly, December 19, 2023), https://documents.un.org/doc/undoc/gen/n23/422/28/pdf/n2342228.pdf.

of a few factors: Big Tech routinely chooses profit over principals, and these companies are both too big to police while their very size increases their impact. Considering this infrastructure may support autonomous weapons systems, such profit-driven ethical flexibility is deeply troubling.

As the Great Power Competition plays out with growing Chinese and American aggression, Big Tech's ecosystems, which are truly critical infrastructure, could affect conflict outcomes. Since 2019, American executive orders restricting Chinese hardware[183] could force other nations to choose between American and Chinese AI platform dominance. This technological crossroads will not only affect technology infrastructure, but also the AI models and data sets used; both of which are associated with the developers' values, assumptions, strategic aims, and biases. While embedded distortions will occur regardless of infrastructure, model and dataset provenance, an increasingly divisive world increases the probability of harmful bias, and makes it more likely that conflict, and thus autonomous weapons, will be used.

5.5 – UAS Military Applications

> *To stay ahead, we're going to create a new state of the art—just as America has before—leveraging attritable, autonomous systems in all domains—which are less expensive, put fewer people in the line of fire, and can be changed, updated, or improved with substantially shorter lead times.*
>
> - Deputy Secretary of Defense Kathleen Hicks, speech, 23.

As the Great Power Competition increasingly hinges on technological leverage, UASs are playing a decisive and evolving role on the battlefield. This section highlights how UASs are being used in military contexts, focusing first on global developments and then narrowing in on the CAF as a Western Military and FVEY member case study. From dual-use platforms and autonomous loitering munitions to classification trends and emerging doctrinal language, current

---

[183] Donald J. Trump, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain" (The White House, May 15, 2019), https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

practice reveals the erosion of clear distinctions between manual, automated, and autonomous weapons. These trends underscore a central argument that legal and strategic frameworks are struggling to keep pace with the rapid integration of increasingly autonomous systems.

Military capabilities using UAS technology can be divided into two groups: dual-use capabilities which have versions used for both civilian and military (Table 7), and military-only capabilities (Table 8). Table 7 provides examples of military platforms associated with dual-use categories. UASs are increasingly used to provide real-time data and ongoing situational awareness which, although civilian applications generally do not include the intelligence portion of ISR, they do include surveillance capabilities used for monitoring tasks associated with critical infrastructure, the environment, and disaster response. Another dual-use UAS application relates to logistic support and moving goods and equipment to remote or dangerous areas. The last category noted in Table 7, Chemical Biological Radiological and Nuclear (CBRN) support is often a predominantly military activity, but civilian agencies are involved.[184]

Table 7 – Dual-Use (Military & Civilian) UAS Task Categories

Category	Purpose	(Military) Examples
ISR: Intelligence, Surveillance & Reconnaissance	Collect, process, disseminate. Monitor area of operation, collect intelligence, real-time data. C2. Search and Rescue. Concerns: privacy & data collection.	MQ-9 Reaper (US), RQ-4 Global Hawk (US)
Air Mobility, Airlift Resupply, Logistics	Deliver equipment and supplies to frontlines and remote areas	TRV-150C Tactical Resupply Unmanned Aircraft System (TRUAS) - US
CBRN Support	Sensors to detect & identify chemical, biological, radiological, nuclear (CBRN) hazards. Force protection.	NATO post-Fukushima programs

Source: Author created based on information collated from manufacturer and government websites

[184] Examples of civilian agencies involved in CBRN include the pioneering work completed by the International Atomic Energy Agency (IAEA) which was tested in the Fukushima Prefecture in Japan, the site of a nuclear accident in 2011.[184]

Table 8 – Military-Specific UAS Task Categories

Category	Purpose	Examples
Application of Force	Combat/strike missions, loitering munitions, kamikaze/suicide drones, overlap with ISR Concerns about LAWS: autonomy in targeting, (human-in-the-loop versus out-of-the-loop), accountability, collateral damage	MQ-9 (US & CAN) Bayraktar TB2 (Turkey), Hero Series (Israel) CH-5 (China)
Decoy & Distract	Mimic aircraft, draw fire, confuse defenses in order to add to cognitive deception as a non-lethal strategic impact	ADM-160 MALD (US)
Electronic Warfare (EW)	Exploits electromagnetic energy to provide SA and achieve offensive and defensive effects. Examples: jam or spoof enemy communications, collect signals intelligence. Concerns: Cyber-AI overlap, ethical ambiguity, escalation risk, impact to civilian infrastructure	Orlan-10 (Russia) ADM-160 MALD (US)

Source: Author created based on information collated from manufacturer and government websites, and Global Defense Insight, 'China's Drones: CH-5 Rainbow Unmanned Combat Aerial Vehicle', 22.

Conversely, categories captured in Table 8, the application of force, decoy and distract, and EW, do not have clear civilian UAS applications for good reasons, and should remain strictly military. Of note, there is a significant overlap between military platforms that carry munitions and those that conduct ISR: for example MQ-9 is cited in both Table 7 for ISR and Table 8 for the application of force. Categories like decoy, distract, and EW, despite being important military UAS applications, have little platform-specific information available publicly facing because advertising can often diminish effectiveness.

As these capabilities evolve, they raise fundamental questions about autonomy, oversight, and decision-making. At what point does a UAS go from automatic to fully autonomous, and at each step, where is the human with regards to the loop? Although LAWSs remains pre-definition, the threshold of autonomy may have already been crossed as evidenced by the UN reported in 2023 that:

> Some States have already tested or fielded a variety of autonomous systems, including uncrewed systems capable of autonomous navigation; coordinated mobility and swarming systems; systems

> that sort and analyze intelligence data; defensive and offensive information and communications technology (ICT) systems; and simulation and training applications."[185]

Current-generation weapon systems, like those pictured in Figure 25, feature a range of autonomy which blurs the line between automation and lethal independence. From loitering munitions to defensive counter-strike platforms, might these platforms be labelled as LAWSs under a future UN definition and if so, will states relinquish them? As military UAS autonomy increases, so too does the urgency of defining control, responsibility, and governance which prompts questions about the capabilities and frameworks Canada possesses to navigate this evolving landscape.

Figure 25 – Current Weapons Systems: AEGIS, HARPY, ONIK-800, and Kargu-2
Source: Author created based on content from Naval Sea Systems Command,'AEGIS Weapon System', 21., Davidovic, 'What's Wrong with Wanting a Human in the Loop?'22., and Peremarty, 'Lethal Autonomous Weapons: Between Myths and Confusion', 23., and images found on Google.

The FVEY's militaries are pursuing UAS capabilities which we will explore through the lens of the CAF who, of this group, has the least mature UAS programme. For example, the Australian Defence Force (ADF) uses a variety of endurance and hand-launchable UAS, [186] and the UK manages its fleet across environments through their Joint Aviation Command (JAC). [187]

---

[185] Report of the Secretary General, "Current Developments in Science and Technology and Their Potential Impacts on International Security and Disarmament Efforts" (General Assembly, United Nations, August 1, 2023), https://docs.un.org/en/A/78/268.

[186] Australian Defence Force, "Uncrewed Aerial Systems," Australian Government, Defence Activities, projects, accessed January 10, 2025, https://www.defence.gov.au/defence-activities/projects/uncrewed-aerial-systems.

[187] DA Staff, "Joint Aviation Command (JAC): Overview and Capabilities," Defense Advancement, December 13, 2024, https://www.defenseadvancement.com/resources/joint-aviation-command-jac-overview-and-capabilities/.

In contrast, as of 2024 the Royal Canadian Navy (RCN) was assessed to be the least advanced of the FVEY navies with regards to uncrewed systems[188] (which includes UAS, uncrewed surface and sub-surface platforms), a deficiency the RCN is tackling by "conducting a fleet mix study, investigating which autonomous systems should be acquired to best-equip the RCN in the future battlespace."[189] In many ways Canada is lagging behind the FVEY group regarding military UAS uptake having more ambitious goals than mechanisms to deliver.

This relative gap places pressure on the CAF to adapt quickly, and Figures 26 and 27 captures the CAF's current UAS fleet managed by DLCSPM 5 whose responsibilities are expanded upon in section 5.6. Just a few years ago COTS UAS platforms appropriate for military applications did not exist, but the market responded to Ukrainian and other ongoing conflicts so there is growing availability. Similarly, CAF organizations are demanding cheaper and lower quality UAS in higher quantities, to enable more testing, more experimentation, and ultimately more applications.[190] One example involves more interest in FPV UAS, a cheaper option often used as a one-way or disposable platform, but that requires greater operator skill and training than more expensive models with GCSs.

---

[188] Which includes uncrewed systems in all environments: UAS, uncrewed surface and sub-surface platforms

[189] Kate Todd, "Lessons for Canada: Comparing Maritime Autonomous Systems Adoption Across the Five Eyes," *Triple Helix*, September 2024, https://www.cgai.ca/lessons_for_canada_comparing_maritime_autonomous_systems_adoption_across_the_five_eyes?

[190] Yan LCol Gauthier, CAF UAS Information: DLCSPM 5, April 25, 2025.

Name	Range	Purpose	Payload
Parrot ANAFI	32 min	Short-range Electro-optical (EO) Infrared (IR) • For SA in all light conditions	Cameras: • Long-wave IR (LWIR) • EO tele lens • Wide angle
Skydio X10D	40 min	• Short range recce • Thermal imaging	Cameras • Forward-looking IR (FLIR) • Thermal
Teal 2 • 1.25kg	32 min	• Short range recce • EO	Cameras: • Long-wave IR (LWIR) • EO tele lens • Wide angle
Sentry • 2.3kg	continuous	• ISR • Comms relay	• EO/IR
Teal Black Widow • 1.63kg	35min	• Short range recce • EO/IR	• Integrated EO/IR

Figure 26 –The CAF's General Purpose UAS (GPUAS) Fleet; Quadcopters
Source: Created by author based on information from a CAF presentation

Name	CU173-Raven B	CU175-Puma	CU172-Blackjack	MQ-9B
Category	Moving to Open • *Airworthiness clearance issued*	Moving to Open • *Flown on flight permits*	Specific • *Airworthiness Clearance issued*	Certified (RPAS)
Range	75 min/10 km	5.5-6.5hrs/20-60 km	16+hrs/100+ km	40+hrs/11,000km
Specification	• 4.4lbs • 4.5ft wingspan	• 23.5lbs • 15ft wingspan	• 81lbs (unloaded) • 16ft wingspan	• 4900lbs • 79ft wingspan
User	• Cdn Army (CA) units • Op Reassurance	Royal Cdn Navy (RCN) • HMCS Ottawa	CA, Royal Cdn Artillery 4th Regiment	RCAF: 1st delivery expected 2028

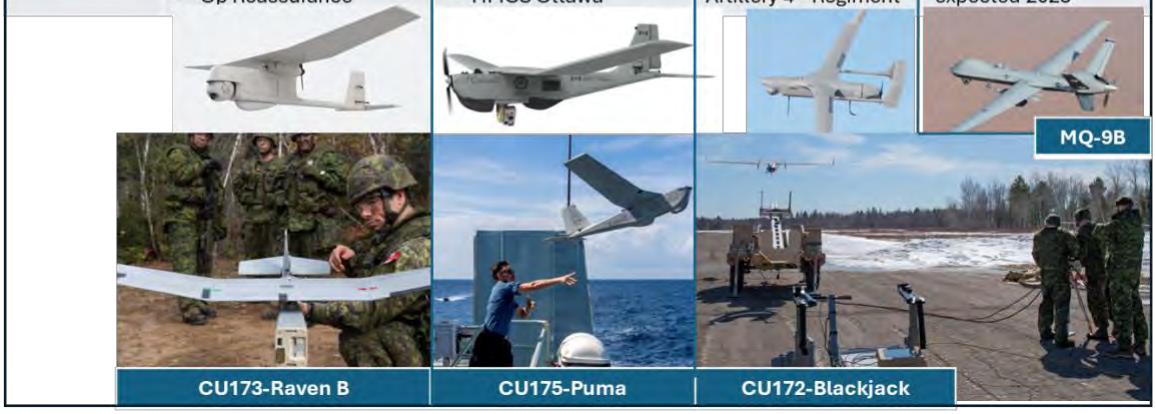


Figure 27 –The CAF's Fixed Wing UAS Fleet
Source: Created by author using combat camera photos, specifications from manufacturer websites, and a CAF presentation

The CAF has six UAS-associated projects: three major capital projects, one urgent operational requirement (UOR), one replacement project, and one minor capital project. Details about the major capital projects are captured in Figure 28. The remaining projects relate to

acquisition of a loitering munition capability for Operation *Reassurance*, UAS components of the Land ISR Modernization Project for light operations and integrating UAS into tactical vehicles for mobile operations, and purchasing and integrating COTS UAS into Arctic and Offshore Patrol Ships (AOPS). In total, all six projects are projected to cost between $1.2-$5.4 billion. As evidenced by these projects, the CAF leans towards automation rather than autonomy which aligns with their official stance on the necessity of human control for UAS platforms. [191]

Remotely Piloted Aircraft Systems (RPAS)	**Counter Uncrewed Aerial Systems (CUAS)**	***Royal Canadian Navy Intelligence, Surveillance, Target Acquisition and Reconnaissance Unmanned Aircraft System (RCN ISTAR UAS)***
Capability for airborne intelligence, surveillance & reconnaissance (ISR), and precision strikes to support CAF domestic and international operations • 11x MQ-9B long range, long endurance, armed remotely piloted • 6x ground control stations CONTRACT DETAILS: • Projected cost: $1-$4.99 Billion • Contract awarded to General Atomics on 18 December 2023 • Fisrt delivery expected 2028, and FOC expected 2030-2033 • Contracts awarded for required updates to 14 Wing Greenwood,19 Wing Comox and the Ottawa expected to be completed NLT 2028	Capability to detect and degrade/defeat non-RF hardened Class 1 UAS using sensors and non-kinetic effects • To address capability gap • To provide integrated/mobile CUAS to defeat Russian Federation Class 1 UAS threats Ensure freedom of action for Operations in the land domain for Op Reassurance Project INFO: • Projected cost: $100-249 Million • Initial delivery projected for 2024-25 fiscal year • Final delivery by the end of the 2026-27 fiscal year. • Forces deployed on Op REASURANCE	Capability for alternate airborne platform operatable from Halifax-class frigates for over the horizon, real-time ISR & target acquisition to minimize risk ISO simple -> multi-threat ops. • Shipborne vertical take-off and landing • Operate in challenging weather conditons Project INFO: • Projected cost: $50-99 Million • Definition phase in progress • Initial deliver expected 2024/25, final delivery expected 2027/28

Figure 28 –The CAF's Current Major Capital Projects Related to UAS
Source: Government of Canada Project Websites

Across a Western context, examined through the CAF, integrating UASs into military operations reflects an accelerating shift toward increasing automation and autonomy in modern warfare. Dual-use capabilities, loitering munitions, and increasingly intelligent swarms are redefining the battlefield and challenging where accountability resides given AI's impact on command and control. For Canada and its allis, these developments underscore the urgency of acquiring new capabilities and ensuring institutional frameworks support that next bound which is the focus of the next section.

---

[191] General Assembly, "General and Complete Disarmament: Lethal Autonomous Weapons Systems Report of the Secretary-General."

5.6 –The CAF's Automated Ambitions and Autonomous Future?

> *The technology will not wait for us to act. With every day that passes, it is becoming more accessible to our competitors and potential adversaries at a lower cost…Falling behind now…[risks] the loss of our operational advantage.*
> - Chief of Defence Staff General Wayne Eyre and Deputy Minister Bill Matthews, 'Department of National Defence and Canadian Armed Forces Artificial Intelligence Strategy', 24.

As militaries adapt to increasingly capable UAS platforms, institutional frameworks and support organizations often lag behind the demand signal. NATO's shifting classification terminology with which the CAF is working to align, shows efforts to standardize expectations and understanding. These institutional choices shape not only operational readiness but also sovereignty, security, and the ethical contours of military AI. This section analyzes how UASs are integrated into Western militaries by examining the CAF's approach, focusing on terminology, responsibility allocation.[192]

NATO currently defines three classes of UAS,[193] but is moving toward alignment with EASA standards of open, specific and certified; both frameworks are captured in Figure 29.[194] Already NATO documentation reflects EASA's nomenclature when describing operator and pilot training requirements which links to operational requirements and assumes human-in-the-loop control.[195] Hybrid and changing classification systems reflect parallel technology shifts in many Western militaries including the CAF whose approach to military UASs is used to ground this

---

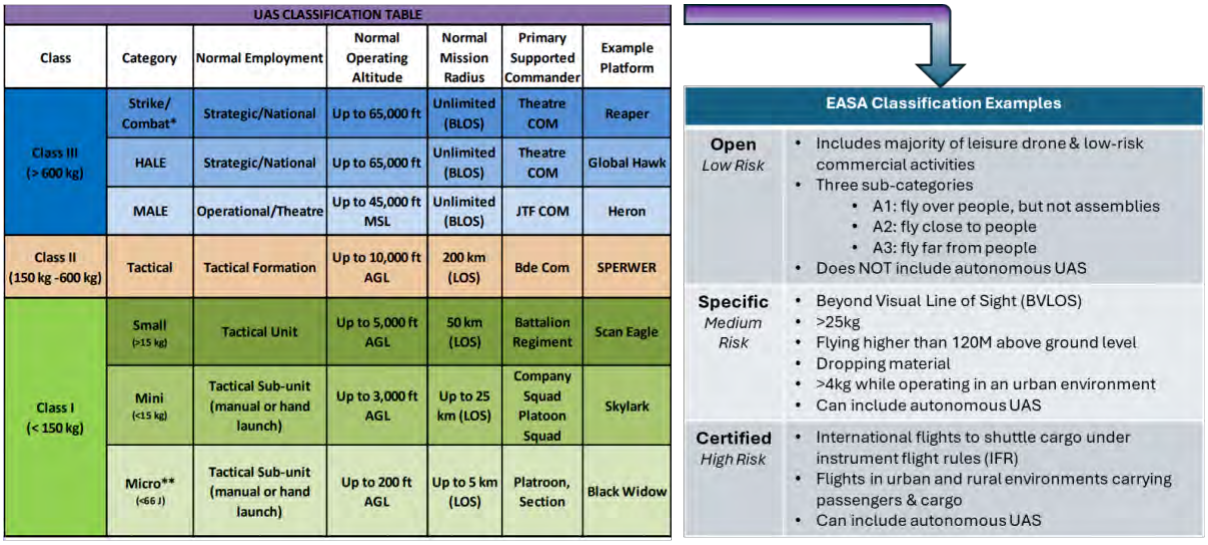
[192] DND, "Pan-Domain Force Employment Concept," 2023.

[193] John E Mayer, "State of the Art of Airworthiness Certification," *NATO Science & Technology Organization*, April 27, 2017, https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/Forms/Meeting%20Proceedings%20Document%20Set/docsethomepage.aspx?ID=42949&FolderCTID=0x0120D5200078F9E87043356C409A0D30823AFA16F602008CF184CAB7588E468F5E9FA364E05BA5&List=7e2cc123-6186-4c30-8082-1ba072228ca7&RootFolder=https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-AVT-273.

[194] Michael Shirley, "RE: Staff College Research Paper," April 29, 2025.

[195] Shirley, "RE: Staff College Research Paper," April 29, 2025.

discussion for the remainder of chapter five. Moving to align with NATO and thus EASA, the CAF uses a mix of NATO, EASA and Transport Canda terminology. In practice, the CAF relates EASA terminology of open, specific and certified to various constraints such as flight rules and air worthiness requirements.[196] NATOs moves to align with EASA, and EASA's inclusion of autonomous UASs in their specific and certified categories, reflects interest from both organizations to integrate autonomy within controlled risk thresholds, reveling growing complexity in defining responsibility across airspace, mission type, and payloads.



UAS CLASSIFICATION TABLE

Class	Category	Normal Employment	Normal Operating Altitude	Normal Mission Radius	Primary Supported Commander	Example Platform
Class III (> 600 kg)	Strike/ Combat*	Strategic/National	Up to 65,000 ft	Unlimited (BLOS)	Theatre COM	Reaper
	HALE	Strategic/National	Up to 65,000 ft	Unlimited (BLOS)	Theatre COM	Global Hawk
	MALE	Operational/Theatre	Up to 45,000 ft MSL	Unlimited (BLOS)	JTF COM	Heron
Class II (150 kg -600 kg)	Tactical	Tactical Formation	Up to 10,000 ft AGL	200 km (LOS)	Bde Com	SPERWER
Class I (< 150 kg)	Small (>15 kg)	Tactical Unit	Up to 5,000 ft AGL	50 km (LOS)	Battalion Regiment	Scan Eagle
	Mini (<15 kg)	Tactical Sub-unit (manual or hand launch)	Up to 3,000 ft AGL	Up to 25 km (LOS)	Company Squad Platoon Squad	Skylark
	Micro** (<66 J)	Tactical Sub-unit (manual or hand launch)	Up to 200 ft AGL	Up to 5 km (LOS)	Platroon, Section	Black Widow

EASA Classification Examples

Open *Low Risk*	• Includes majority of leisure drone & low-risk commercial activities
	• Three sub-categories
	  • A1: fly over people, but not assemblies
	  • A2: fly close to people
	  • A3: fly far from people
	• Does NOT include autonomous UAS

Specific *Medium Risk*	• Beyond Visual Line of Sight (BVLOS) • >25kg • Flying higher than 120M above ground level • Dropping material • >4kg while operating in an urban environment • Can include autonomous UAS
Certified *High Risk*	• International flights to shuttle cargo under instrument flight rules (IFR) • Flights in urban and rural environments carrying passengers & cargo • Can include autonomous UAS

Figure 29 –UAS Classification Nomenclature

Source: Author created using content from Mayer, 'State of the Art of Airworthiness Certification',17., and European Union Aviation Safety Agency (EUASA) website, 25.

NATO's UAS terminology offers a standardized framework for organizing UAS capabilities, and its impact can be seen when members, like Canada, adopt this framework into doctrine and procurement. As a middle power and a FYEY member, Canada sits at the intersection of alliance expectations and national priorities, navigating how to integrate UASs capabilities amid shifting technological and geopolitical realities. Canada's approach to UAS

[196] LCol Gauthier, CAF UAS Information: DLCSPM 5.

oversight remains grounded in human-centric models of control, aligning with NATO's expected shift away from weight-based classifications to a more nuanced risk-based framework: open, specific, and certified. This aligns with NATO's operator training requirements using these categories in combination with a mission-based scoring matrix which assumes a human-in-the-loop structure.[197]

Canada's military UAS ambitions are reflected in the last three defence policy update documents starting with the *Canda First Defence Strategy* in 2008 which did not mention UAS in any capacity.[198] In comparison, *Strong Secure Engaged* in 2017 identified a variety of roles associated with remotely piloted systems in all environments including joint ISR, strike, ground-based air defence and support to arctic sovereignty.[199] While most of those capabilities did not materialize, the defence policy update *Our Noth, Strong and Free* in 2024 referenced the threat of *drones* and a requirement for the CAF to procure counter-UAS capabilities and UAS strike and surveillance capabilities.[200]

As the CAF's approach to UAS management moves to the institutional rather than element or domain level, it is beginning to align with the CAF's pan-domain doctrine which focuses on integration with allies and across systems, elements, and domains. DND's L1 organizations supporting UAS include the 1 Canadian Air Division (CAD), Vice Chief of Defence Staff (VCDS), and Assistant Deputy Minster Material (ADM(MAT)) as described in Table 9. The work done by DTAES in the same table, highlights the transitional and patchwork

---

[197] Shirley, "RE: Staff College Research Paper," April 29, 2025.
[198] "Canada First Defence Strategy" (Ottawa, Ontario, 2008), publications.gc.ca/pub?id=9.693410&sl=0.
[199] *Strong Secure Engaged: Canada's Defence Policy* (Ottawa, ON, CA: National Defence, 2017).
[200] *Our North Strong and Free: A Renewed Vision for Canada's Defence* (Ottawa: National Defence = Défense nationale, 2024).

nature of current oversight, and emphasizes that while automation is increasing, control mechanisms remain human-dependent.

Table 9 –UAS-Related CAF Organizations and Their Responsibilities

Organization	UAS Responsibilities
Royal Canadian Air Force (**RCAF**)	
• 1 Canadian Air Division (**1 CAD**)	
○ Fleet Readiness	Senior Staff Officer (SSO) UAS ▪ Responsible for RPAS (similar to other fleets)
Vice Chief of Defence Staff (**VCDS**)	
• Chief of Combat Systems Integration (**CCSI**)	Joint Counter-UAS Office (**JCO**)
Assistant Deputy Minster Material (**ADM(MAT)**)	
• Director General Major Projects Division (**DGMPD**)	Air and Land (A&L) • Project management & Procurement for NATO Class III systems (CAF termed RPAS)
• Director General Aerospace Equipment Program Manager (**DGAEPM**)	Responsible for In-service support for NATO Class III systems (CAF termed RPAS)
○ Director Technical Airworthiness and Engineering Support (**DTAES**)	Technical Airworthiness Authority (**TAA**) • Responsible for RPAS certification • Provides support for airworthiness oversight of Specific UAS taskings via ○ Specific Purpose Flight Permits (SPFP) ○ Experimental Flight Permits (EFP) with supporting risk assessments (rare) ○ Temporary Authority to Operate through MOU with Transport Canada, supported by SPFP, Records of Airworthiness Risk Management (RARM) from TAA and Operational Airworthiness Authority (OAA) • Supports ongoing NATO's UAS System Airworthiness Requirement (USAR) development
• Director Land Command Systems Programme Management (**DLCSPM**)	
○ Director Land Command Systems Programme Management (**DLCSPM**)	**DLCSPM 5** or Joint Weapon-System Manager UAS (**JWSM**) • procurement, maintenance and continuous enhancement of UAS capabilities in alignment with NATO standards • Joint: UAS expertise organically grew within the army, but now supports all environments • Technical Authority (TA) for ○ NATO Classification I and II ○ Open and specific categories • Procurement, maintenance and continuous enhancement of UAS capabilities in alignment with NATO standards

Source: Author created based on content from a CAF presentation

The CAF's Joint Weapon-System Manager (JWSM) for UAS, the section responsible for the CAF's NATO Class I and II systems within the open and specific categories, is also responsible for their procurement. One major cyber-attack vector is via supply chain: AI systems often rely on commercial hardware or cloud-based infrastructures provided by private

corporations, many of which operate transnationally. As noted by the US's Cybersecurity Infrastructure Security Agency (CISA), supply chain compromises like altered firmware or hidden components can quietly degrade system reliability or insert remote access points;[201] this position was solidified by a supporting US Executive order in 2019.[202] When these systems are integrated into platforms capable of lethal force, the consequences could be catastrophic. Without secure infrastructure, autonomous systems will lack accountability and control. One method DLCSPM 5 uses to ensure supply chain integrity involves procuring UAS already vetted by the Defense Innovation Unit (DIU) Blue Book to ensure adequate cybersecurity and equipment that is safe to fly.[203] The DIU is an American military unit focused on "accelerating the adoption of leading commercial technology,"[204] and they have a standing list of UAS cleared to meet American policy[205] which currently includes 19 platform configurations produced by 13 different companies, and a list of interoperable and NDAA compliant components and software.

As Canada integrates UAS platforms into its fleet of capabilities, planning is increasingly influenced by anticipated operational realities rather than abstract policy: evolving battlefield geometry highlights how UAS capabilities can close gaps. For example, the Canadian Army (CA) is interested in matching UASs capable of conducting target acquisition with new longer-range weapons to direct fires at their maximum ranges.[206] Simultaneously, the CAF is closely

---

[201] "Testimony to Federal Committees Etc: Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risks" (Federal Government Accountability Office (GAO), May 25, 2021), https://www.gao.gov/assets/gao-21-594t.pdf.

[202] Trump, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain."

[203] LCol Gauthier, CAF UAS Information: DLCSPM 5.

[204] Defense Innovation Unit, "Blue UAS Cleared List," US DoD, DIU, April 2025, https://www.diu.mil/blue-uas-cleared-list.

[205] Relevant American UAS policy includes: (1) Fiscal Year (FY) 2024 National Defense Authorization Act (NDAA) passed 22 December 202 and includes the American Security Drone Act. (2) the FY 23 NDAA chapter 817 passed 23 December 2022 which remains in effect. (3) the FY 20 NDAA chapter 848 passed 20 December 2019 which remains in effect.

[206] CF LCol Durant, "UAS Question for Staff College/JCSP Paper - CA Perspective," May 5, 2025.

watching Ukraine's high-tempo, mass-scale drone warfare which is informing how assessments of electromagnetic resilience, automated flight, and scalable deployment can be incorporated into future UAS procurement.

Canada's UAS acquisition strategy reflects a broader global phenomenon: the pursuit of technologically advanced capabilities that moves parallel rather than within coherent ethical, legal and operational frameworks. The CAF's UAS and RPAS procurement focuses on increasing automation rather than autonomy which aligns with the country's position on LAWSs provided to the UN extolling the necessity of human control.[207] However, eventually future iterations of increasingly complex automation used in complex and dynamic real-world environments will blur the line between automation and autonomy. Combining that trajectory with an increasing demand for autonomy to meet operational requirements, even nations like Canada which value human control need to work towards technological development and regulatory governance to address systemic challenges related to military technologies integrated with AI. This necessitates a forward-looking perspective to meet those challenges.

While Canada focuses on increasing automation, doctrinal and technical efforts to keep humans in-the-loop can mask realistic and limited influence an operator can exert in complex, high-speed engagements. As raised in chapter 2, this false accountability risks creating what scholars have called a moral crumple zone**:** a scenario in which human actors absorb ethical and legal blame for the actions of systems they do not meaningfully control.[208] This begs the question, what is the maximum level of system complexity that a human meaningfully control? Which in turn, brings us back to the definitional quandary, what is meaningful human control?

---

[207] General Assembly, "General and Complete Disarmament: Lethal Autonomous Weapons Systems Report of the Secretary-General."

[208] Elish, "Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction."

As with AVs, the ability to assign responsibility and ensure traceable, explainable system behavior will determine whether autonomous military technologies can remain ethically and legally accountable. Civilian autonomy challenges offer critical foresight: without designing traceability and human-centric accountability into systems from the outset, military use risks accelerating the erosion of meaningful human control over life-and-death decisions. Taken together, Canada's reliance on foreign infrastructure, doctrinal ambiguity, and private-sector control over key technologies illustrates a broader challenge faced by allied militaries: the accelerating adoption of UASs is outpacing institutional capacity to govern their use coherently. While military and civilian domains may have diverging goals, they share overlapping vulnerabilities around autonomy, data dependency, and legal ambiguity. These trends underscore the urgency of national and alliance-level adaptation.

5.7 – Conclusion: Autonomy, Accountability, and the Airspace Ahead

> *The future's not set. There's no fate but what we make for ourselves.*
> - Paul Scharre, Army of None: Autonomous Weapons and the Future of War

This chapter explored how AVs' technical components are also integrated into increasingly autonomous military UASs generally and through the lens of the CAF's UAS programme. The overlap in technology means innovations intended for civilian applications can be repurposed for a variety of different, potentially lethal, military applications. Dual-use technology and easily adaptable civilian technology means non-state actors can easily leverage it with devastating results. These trends, and an institutional mismatch between ambition and capability, suggest that the transition from greater automation to greater autonomy is already unfolding.

As UASs continue to evolve in sophistication, the boundary between remotely operated tools, automated systems, and fully autonomous weapons systems becomes increasingly blurred.

This evolution mirrors the philosophical and technical tensions outlined earlier: between the human-in-the-loop concepts from section 2.4 and the architectural realities of adaptive AI explored in chapter 3. Understanding this convergence is critical not just for evaluating platform capabilities, but for anticipating the legal, moral, and strategic implications of autonomy in warfare. Together, these insights show that autonomous system governance needs to account for technological trajectories and the institutional, and operational contexts in which they must exist and with whom they will coevolve. With each step toward greater independence, these systems inch closer to the domain of LAWS, where questions of responsibility, oversight, and human control become not just complex, but urgent. To safeguard national interests and uphold international norms, Canada must accelerate the adaptation of its legal and strategic frameworks and aligning them with the complex realities of autonomous military systems and the shifting dynamics of global power competition.

CHAPTER 6 - CONCLUSION: CLOSING THE CIRCUIT AND RELOADING, RESPONSIBILITY

> *It's going to be interesting to see how society deals with artificial intelligence, but it will definitely be cool.*
>
> - Colin Angle, CEO and founder of iRobot

From AVs to military UASs with increasingly autonomous functions, this paper explored how AI is reshaping not only the technical aspects of modern life, but also the ethical concerns and institutional frameworks that have historically governed responsibility and legality. Autonomous systems are reshaping civilian and military foundations which were examined through the disruptive technologies of AVs and UASs with the backdrop of the UN working to define LAWSs. At the heart of this shift is AI's growing autonomy thus bringing into question meaningful human control and existential concerns.

AVs are a useful starting point. Their development illustrates the interplay of technical progress, societal trust, and legal uncertainty, all of which are pushed by the commercial interests of multiple industries. As AVs move onto public roads and common usage, they bring accessible documentation related to regulatory frameworks, safety studies, insurance models, and technical innovation. This accessibility allows AV to act as proxy for less transparent systems like military UASs and LAWSs. Many of the core challenges, both ethical and technical, faced by military applications of UASs are reflected in civilian AV scenarios. If an AV crashes, a pedestrian might die. If a military UAS misidentifies a target, it could be a war crime with far more casualties and cascading consequences.

The terminology *human-in-the-loop* versus *human-on-the-loop* versus *human-out-of-the-loop* reflects different levels of human acceptance of automation and autonomy. How much human control is meaningful? How much of a difference is there between the automatic application of brakes to avoid a crash and an AV? When autonomy becomes key to operational

speed or tactical advantage, is human oversight even viable? As AI becomes more autonomous, the question is no longer what is technically possible, but rather what level of control is society willing to reallocate. Autonomy enables scale, endurance, and precision, but it can also introduce questionable accountability, especially when something goes wrong. And in war, something always goes wrong.

There is a technical convergence between civilian and military applications; systems developed for convenience can be used in conflict. This overlap is not hypothetical, and there are blurred lines between commercial and military applications and dual-use platforms. The same AI models that enable route planning for delivery vehicles also powers autonomous patrols in contested airspace. The same object perception and sensor technology used to identify traffic signs also identifies military targets. In addition to technical scrutiny, these dual-use dynamics require political awareness and regulatory foresight.

AI advances like model editing, federated learning, and continual learning offer promising ways to adapt systems, preserve privacy, and reduce bias. But technical solutions alone cannot resolve moral dilemmas because AI is not a neutral tool. It reflects the values, assumptions, and power structures of the developers and users. Autonomous military UASs programmed to follow International LOAC, will still reflect its creators interpretation of those laws. A system designed to minimize collateral damage, whether it is an AV or a military UAS, must still weigh lives against lives, and probabilities against outcomes. Society cannot engineer our way out of applied trolley problems. Because AI requires code however, which reflects choice and thus societal decisions, we can choose to embed layers of technology during the design phase upon which we can iteratively improve to deliberately build and improve accountability.

Responsibility is central. Autonomy does not remove the need for accountability but rather intensifies it. Who is responsible when an autonomous military UAS strikes the wrong target: the manufacturer? the programmer? the military operator? the chain of command? XAI methodology, interpreting how AI decisions are made after the fact is one component of a potential technical solution enabling accountability. Meanwhile, international governance struggles to keep up. The UN and other multilateral institutions have opened discussions around LAWS, but progress is slow and fragmented. Powerful nations differ as to whether LAWS should be banned, restricted, or developed freely. In the absence of consensus, automation and autonomy continue to advance in real-world deployments. UASs with loitering munitions, autonomous navigation, and onboard target identification are already operating around the world. Governments and non-state actors alike are not waiting for an updated Geneva Convention to address AI and LAWSs. The debate surrounding LAWSs is no longer theoretical.

However, based on appropriate governance and ethical frameworks, technical solutions are possible to the inherently ethical problem positioning military exigency against human control. Emerging AI capabilities such as XAI, model editing, world modeling, and agentic design offer the foundation for systems that not only act autonomously but also operate within clearly defined moral and legal boundaries. When combined with robust oversight structures, these technologies can be used to encode rules of engagement, apply interpretability to autonomous decisions, and enable post-hoc accountability. In this way, AI does not replace human judgment but rather extends and operationalizes it under well-specified constraints. The key lies in aligning technical development with societal expectations and legal norms from the outset. Military UASs, and eventually LAWSs, need not be deployed in an ethical vacuum. If designed transparently, regulated multilaterally, and continuously monitored, autonomous

systems can reflect collective decisions within acceptable limits of AI action. Autonomy becomes not a surrender of control, but a reframing of it: machines executing goals set by humans, with traceable reasoning and bounded discretion.

This vision of ethically grounded autonomy is neither utopian nor impossible. It is a call for deliberate and informed collaboration across disciplines – from engineers to ethicists, policymakers to military leaders — to ensure that the pursuit of operational effectiveness does not eclipse the foundational principles of responsibility, proportionality, and human dignity. In doing so, the world may move toward a future in which autonomous systems are not only powerful, but principled; faster than human decision-making and simultaneously safer and more accountable because of the frameworks within which they operate. The global evolution of UAS technologies across commercial and military domains forces government and military leaders to reckon with unprecedented challenges in autonomy, accountability and meaningful human control. Canada's current approach to military UAS programme, while measured, remains anchored in legacy procurement processes, legal ambiguities, and a doctrine that does not yet reflect the tempo of technological change and operational requirement. The ethical tensions of chapter 2 illustrated by trolley problem, the accountability gaps illustrated through insurance in section 4.4, and the technical applications and capabilities highlighted in chapters 4 and 5 through the lenses of AVs, UAS, and the CAF's military use of UASs, all converge at the precipice of emerging LAWSs where policy, doctrine, and technology must now reconcile.

Ultimately, autonomy in warfighting is not just about performance, but about judgment. The story of Captain Petrov, the Russian who chose not to follow protocol and may have prevented a nuclear war, serves as a sobering reminder of what's at stake when decisions are made in the absence of context, intuition, and ethical reflection. As we move toward systems that

act faster than humans can respond, are we ready to trust machines with choices we ourselves struggle to make? And given that LAWSs, but for the formal legal definition, already exist, what technological scaffolding can we use to ensure the right call is made by the future AI version of Captain Petrov?

BIBLIOGRAPHY

36Kr English. “The Current State of Self-Driving Across China in 2024,” May 20, 2024.

Advisory Group on Advanced Technologies. “Artificial Intelligence Demystified.” Economic Commission for Europe, Executive Committee: United Nations Economic and Social Council, April 13, 2021.

Army Recognition Group. “Shahed-136; Loitering Munition/Kamikaze-Suicide Drone - Iran.” Global Defense News, March 12, 2025. https://armyrecognition.com/military-products/army/unmanned-systems/unmanned-aerial-vehicles/shahed-136-loitering-munition-kamikaze-suicide-drone-technical-data.

Atakishiyev, Shahin, Mohammad Salameh, and Randy Goebel. “Safety Implications of Explainable Artificial Intelligence in End-to-End Autonomous Driving.” arXiv, 2024. https://doi.org/10.48550/ARXIV.2403.12176.

Australian Defence Force. “Uncrewed Aerial Systems.” Australian Government. Defence Activities, projects. Accessed January 10, 2025. https://www.defence.gov.au/defence-activities/projects/uncrewed-aerial-systems.

Australian Defence Force, and Ryan Hodson. “The Weaponization of Toys and Implications for the Air Force.” *Air/Space* 3 (2024): bp41568060. https://doi.org/10.58930/bp41568060.

Awad, Edmond, Iyad Rahwan, Jean-Francois Bonnefon, and Azim Shariff. “The Moral Machine,” n.d. https://www.moralmachine.net/.

Axe, David. “A Two-Pound Ukrainian Drone May Have Shot Down a 12-Ton Russian Helicopter.” *Forbes*, July 31, 2024, sec. Aerospace & Defense. https://www.forbes.com/sites/davidaxe/2024/07/31/a-two-pound-ukrainian-drone-just-shot-down-a-12-ton-russian-helicopter/.

Ball, Mike. “GPS/GNSS Spoofing Technology for Drones & UAS.” *Unmanned Systems Technology* (blog), 15 Nov 23. https://www.unmannedsystemstechnology.com/expo/drone-gps-spoofing/.

Bartneck, Christoph, Christoph Lütge, Alan Wagner, and Sean Welsh. *An Introduction to Ethics in Robotics and AI*. SpringerBriefs in Ethics. Cham: Springer International Publishing, 2021. https://doi.org/10.1007/978-3-030-51110-4.

BBC. “Robotaxis: Driverless Cars Arriving in US Cities.” April 11, 2024. https://www.bbc.co.uk/newsround/68777656.

“Canada First Defence Strategy.” Ottawa, Ontario, 2008. publications.gc.ca/pub?id=9.693410&sl=0.

Carlini, Nicholas, Daphne Ippolito, Matthew Jagielski, Katherine Lee, Florian Tramer, and Chiyuan Zhang. “Quantifying Memorization Across Neural Language Models.” arXiv, March 6, 2023. https://doi.org/10.48550/arXiv.2202.07646.

Castillo Ossa, Luis Fernando. *Trends in Sustainable Smart Cities and Territories*. 1st ed. Lecture Notes in Networks and Systems Series, v. 732. Cham: Springer International Publishing AG, 2023.

Center for Preventive Action. “Conflict in Yemen and the Red Sea,” October 8, 2024. https://www.cfr.org/global-conflict-tracker/conflict/war-yemen.

Charlton, Alistair. “BMW Drops Controversial Heated Seats Subscription, To Refocus on Software Services.” *Forbes*, September 7, 2023.

Cheung, Rachel. “The Roadblock Facing China’s Self-Driving Vehicles.” *The Wire China*, September 8, 2024.

Clow, Rachel, Allison Rutter, and Barbara A. Zeeb. “Residual DDT Distribution in the Soils and Sediments of Point Pelee National Park: Implications and Tools for Remediation.” *Canadian Journal of Soil Science*, November 10, 2016, CJSS-2016-0048. https://doi.org/10.1139/CJSS-2016-0048.

“Common Crawl.” Free, Open Repository of Web Crawl Data. Accessed January 21, 2025. https://commoncrawl.org/.

Cooper, A. Feder, and James Grimmelmann. “The Files Are in the Computer: Copyright, Memorization, and Generative AI.” arXiv, November 11, 2024. https://doi.org/10.48550/arXiv.2404.12590.

Craft Law Firm. “Autonomous Vehicle Accidents: NHTSA Crash Data (2019-2024).” Accessed May 8, 2025. https://www.craftlawfirm.com/autonomous-vehicle-accidents-2019-2024-crash-data/#ads-crash-details.

Cummings, Mary L. “Missy.” “What Self-Driving Cars Tell Us About AI Risks.” *IEEE Spectrum*, June 30, 2023.

DA Staff. “Joint Aviation Command (JAC): Overview and Capabilities.” Defense Advancement, December 13, 2024. https://www.defenseadvancement.com/resources/joint-aviation-command-jac-overview-and-capabilities/.

Davidovic, Jovana. “What’s Wrong with Wanting a ‘Human in the Loop’?” *War on The Rocks*, June 23, 2022. https://warontherocks.com/2022/06/whats-wrong-with-wanting-a-human-in-the-loop/.

Deepgram. “End-to-End Learning,” June 18, 2024. https://deepgram.com/ai-glossary/end-to-end-learning.

Defense Innovation Unit. “Blue UAS Cleared List.” US DoD, DIU, April 2025. https://www.diu.mil/blue-uas-cleared-list.

Dehuri, Satchidananda, Sung-Bae Cho, Venkat Prasad Padhy, Poonkuntrun Shanmugam, and Ashish Ghosh, eds. *Machine Intelligence, Tools, and Applications: Proceedings of the International Conference on Machine Intelligence, Tools, and Applications—ICMITA 2024*. 1st ed. 2024. Learning and Analytics in Intelligent Systems 40. Cham: Springer Nature Switzerland, 2024. https://doi.org/10.1007/978-3-031-65392-6.

DND. “Pan-Domain Force Employment Concept,” 2023.

Dow, Cat. “What Are the Six SAE Levels of Self-Driving Cars?” *Top Gear Advice* (blog), March 6, 2023. https://www.topgear.com/car%20news/what-are-sae-levels-autonomous-driving-uk.

Drezner, Daniel W., Henry Farrell, and Abraham L. Newman, eds. *The Uses and Abuses of Weaponized Interdependence*. Erscheinungsort nicht ermittelbar: Nomos Verlagsgesellschaft mbH & Co. KG, 2021. https://doi.org/10.5771/9780815738381.

EASA. “European Union Aviation Safety Agency.” Accessed May 4, 2025. https://www.easa.europa.eu/en/domains/civil-drones.

———. “FAQ > Drones (UAS).” European Union Aviation Safety Agency, n.d. https://www.easa.europa.eu/en/the-agency/faqs/drones-uas#category-regulations-on-uas-drone-explained.

Elish, Madeleine Clare. “Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction.” *Engaging Science, Technology, and Society* 5 (March 23, 2019). https://estsjournal.org/index.php/ests/article/view/260.

Erdemir, Ahmet, and Daniel Blankenberg. “How Quantum Computing Will Affect Artificial Intelligence Applications in Healthcare,” July 29, 2024. https://www.lerner.ccf.org/news/article/?title=+How+quantum+computing+will+affect+artificial+intelligence+applications+in+healthcare+&id=79c89a1fcb93c39e8321c3313ded4b84005e9d44.

Ettzioni, Amitai, and Oren Etzioni. “Pros and Cons of Autonomous Weapons Systems.” *Army Univeristy Press, Military Review, The Professional Journal of the U.S. Army* May-June 2017 (2017).

everything RF. “everythingRF.” RF, Microwave & Wireless Industry. Accessed March 12, 2025. https://www.everythingrf.com.

Fawole, Oluwajuwon A., and Danda B. Rawat. “Recent Advances in 3D Object Detection for Self-Driving Vehicles: A Survey.” *AI* 5, no. 3 (July 25, 2024): 1255–85. https://doi.org/10.3390/ai5030061.

Fuertes, Rechelle Ann. “Explainable AI in Autonomous Vehicles: Building Transparency and Trust on the Road.” *Smyth OS* (blog), February 21, 2025. https://smythos.com/ai-industry-solutions/automotive/explainable-ai-in-autonomous-vehicles/.

General Assembly. “General and Complete Disarmament: Lethal Autonomous Weapons Systems Report of the Secretary-General.” United Nations General Assembly, July 1, 2024. https://docs.un.org/en/A/79/88.

———. “General and Complete Disarmament: Lethal Autonomous Weapons Systems Resolution 79/62.” United Nations General Assembly, December 10, 2024. https://docs.un.org/en/A/RES/79/62.

———. “Promotion and Protection of Human Rights in the Context of Digital Technologies.” United Nations General Assembly, December 19, 2023. https://documents.un.org/doc/undoc/gen/n23/422/28/pdf/n2342228.pdf.

González, Roberto J. *Militarizing Culture: Essays on the Warfare State*. London: Routledge, 2016. https://doi.org/10.4324/9781315424699.

Google Cloud Learn. “Artificial Intelligence (AI) vs Machine Learning (ML),” n.d. https://cloud.google.com/learn/artificial-intelligence-vs-machine-learning#what-is-artificial-intelligence.

Government of BC. “Automated (Self-Driving) Vehicles.” Accessed April 15, 2025. https://www2.gov.bc.ca/gov/content/transportation/driving-and-cycling/road-safety-rules-and-consequences/self-drive.

Hambling, David. “Ukraine Fiels Unjammable Fiber Optic FPV Attack Drone.” *Forbes*, November 7, 2024. https://www.forbes.com/sites/davidhambling/2024/11/07/ukraine-fields-reboff-unjammable-fiber-optic-fpv-attack-drone/.

Hardesty, Larry. “Explained: Neural Networks.” *MIT News*, April 14, 2017.

Huawei Technologies Co., Ltd. *Artificial Intelligence Technology*. Singapore: Springer Nature, 2023.

Hunder, Max. “Ukraine Rushes to Create AI-Enabled War Drones.” *Reuters*, July 18, 2024. https://www.reuters.com/technology/artificial-intelligence/ukraine-rushes-create-ai-enabled-war-drones-2024-07-18/.

Jordan, John M. “The Czech Play That Gave Us the Word ‘Robot.’” *The MIT Press Reader*, July 29, 2019. https://thereader.mitpress.mit.edu/origin-word-robot-rur/.

Kak, Amba. “Make No Mistake - AI Is Owned by Big Tech.” *MIT Technology Review* (blog), December 5, 2023. https://www.technologyreview.com/2023/12/05/1084393/make-no-mistake-ai-is-owned-by-big-tech/.

Kinger, Shakti, and Vrushali Kulkarni. “Demystifying the Black Box: An Overview of Explainability Methods in Machine Learning.” *International Journal of Computers and Applications* 46, no. 2 (February 2024): 90–100. https://doi.org/10.1080/1206212X.2023.2285533.

Kobie, Nicole. “Is Waymo Coming To Your City? Google Robotaxis Hit the Road for Tests.” *Forbes*, January 31, 2025. https://www.forbes.com/sites/nicolekobie/2025/01/31/is-waymo-coming-to-your-city-google-robotaxis-hit-the-road-for-tests/.

Lark Editorial Team. “Rule Based Systems in AI,” December 27, 2023. https://www.larksuite.com/en_us/topics/ai-glossary/rule-based-systems-in-ai.

LCol Durant, CF. “UAS Question for Staff College/JCSP Paper - CA Perspective,” May 5, 2025.

LCol Gauthier, Yan. CAF UAS Information: DLCSPM 5, April 25, 2025.

Leffer, Lauren. “Your Personal Information Is Probably Being Used to Train Generative AI Models,” October 19, 2023. https://www.scientificamerican.com/article/your-personal-information-is-probably-being-used-to-train-generative-ai-models/.

Magdolna, Felicia. “Drone Signal Jamming & Interference.” FlyEye, February 17, 2025. https://www.flyeye.io/drone-technology-signal-jamming/.

Malik, Kamal, Moolchand Sharma, Suman Deswal, Umesh Gupta, Deevyankar Agarwal, and Yahya Obaid Bakheet Al Shamsi. *Explainable Artificial Intelligence for Autonomous Vehicles: Concepts, Challenges, and Applications*. 1st ed. Boca Raton: CRC Press, 2024. https://doi.org/10.1201/9781003502432.

Manley, Cameron. “Houthi Rebel Footage Appears to Show a Downed US Reaper Drone Worth $30 Million,” June 1, 2024. https://www.businessinsider.com/houthis-downed-3rd-us-reaper-drone-worth-30m-1-month-2024-5#:~:text=Related%20stories,unit%20costs%20around%20%2430%20million.

Mayer, John E. “State of the Art of Airworthiness Certification.” *NATO Science & Technology Organization*, April 27, 2017. https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/Forms/Meeting%20Proceedings%20Document%20Set/docsethomepage.aspx?ID=42949&FolderCTID=0x0120D5200078F9E87043356C409A0D30823AFA16F602008CF184CAB7588E468F5E9FA364E05BA5&List=7e2cc123-6186-4c30-8082-1ba072228ca7&RootFolder=https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-AVT-273.

McGrath, Amanda, and Alexandra Jonker. “What Is AI Interpretability?” IBM, October 8, 2024. https://www.ibm.com/think/topics/interpretability.

McKay, Tom. “Amazon’s Human Helpers Are Quietly Listening in on Some Alexa Recordings.” *Gizmodo*, April 10, 2019. https://gizmodo.com/amazons-human-helpers-are-quietly-listening-in-on-some-1833960052.

Mittal, Vikram. “Russians Capture Ukrainian Drones Which Infect Their Systems With Malware,” April 2, 2025. https://www.forbes.com/sites/vikrammittal/2025/04/02/russians-capture-ukrainian-drones-which-infect-their-systems-with-malware/.

Naeem, Muhammad Ali, Sushank Chaudhary, and Yahui Meng. “Road to Efficiency: V2V Enabled Intelligent Transportation System.” *Electronics* 13, no. 13 (July 8, 2024): 2673. https://doi.org/10.3390/electronics13132673.

Nagarjuna, Phani. “Customer Lifetime Value and The Subscription Economy.” *Forbes*, December 20, 2019, Forbes Technology Council edition. https://www.forbes.com/councils/forbestechcouncil/2019/12/20/customer-lifetime-value-and-the-subscription-economy/.

NATO Has Missed the Drone Revolution. YouTube, 2025. https://www.youtube.com/watch?v=gZL1KzV54Cw.

Nicole. “Ottawa Treaty and the Convention on Cluster Munitions: Recent Developments.” *House of Lords Library*, March 31, 2025. https://lordslibrary.parliament.uk/ottawa-treaty-and-the-convention-on-cluster-munitions-recent-developments/.

O’Neil, Kate. “Facebook’s ‘10 Year Challenge’ Is Just a Harmless Meme - Right?” *Wired*, January 15, 2019. https://www.wired.com/story/facebook-10-year-meme-challenge/.

Osmani, Khaled, and Detlef Schulz. “Comprehensive Investigation of Unmanned Aerial Vehicles (UAVs): An In-Depth Analysis of Avionics Systems.” *Sensors* 24, no. 10 (May 11, 2024): 3064. https://doi.org/10.3390/s24103064.

Our North Strong and Free: A Renewed Vision for Canada’s Defence. Ottawa: National Defence = Défense nationale, 2024.

Peeva, Aleksandra. “Now Available: New Drone Technology for Radiological Monitoring in Emergency Situations.” *International Atomic Energy Agency* (blog), February 1, 2021. https://www.iaea.org/newscenter/news/now-available-new-drone-technology-for-radiological-monitoring-in-emergency-situations.

Peremarty, Lea. “Lethal Autonomous Weapons: Between Myths and Confusion.” *Network for Strategic Analysis*, July 26, 2023. https://ras-nsa.ca/lethal-autonomous-weapons-between-myths-and-confusion/.

Perrin, Benjamin. “Lethal Autonomous Weapons Systems & International Law: Growing Momentum Towards a New International Treaty.” *American Society of International Law* 29, no. 1 (January 24, 2025). https://www.asil.org/insights/volume/29/issue/1.

Phillips, Dave. “The Unseen Scars of Those Who Kill Via Remote Control.” *The New York Times*, Aril 2022. https://www.proquest.com/blogs-podcasts-websites/unseen-scars-those-who-kill-via-remote-control/docview/2650321771/se-2?accountid=9867.

RAeS. “Highlights from the RAeS Future Combat Air & Space Capabilities Summit.” Royal Aeronautical Society, 2023. https://www.aerosociety.com/news/highlights-from-the-raes-future-combat-air-space-capabilities-summit/#:~:text=He%20notes%20that,accomplishing%20its%20objective.%E2%80%9D.

Ramlochan, Sunil. “Exploring the IEEE Paper: Human-in-the-Loop, Explainable AI, and the Role of Human Bias.” *Prompt Engineering & AI Institute* (blog), March 27, 2024. https://promptengineering.org/exploring-the-ieee-paper-human-in-the-loop-explainable-ai-and-the-role-of-human-bias/#1-introduction.

Rashid, Adib Bin, and Md Ashfakul Karim Kausik. “AI Revolutionizing Industries Worldwide: A Comprehensive Overview of Its Diverse Applications.” *Hybrid Advances* 7 (December 2024): 100277. https://doi.org/10.1016/j.hybadv.2024.100277.

Report of the Secretary General. “Current Developments in Science and Technology and Their Potential Impacts on International Security and Disarmament Efforts.” General Assembly, United Nations, August 1, 2023. https://docs.un.org/en/A/78/268.

Report of the Special Rapporteur on Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance. “Racial Discrimination and Emerging Digital Technologies: A Human Rights Analysis.” United Nations Human Rights Council, June 18, 2020.

Ridpath, Michael. “Nuclear Near Misses.” Aspects of History. Accessed March 21, 2025. https://aspectsofhistory.com/nuclear-near-misses/.

Rollins, John W. “Armed Drones: Evolution as a Counterterrorism Tool.” Congressional Research Service, November 7, 2023. https://www.congress.gov/crs-product/IF12342.

SAE International. “SAE Levels of Driving Automation Refined for Clarity and International Audience,” May 3, 2021. https://www.sae.org/blog/sae-j3016-update.

Scales, Adam F. “*Not So Fast* : A Brief Plea for Muddling Through the Problems of Autonomous Vehicle Liability.” *Journal of Tort Law* 13, no. 2 (November 18, 2020): 189–95. https://doi.org/10.1515/jtl-2020-2012.

Scanlon, John M., Kristofer D. Kusano, Laura A. Fraade-Blanar, Timothy L. McMurry, Yin-Hsiu Chen, and Trent Victor. “Benchmarks for Retrospective Automated Driving System Crash Rate Analysis Using Police-Reported Crash Data.” *Traffic Injury Prevention* 25, no. sup1 (November 2024): 7. https://doi.org/10.1080/15389588.2024.2380522.

Schmidt, Douglas C., and Team from Vanderbilt University from Dept of Computer Science. “Google Data Collection.” Digital Content Next (DCN), August 2018. https://digitalcontentnext.org/wp-content/uploads/2018/08/DCN-Google-Data-Collection-Paper.pdf.

Secretary-General. “Right to Privacy.” United Nations General Assembly, July 17, 2024.

Sever, Tina, and Giuseppe Contissa. “Automated Driving Regulations – Where Are We Now?” *Transportation Research Interdisciplinary Perspectives* 24 (March 2024): 101033. https://doi.org/10.1016/j.trip.2024.101033.

Seymour, Kiley, Jarrod McNicoll, and Roger Koenig-Robert. “Big Brother: The Effects of Surveillance on Fundamental Aspects of Social Vision.” *Neuroscience of Consciousness* 2024, no. 1 (December 10, 2024): niae039. https://doi.org/10.1093/nc/niae039.

Shah, Raj M., and Christopher Kirchhoff. *Unit X: How the Pentagon and Silicon Valley Are Transforming the Future of War*. First Scribner hardcover edition. New York: Scribner, 2024.

Shirley, Michael. “RE: Staff College Research Paper,” April 29, 2025.

SIG ML. “Automation, Autonomy...Same Thing, Right?,” February 7, 2024. https://www.sigmachinelearning.com/post/automation-autonomy-same-thing-right.

Simonite, Tom. “3 Years After the Project Maven Uproar, Google Cozies to the Pentagon.” *Wired*, November 18, 2021. https://www.wired.com/story/3-years-maven-uproar-google-warms-pentagon/.

Singh, Jobanbir, Avishesh Sharma, Anubhav Sharma, and Sandeep Kaur. “Autonomous Driving and ADAS Embedded with AI: Comparing the AI Norms.” In *2024 International Conference on Intelligent Systems for Cybersecurity (ISCS)*, 1–6. Gurugram, India: IEEE, 2024. https://doi.org/10.1109/ISCS61804.2024.10581391.

Sitaraman, Ganesh. “Too Big to Prevail: The National Security Case for Breaking Up Big Tech.” *Foreign Affairs; New York* 99, no. 2 (April 2020): 116-120,122-126.

Slattery, Peter. “What Drives Progress in AI? Trends in Compute.” *FutureTech* (blog), January 3, 2025.

Slayton, Nicholas. “Cheap Houthi Drones Are Draining the Pentagon’s Coffers.” *New Lines Magazine*, July 29, 2024. https://newlinesmag.com/argument/cheap-houthi-drones-are-draining-the-pentagons-coffers/.

Sluka, Jeffrey A. “Death from Above: UAVs and Losing Hearts and Minds.” *Military Review* March-April (2013). https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20130430_art013.pdf.

Sparrow, Rob. “Ethics as a Source of Law: The Martens Clause and Autonomous Weapons.” *Humanitarian Law & Policy*, November 14, 2017. https://blogs.icrc.org/law-and-policy/2017/11/14/ethics-source-law-martens-clause-autonomous-weapons/.

Starkov, Nick. “Russia Drones Smash Power Network In Odesa.” *Reuters*, December 11, 2022. https://www.reuters.com/world/europe/russian-drone-attacks-target-power-network-ukraines-odesa-officials-2022-12-10/.

Stefanovic, Maja. “How Close Are We to Self-Driving Taxis in Europe?” *HERE360 News* (blog), February 5, 2025.

Stoner, Jacob. “What Is FPV (First Person View) & How Does It Work?” FlyEye, June 5, 2024. https://www.flyeye.io/drone-acronym-fpv/.

Stoner, Jacob, and Felicia Magdolna. “AI Guide.” FlyEye, February 2025. https://www.flyeye.io/ai-powered-drone-technology/.

Stop Killer Robots. “Less Autonomy. More Humanity.” Accessed March 20, 2025. https://www.stopkillerrobots.org/.

Strong Secure Engaged: Canada’s Defence Policy. Ottawa, ON, CA: National Defence, 2017.

Stryker, Cole, and Eda Kavlokoglu. “What Is AI?” IBM, August 9, 2024. https://www.ibm.com/think/topics/artificial-intelligence.

Tencent Research Institute, CAICT, Tencent AI Lab, and Tencent open platform, eds. *Artificial Intelligence: A National Strategic Initiative*. Singapore: Springer Singapore, 2021. https://doi.org/10.1007/978-981-15-6548-9.

“Testimony to Federal Committees Etc: Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risks.” Federal Government Accountability Office (GAO), May 25, 2021. https://www.gao.gov/assets/gao-21-594t.pdf.

Tiwari, Vaibhavi, Dharshana Rajasekar, and Jiayin Wang. “A Survey: Emerging Cybersecurity Threats in Driverless Cars.” In *2024 IEEE 15th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, 183–89. Yorktown Heights, NY, USA: IEEE, 2024. https://doi.org/10.1109/UEMCON62879.2024.10754688.

Todd, Kate. “Lessons for Canada: Comparing Maritime Autonomous Systems Adoption Across the Five Eyes.” *Triple Helix*, September 2024. https://www.cgai.ca/lessons_for_canada_comparing_maritime_autonomous_systems_adoption_across_the_five_eyes?

Transport Canada. *Aeronautical Information Manual (AIM)*. Vol. Effective 0901Z, October 3, 2024 to 0901Z, March 20, 20254. TP 14371E, n.d. https://tc.canada.ca/sites/default/files/2024-09/aim-2024-2_access_e.pdf.

———. “Drone Safety.” Government of Canada, March 3, 2025. https://tc.canada.ca/en/aviation/drone-safety.

———. *Transport Canada’s Vehicle Cyber Security Strategy*. Ottawa: Transport Canada = Transports Canada, 2021.

Trump, Donald J. “Executive Order on Securing the Information and Communications Technology and Services Supply Chain.” The White House, May 15, 2019.

https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

Tsang, Daisy. “White Box vs. Black Box Algorithms in Machine Learning.” *Activestate* (blog), July 19, 2023. https://www.activestate.com/blog/white-box-vs-black-box-algorithms-in-machine-learning/.

Turi, Abeba Nigussie, and Pooja Lekhi, eds. *Innovation, Sustainability, and Technological Megatrends in the Face of Uncertainties: Core Developments and Solutions*. Future of Business and Finance. Cham: Springer Nature Switzerland, 2024. https://doi.org/10.1007/978-3-031-46189-7.

Ukrainian World Congress, and Ministry of Digital Transformation of Ukraine. “Army of Drones.” Ukrainian World Congress. Accessed January 7, 2025. https://www.ukrainianworldcongress.org/united24/.

UNCTAD Secretariat. “Strengthening Consumer Protection and Competition in the Digital Economy.” United Nations, July 29, 2020.

United Nations Office for Disarmament Affairs (UNODA). “Lethal Autonomous Weapons Systems (LAWS).” United Nations. Accessed January 16, 2025. https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/.

Van Der Vlist, Fernando, Anne Helmond, and Fabian Ferrari. “Big AI: Cloud Infrastructure Dependence and the Industrialization of Artificial Intelligence.” *Big Data & Society* 11, no. 1 (March 2024): 20539517241232630. https://doi.org/10.1177/20539517241232630.

Wakefield, Jane. “Microsoft Chatbot Is Taught to Swear on Twitter.” *BBC*, March 24, 2016. https://www.bbc.com/news/technology-35890188.

Watling, Jack. “Automation Does Not Lead to Leander Land Forces.” *War on The Rocks*, February 7, 2024. https://warontherocks.com/2024/02/automation-does-not-lead-to-leaner-land-forces/.

Weijer, Carlo van der, and Alwin Bakker. What the World could Learn From China’s Autonomous Vehicle Innovations, July 2, 2024.

Xu, Wei. “From Automation to Autonomy and Autonomous Vehicles: Challenges and Opportunities for Human-Computer Interaction.” *Interactions* 28, no. 1 (January 2021): 48–53. https://doi.org/10.1145/3434580.

Zafra, Mariano, Max Hunder, Anurag Rao, and Sudev Kiyada. “How Drone Combat in Ukraine Is Changing Warfare.” *Reuters*, March 26, 2024. https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/.

Zaluzhnyi, Valerii. “How Drones, Data and AI Transformed Our Military - and Why the US Must Follow Suit.” *Defense One*, April 10, 2025.

https://www.defenseone.com/ideas/2025/04/how-drones-data-and-ai-transformed-our-militaryand-why-us-must-follow-suit/404444/.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. First trade paperback edition. New York, NY: PublicAffairs, 2020.