Autonomous Vehicles
THREATS, RISKS, AND OPPORTUNITIES

Researchers: Ishmael Bhila, Peter Lee, and Alison Wakefield
Autonomous Vehicles: Threats, Risks, and Opportunities

Researchers:
Ishmael Bhila,
Peter Lee,
Alison Wakefield

This research is made possible by the ASIS Foundation. The ASIS Foundation is supported by generous donations from ASIS members, chapters, and organizations.

Give back to the security industry and make a donation today!

Copyright © 2024 ASIS Foundation

All rights reserved. No part of this report may be reproduced, translated into another language, stored in a retrieval system, or transmitted in any form without prior written consent of the copyright owner.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>TABLE OF CONTENTS</td>
<td>3</td>
</tr>
<tr>
<td>LIST OF ABBREVIATIONS</td>
<td>5</td>
</tr>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>6</td>
</tr>
<tr>
<td>- Characteristics and Opportunities of Existing Autonomous Vehicles</td>
<td>6</td>
</tr>
<tr>
<td>- Threats and Risks Posed by Autonomous Vehicles</td>
<td>7</td>
</tr>
<tr>
<td>- Regulatory Environment</td>
<td>9</td>
</tr>
<tr>
<td>- Implications for the Security Sector</td>
<td>9</td>
</tr>
<tr>
<td>- Conclusion</td>
<td>10</td>
</tr>
<tr>
<td>- Research Methodology</td>
<td>10</td>
</tr>
<tr>
<td>CHAPTER 1: ABOUT THIS REPORT</td>
<td>11</td>
</tr>
<tr>
<td>- Study Aim</td>
<td>11</td>
</tr>
<tr>
<td>- Methodology</td>
<td>12</td>
</tr>
<tr>
<td>CHAPTER 2: CHARACTERIZATION, CATEGORIZATION, AND OPPORTUNITIES OF EXISTING AUTONOMOUS VEHICLES</td>
<td>15</td>
</tr>
<tr>
<td>- Introduction</td>
<td>15</td>
</tr>
<tr>
<td>- Uncrewed Aerial Vehicles</td>
<td>16</td>
</tr>
<tr>
<td>- Autonomous Ground Vehicles</td>
<td>18</td>
</tr>
<tr>
<td>- Autonomous Maritime Vehicles</td>
<td>19</td>
</tr>
<tr>
<td>- Autonomous Weapons Systems</td>
<td>21</td>
</tr>
<tr>
<td>- Classification and Levels of Autonomy</td>
<td>22</td>
</tr>
<tr>
<td>- Summary</td>
<td>24</td>
</tr>
<tr>
<td>CHAPTER 3: RISKS AND THREATS POSED BY AUTONOMOUS VEHICLES</td>
<td>25</td>
</tr>
<tr>
<td>- Introduction</td>
<td>25</td>
</tr>
<tr>
<td>- Threats to Autonomous Vehicles</td>
<td>25</td>
</tr>
<tr>
<td>- Threats From Autonomous Vehicles</td>
<td>26</td>
</tr>
<tr>
<td>- Hardware and Performance</td>
<td>29</td>
</tr>
<tr>
<td>- Black-Box Challenges and Explainability</td>
<td>29</td>
</tr>
<tr>
<td>- Autonomy Levels, System Function and Degrees of Risk</td>
<td>30</td>
</tr>
<tr>
<td>- Ethical Challenges</td>
<td>31</td>
</tr>
<tr>
<td>- Public Perceptions</td>
<td>33</td>
</tr>
<tr>
<td>- Summary</td>
<td>34</td>
</tr>
</tbody>
</table>
## LIST OF ABBREVIATIONS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AAV</td>
<td>Autonomous Aerial Vehicle</td>
</tr>
<tr>
<td>ADS</td>
<td>Automated Driving Systems</td>
</tr>
<tr>
<td>ADAS</td>
<td>Advanced Driver Assistance</td>
</tr>
<tr>
<td>AGVs</td>
<td>Autonomous Ground Vehicles</td>
</tr>
<tr>
<td>AMVs</td>
<td>Autonomous Maritime Vehicles</td>
</tr>
<tr>
<td>ASVs</td>
<td>Autonomous Surface Vehicles</td>
</tr>
<tr>
<td>AV</td>
<td>Autonomous Vehicles</td>
</tr>
<tr>
<td>AUV</td>
<td>Autonomous Underwater Vehicles</td>
</tr>
<tr>
<td>AWS</td>
<td>Autonomous Weapons Systems</td>
</tr>
<tr>
<td>DILR</td>
<td>Detect, Identify, Locate, and Report</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FAA</td>
<td>Federal Aviation Administration (FAA) (US)</td>
</tr>
<tr>
<td>GGE on LAWS</td>
<td>Group of Governmental Experts on Lethal Autonomous Weapons Systems</td>
</tr>
<tr>
<td>GPS</td>
<td>Global Positioning System</td>
</tr>
<tr>
<td>IEEE</td>
<td>Institute of Electrical and Electronics Engineers</td>
</tr>
<tr>
<td>IHL</td>
<td>International Humanitarian Law</td>
</tr>
<tr>
<td>IP</td>
<td>Intellectual Property</td>
</tr>
<tr>
<td>IS</td>
<td>Islamic State</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>NHTSA</td>
<td>National Highway Traffic Safety Administration</td>
</tr>
<tr>
<td>PTA</td>
<td>Pilotless Target Aircraft (PTA)</td>
</tr>
<tr>
<td>PRISMA</td>
<td>Preferred Reporting Items for Systematic reviews and Meta-Analyzes</td>
</tr>
<tr>
<td>SEAD</td>
<td>Suppression of Enemy Air Defenses</td>
</tr>
<tr>
<td>SAE</td>
<td>Society of Automobile Engineers</td>
</tr>
<tr>
<td>SIPRI</td>
<td>Stockholm International Peace Research Institute</td>
</tr>
<tr>
<td>UAV</td>
<td>Uncrewed Aerial Vehicle (or Unmanned Aerial Vehicle)</td>
</tr>
<tr>
<td>UAS</td>
<td>Uncrewed Aircraft System (or Unmanned Aircraft System)</td>
</tr>
<tr>
<td>UNESCO</td>
<td>United Nations Educational, Scientific, and Cultural Organization</td>
</tr>
<tr>
<td>XAI</td>
<td>Explainable Artificial Intelligence</td>
</tr>
</tbody>
</table>
EXECUTIVE SUMMARY

The potential of autonomous vehicles (AVs) has been growing since the 1990s. Though AV proponents have often over-promised and under-delivered in the past, advances in artificial intelligence (AI) are now enabling autonomous applications to develop at faster rates. Opportunities for the use of AVs span commercial, military, and security sectors and cover land, air, sea, and under-the-sea domains. These new technologies offer logistical, operational, and technical benefits, but they also bring with them a range of threats, risks, and challenges that may limit their use or slow down their deployment.

This report documents the threats, risks, challenges, and opportunities presented by AVs in several fields to provide recommendations for their use by security practitioners. It shows how practitioners can benefit from advances in AV technologies while avoiding unexpected or unintended consequences.

AVs may be characterized as systems that can operate with minimal degrees of human input or none. Automation in vehicles implies the replacement of some or all human control in a system by electronic, mechanical, or other sensory devices.1 Autonomy in systems has been applied for mobility (homing, navigation, take-off and landing), remote control of systems by human operators (carrying out pre-programmed activities), targeting (target recognition and tracking), intelligence (detection of objects, devices, intrusion, weapon fire, map generation, threat assessment, and big data analytics), interoperability (cooperating with other security/military systems), and the health management of systems (self-recharging/refueling, diagnosis, and repair).2

For security practitioners, there is a bewildering array of national and international regulations, industry frameworks, and emerging standards and guides to be navigated. Even the term "autonomous" is problematic because it is used to mean so many different things, from programmed automation to systems with self-learning capabilities. The aim of this research was to help security practitioners better understand this complex, disparate field to better manage the associated threats, risks, and opportunities.

Characteristics and Opportunities of Existing Autonomous Vehicles

The development and manufacture of autonomous vehicles are expanding rapidly for maritime, ground, and aerial use. The practical and ethical challenges they generate are highly complex and will continue for the foreseeable future. The degree of complexity, in turn, is influenced by the level of autonomy within a particular vehicle or system. This is happening across both civilian and military contexts and extends to include autonomous weapon systems. Security practitioners will need to keep abreast of developments in the legal and safety frameworks to which they must comply. However, potential rewards are significant, given the wide range of current and potential applications, including:

- Accessing remote and challenging terrains
- Acoustic sensors to detect loud noises such as explosions
- Asset inspection
- Carriage and transportation of goods
- Data collection for security operations
- Detection and disposal of explosives
Firearm response
Identification and retrieval of lost assets
Personnel transportation
Risk assessment
Search and rescue of personnel
Securing infrastructure
Securing personnel
Security communications and information exchange
Thermal imaging
Video surveillance

Advances in AV development present significant new commercial opportunities for businesses. Compared with conventional vehicles, autonomous systems can be less costly, more reliable, faster in performing tasks, and more environmentally sustainable; reduce labor costs; increase safety because of the absence of human error; and allow for the concurrent execution of tasks. Flexible consumption models (FCMs), also called ‘as-a-service’ (XaaS) models, bring further benefits by supplying services on a non-ownership, pay-as-you-go basis. These are adaptable to the pace of technological advancement, since they save the potential user from investing in technology that quickly becomes obsolete; they are more environmentally sustainable; and they can be significantly more cost-effective. ‘Drone-as-a-security-service’ innovations include the development of drone-in-a-box systems, which can cover much greater areas than ground-based equipment and personnel; providing an additional layer of security for patrol and quick reaction; and tethered drone systems, with theoretically unlimited flight times.

Threats and Risks Posed by Autonomous Vehicles

The positive impacts and potential opportunities for AVs are numerous. However, their production and use, particularly at these early stages of their evolution, present various challenges to the safety and security of AV systems, including unlawful uses, hardware and performance issues, the explainability of the AI that powers autonomy, ethical concerns, and public mistrust.

Key threats to the safety and security of AVs relate to their safe operation and cybersecurity, since they are based on a combination of digital technologies, sensory techniques, and AI platforms. The primary focus of the regulation of civilian AVs is safety, and the proliferation of AVs requires robust safety and quality standards. Kobaszyńska-Twardowska, et al., identify six sources of potential hazards to UAV operation, which are equally applicable to other types of AVs. These are:

- Human error (due to such factors as poor communication among the operating team, insufficient training of personnel, fatigue, or pressure from a supervisor to deploy in inappropriate conditions)
- Failure to comply with procedures
- Failure of the vehicle or system
- The appearance of another vehicle on a collision course
- Rapid deterioration in weather conditions
- Deterioration in the performance of systems used in steering or navigation, such as GPS.
Cybersecurity of AVs is also a significant concern, since they communicate through wireless channels that are not secure by default. These platforms are liable to cyberattack by actors who intend to disrupt, damage, or tamper with AVs. Threat actors, which range from individual, autonomous attackers to organized groups operating as part of a criminal enterprise or on behalf of a nation state, work to infiltrate, destabilize, or attack computer systems on which AVs operate.

A classification by Jackman and Hooper divides the threats from AV systems into four categories:

- Image and video capture (of critical or sensitive infrastructure, commercial sites or activities, or emergency service operations; for reconnaissance; to invade privacy; or as a means of abuse or stalking of individuals, e.g., ex-partners)
- Transport and carrying of weaponry or contraband
- Data collection (for cyberattacks or corporate espionage)
- Disruption (of sites, events, or activities, such as airports, political events, sporting events, or emergency service operations)

The weaponization of small, off-the-shelf commercial drones is now a significant dimension of warfighting in Yemen, Ukraine, and Gaza. These commercial-grade drones are used for reconnaissance, situational awareness, and the deployment of small explosives or grenades. Terrorists developing similar capability increases the potential threat to national infrastructure and other buildings and objects. Small UAVs can be fast, agile, and difficult to identify and track, and harder still to forcefully remove from the sky.

Notable drone attacks on critical infrastructure, each attributed to Houthi terrorists in Yemen, include:

- A swarm attack of 25 drones and missiles on Saudi Aramco oil processing facilities at Abqaiq and Khurais in Saudi Arabia, disrupting production by around 5 million barrels per day, equivalent to 5 percent of global production (2019)
- Attacks on oil tankers near Abu Dhabi International Airport, killing three and injuring six others (2022)
- Multiple attacks on commercial shipping vessels in the Red Sea, one of the world’s most important trade routes.

Where AVs incorporate higher and higher levels of autonomous capability, signal disruption becomes less of a threat, but the AI involved in such systems bring their own challenges to ensure consistency, safety, and reliability. The cyber element alone poses multiple threats: damage can render a system unusable, hacking could result in control of an AV even being taken by criminals or terrorists, while spoofing—confusing the system—could have similarly disastrous consequences. Looking to the future, the following trends are anticipated:

- Security concerns will escalate as commercial AVs are increasingly adapted by criminal organizations and terrorist groups as lessons are learned from war zones like Ukraine and Gaza.
- The relatively low cost of sophisticated surveillance capabilities will challenge security, police, and military organizations.
- The interconnectedness of AVs in air, land, and surface and subsurface sea domains will further test security capabilities.
- Where commercial AVs rely on a live signal to operate, these will become increasingly vulnerable to hacking and spoofing.
Public perceptions of the trustworthiness of AVs and autonomous systems overall will have significant impact on whether governments will take social and economic risks to license new systems. Manufacturers and developers will also need to make careful risk calculations about systems that may be less predictable than their analog forebears. New ethical challenges will continue to emerge as autonomy develops in sophistication and application. For example, if autonomous systems include CCTV or facial recognition, the right to privacy of private citizens may be violated if the systems are used in public places. This could be further compounded if the AI which powers the autonomous system is not sufficiently explainable to provide reasons why the violation of privacy occurred.

Regulatory Environment

Faced by the risks presented by AI systems and the autonomous systems supported by AI, the global community is now engaged in a “race to AI regulation.” Efforts to regulate AI in its application to AVs have been disparate and fragmented. Some have characterized efforts to govern AI as an exercise similar to herding cats, especially if policy makers focus on the nature of technologies instead of the risks and opportunities presented by AI.18 Autonomous land, aerial, and maritime vehicles have all been treated differently when it comes to the development of regulations even though some systems, for example swarming systems, operate across all those domains and may utilize the same models for their operation. Thus, there are five strands to the regulation of AVs:

1. General AI regulation through international, national, and institutional initiatives: most AVs are likely to utilize AI-based technologies, especially with developments in machine learning

2. Regulation of uncrewed aerial vehicles

3. Regulation of autonomous ground vehicles

4. Regulation of autonomous maritime vehicles

5. Regulation of autonomous weapons systems

Governments and international organizations are wrestling with how to regulate AVs in ways that will maximize social, economic, and military benefit while minimizing harm. Different bodies take different approaches, with some focusing on technical aspects and capabilities, while other approaches concentrate on the risks and opportunities involved. These efforts have not fully addressed the needs and risks presented by emerging technologies in the area of AVs or employed a holistic approach to regulation. A multisectoral and integrated regulatory framework is needed that governs the development and use of the five strands of AV technologies more comprehensively.

Implications for the Security Sector

The management of risks and threats presented by AVs is a pressing concern for security practitioners, especially as the technologies become more ubiquitous, with uncrewed aircraft systems being a key area of focus. They must be cognizant of the security risks and threats to AVs being employed by their organizations or clients, as part of the growing cyber-physical organizational landscape. This requires the recognition of such risks in organizational risk management frameworks, based on a strong understanding of prevention, detection, and mitigation countermeasures, as well as an awareness of challenges on the horizon and key areas of future innovation. A collaborative approach to security is also needed, in recognition of the pace of technological advancement and the complexity of the risk environment. Organizations like ASIS Interna-
tional can play a key role in bringing stakeholder communities together and sharing expertise.

In contributing to the protection of such systems, security practitioners can capitalize on the benefits of AVs that are transforming other sectors and incorporate them more actively in the security arsenal: such technologies have never been cheaper or more accessible. They must also keep up to date with necessary legislation and regulatory requirements in the jurisdictions where AVs and autonomous systems are designed and built, as well as where they may be used or sold. With regulations proliferating, this challenge will only grow.

Conclusion

AVs present pressing security challenges, both as a risk to be managed, and as increasingly important organizational tools forming part of the cyber-physical landscape needing to be secured. This report highlights key considerations in delivering security in these two respects. AVs also have the potential to transform and improve security practice. The use of AVs has been transformative in many sectors, and had a dramatic impact on markets, user behavior, and attitudes toward the services provided. The security sector should anticipate such changes, while at the same time being prepared to contribute to the harmonization of service provision in accordance with multisectoral needs, national and international guidelines and laws, and public perceptions of the use of emerging technologies.

Research Methodology

The research was commissioned by the ASIS Foundation and undertaken between August 2023 and February 2024. It employed the methodology of a scoping review: a type of knowledge synthesis suitable for exploratory research projects. It is based on a systematic approach to mapping the evidence on a topic and identifying key concepts, theories, findings, sources of evidence, and knowledge gaps. Like a systematic review, it is a systematic, transparent, and replicable process that provides a useful approach to examining emerging evidence when the more specific questions that can be addressed through a more precise systematic review are not yet clear. A scoping review can extend to gray literature that is not published by commercial publishers, or indexed in research databases, such as governmental or private sector research or white papers, dissertations, and conference papers.

In the case of AVs, the vast and rapidly evolving literature spans the different technological dimensions and categories of autonomous vehicles; ranges across several academic disciplines; includes an extensive gray literature alongside the academic, including government documents and industry white papers; and includes existent and prospective laws and regulatory frameworks across multiple jurisdictions. The chosen methodology reflects the difficulty in capturing such a broad range of dimensions through empirical research, and the need to synthesize the existing body of knowledge in the first instance to identify the key parameters and dimensions of the field.
The potential of autonomous vehicles (AVs) has been growing since the 1990s. Though AV proponents have often over-promised and under-delivered in the past, advances in artificial intelligence (AI) are now enabling autonomous applications to develop at faster rates. Highly automated vehicles, human-operated vehicles with AI-based assistance, and self-driving vehicles all fall under the banner of AV in this report. Opportunities for the use of AVs span commercial, military, and security sectors and cover land, air, and sea domains. These new technologies offer logistical, operational, and technical benefits, but they also bring with them a range of threats, risks, and challenges.

The following drone examples highlight the scale of the challenge and the ways in which security interests can overlap with military and commercial activities. In Columbia, small, commercial drones have been used for several years by drug gangs and narco-terrorist groups for surveillance. However, they are now being converted to carry small amounts of explosives. Similarly, two explosive-equipped small drone attacks in the Moscow financial district brought new security challenges into the realm of commercial and banking activity. At the time of writing, Iran-supporting Houthis in Yemen are using drones to attack cargo ships and disrupt maritime traffic in the Red Sea, one of the world’s busiest shipping lanes, disrupting supply chains while posing military challenges and security problems for shipping companies.

In this research report, Bhila, Wakefield, and Lee have identified a significant change in the complexity and level of security threat posed by rapid advancements in AVs. This report documents the threats, risks, challenges, and opportunities presented by AVs in several fields to provide recommendations for their use by security practitioners. It shows how such practitioners can benefit from advances in AV technologies while avoiding unexpected or unintended consequences.

AVs may be characterized as systems that can operate with minimal degrees of human input or none. Automation in vehicles implies the replacement of some or all human control in a system by electronic, mechanical, or other sensory devices. Autonomy in systems has been applied for mobility (homing, navigation, take-off, and landing); remote control of systems by human operators (carrying out pre-programmed activities); targeting (target recognition and tracking); intelligence (detection of objects, devices, intrusion, weapon fire, map generation, threat assessment, and big data analytics); interoperability (cooperating with other security or military systems); and the health management of systems (self-recharging or refueling, diagnosis, and repair).

For security practitioners, there is a bewildering array of national and international regulations, industry frameworks, and emerging standards and guides to be navigated. Even the term “autonomous” is problematic because it is used to mean so many different things, from programmed automation to systems with self-learning capabilities.

**STUDY AIM**

The aim of this research is to help security practitioners better understand this complex, disparate field to better manage the associated threats, risks, and opportunities. This report walks the reader through key considerations associated with AVs: the different forms they take and the opportunities they present; the threats and risks both to and from AVs in civil, commercial, and military spaces, encompassing ethical, legal,
cybersecurity, privacy and technical challenges; existing regulatory frameworks; prospects for new regulatory frameworks that will demand future compliance; and the key implications of AVs for the security sector.

There is a greater emphasis on uncrewed aerial vehicles (UAVs)\textsuperscript{24} in the report than other types of AVs. This reflects the distinct ways in which different types of AV have emerged. AVs have been conceptualized and developed since the 1950s\textsuperscript{25} and, due to recent and ongoing developments in AI, AVs have become easily accessible to the public. Low-cost, small, off-the-shelf UAVs, or hobby drones, have proliferated. Each has prompted significant controversy and greater political, public, and professional discussion about legality, human rights, privacy, and other concerns about regulatory frameworks. In this report, we use the term ‘drone’ according to its most common usage, as an alternative term for a UAV. The term uncrewed aircraft system (UAS) is also commonly used in relation to UAVs, the difference being that a UAS encompasses the UAV (or drone) as well as the equipment to control it remotely.\textsuperscript{26,27} Related security guidance often refers to the whole system, not just the UAV.

In addition to new regulatory frameworks, AVs prompt ethical questions in a way that previous generations of technology did not. These include issues surrounding human-machine interaction, predictability, trustworthiness, terminability, ability to evolve, algorithmic bias, explainability, traceability, accountability, and responsibility. A novel feature of this study is its global, context-based approach when considering the use of AVs in security.

**METHODOLOGY**

The research employed the methodology of a scoping review: a type of knowledge synthesis suitable for exploratory research projects. It is based on a systematic approach to mapping the evidence on a topic and identifying key concepts, theories, findings, sources of evidence, and knowledge gaps. Like a systematic review, it is a systematic, transparent, and replicable process that provides a useful approach to examining emerging evidence when the more specific questions that can be addressed through a more precise systematic review are not yet clear. A scoping review can extend to gray literature that is not published by commercial publishers, or indexed in research databases, such as governmental or private sector research or white papers, dissertations, and conference papers.

In addition to new regulatory frameworks, AVs prompt ethical questions in a way that previous generations of technology did not.

In the case of AVs, the vast and rapidly evolving literature spans the different technological dimensions and categories of autonomous vehicles; ranges across several academic disciplines; includes an extensive gray literature alongside the academic, including government documents and industry white papers; and includes existent and prospective laws and regulatory frameworks across multiple jurisdictions. The chosen methodology reflects the difficulty in capturing such a broad range of dimensions through empirical research, and the need to synthesize the existing body of knowledge in the first instance to identify the key parameters and dimensions of the field.

Our approach is summarized in Figure 1.1. The research, commissioned by the ASIS Foundation and undertaken between August 2023 and February 2024, utilized two sources of data: academic and gray literature. The academic data collection comprised searches for academic literature from Scopus, Web of Science, and Google Schol-
Searches were for English language sources using the terms "autonomous + vehicles" in social science and arts and humanities literature. This search criterion was also limited only to “autonomous underwater vehicles, unmanned aerial vehicles, and unmanned surface vehicles.” This yielded 132 articles and books. Separate searches were run for “autonomous underwater vehicles + autonomous maritime vehicles + threats” (nine articles), “autonomous underwater vehicles + autonomous maritime vehicles + risks” (28 articles), and “autonomous underwater vehicles + autonomous maritime vehicles + opportunities” (17 articles).

These searches were repeated for unmanned aerial vehicles and autonomous ground vehicles controlling for threats, risks, and opportunities. A total of 1,244 articles and books or chapters were found. Researchers completed the following initial removals: incomplete sources, no author (n=37), no source (n=27), duplicates (n=247). This narrowed down the sources to 932. Of these 932, only 4.6 percent (n=43) addressed our topic directly. The rest addressed issues such as how to deal with technical problems of AVs, laboratory tests of new types of AVs, enhancing communication systems in AVs, and other technical tests.

Figure 1.1: Flow diagram of the systematic scoping review
The second source was gray literature from databases. Researchers sought policy documents from the following organizations:

- Centre for the Governance of AI
- European Union
- Institute of Electrical and Electronics Engineers (IEEE)
- International Organization for Standardization (ISO)
- International Maritime Organization (IMO)
- National Institute of Standards and Technology (NIST), US Department of Commerce
- OECD.AI repository for AI policies and strategies
- Stockholm International Peace Research Institute (SIPRI) database on autonomy in weapons
- Society of Automotive Engineers (SAE) International
- Stanford Institute for Human-Centered Artificial Intelligence (HAI)
- United Nations Educational, Scientific and Cultural Organization (UNESCO)
CHAPTER 2: CHARACTERIZATION, CATEGORIZATION, AND OPPORTUNITIES OF EXISTING AUTONOMOUS VEHICLES

INTRODUCTION

Three categories of autonomous vehicles (maritime, aerial, and ground) and a separate category of autonomous weapons systems are examined in this chapter. The first three refer to autonomous vehicles for either civilian or military use. The fourth category of weapon systems incorporates maritime, aerial, and land autonomous elements. Opportunities associated with the different categories and uses of AVs will be discussed in each section. Although this chapter classifies and treats AVs in separate categories, it is essential to note that the potential presented by the interoperability of AVs from all the different categories is an opportunity from which the security sector can greatly benefit. Systems can collaboratively work together regardless of the domain they belong to and share information about targets, secured assets, and other factors, making decisions faster and security more efficient.

This chapter will also describe the characteristics and levels of autonomy set out by the Society of Automobile Engineers (SAE) in a well-recognized classification used by such bodies as the European Union (EU) and the US National Highway Traffic Safety Administration (NHTSA) as they develop legal and safety frameworks for the development and deployment of autonomous vehicles. While the original SAE classification was intended for automobiles, it now provides a helpful basis for classifications across all land, sea, and air domains.

AVs have a wide variety of current and potential applications in security, military, and civilian domains, including personnel transportation, cargo transportation, communications, surveillance, fire detection, mine detection, defense, targeting, and attacking of targets. They can operate in single robot or swarm form. A robotic swarm is defined as a collective of autonomous vehicles that operate in cooperation while utilizing the same hardware and software.28 Swarm robotics are inspired by the organization and working of insects like bees, ants, and termites, and other living organisms like fish, bats, and birds.29 These swarms have the capability to work in unison and to utilize independent intelligence based on their environment of operation.30 Swarm robotics can operate more effectively than bigger AVs in complex or small spaces or environments.31 An example of such a system is the bat algorithm (BAT), which employs echolocation (the use of reflected sound waves) to identify and avoid obstacles.32 The many applications of swarming technology include farming, emergency response in disasters, and even entertainment.33

Advances in AV development are enhancing their safety and making them cheaper.34 Compared with conventional vehicles, autonomous systems can be less costly, more reliable, and faster in performing tasks; reduce labor costs; increase safety because of the absence of human error; enable access to remote and dangerous areas; allow for the concurrent execution of tasks; and present new commercial opportunities for businesses.35 Some AVs have the capability to operate in environments with little or no GPS or internet communications.36 37 Human-machine collaboration (HMC) and human-machine teaming (HMT) can enable users to get the best out of such technologies, “augmenting human weaknesses with machine strengths (and vice versa),” with HMC focusing on optimizing cognitive tasks, particularly decision-making, and HMT focused on more effectively executing a
wider range of complex tasks in physical spaces. Flexible consumption models (FCMs), also called “as-a-service” (XaaS) models, are a growing business model in the technology industry that make products more accessible to potential users by providing them on a non-ownership basis. Concepts like “drone-as-a-service,” “autonomy-as-a-service,” and “mobility-as-a-service” refer to the supply of autonomous vehicles according to this model, giving a means for potential users to harness the benefits of such products cost-effectively. Given the pace of AV development, the as-a-service model protects an organization from purchasing a product that could be obsolete by the time it is fully integrated into the organization’s processes.

In a variety of ways, AVs can be much more environmentally sustainable than conventional vehicles by reducing the amount of fuel used: they are generally smaller than comparable crewed vehicles; they employ connectivity technology and automated driving support systems to optimize journey routes; they use sustainable power sources; and they can employ vehicular platooning (the joining of two or more vehicles in convoy), which reduces air-drag friction. It was claimed that the Yara Birkeland autonomous electric ship, which had its first voyage in 2021, would reduce CO2 emissions by 1,000 tons and replace 40,000 trips by diesel-powered trucks per year. Shared autonomous vehicles (SAVs), providing on-demand mobility services offer the prospect of reducing vehicle emissions and improving energy efficiency while also meeting increasing travel demand and enhancing the performance of the urban transportation system.

**UNCREWED AERIAL VEHICLES**

Uncrewed Aerial Vehicles (UAVs) are the focus of this section, as opposed to Autonomous Aerial Vehicles (AAVs). While AAVs are under development, at the time of writing no fully autonomous systems are operational. The combination of UAV and Internet of things (IoT) technology has enabled numerous innovations, in conjunction with IoT sensors on the ground, including the Internet of drones (IoD), which is concerned with the potential of drones to be networked and remotely controlled. It is no surprise that the market for UAVs is expanding rapidly: according to Research and Markets, the global drone market is anticipated to exceed USD 185 billion per annum by 2028, increasing from USD 45.63 billion in 2022.

In response to market demands, UAVs come in different shapes, sizes, and with different uses and capabilities, with various degrees of system complexity. Adding to that complexity is the introduction of increasingly autonomous elements in systems. At one end of the scale are large, fixed-wing drones, like the American Global Hawk and Sky Guardian, the Turkish TAI Aksungur, or the Chinese Gongji-11 Sharp Sword, and at the other are small, off-the-shelf units. Kong divides UAVs into the following three classes in terms of size, operating altitude, and flying range:

- **Small UAV:** Operates at an altitude up to 300 meters, and a range of up to 3 kilometers. Weight for small UAV should not exceed 24 kilograms.
- **Medium UAV:** Operates at an altitude above 300 meters but below 5,500 meters, and a range above 3 kilometers but below 200 kilometers.
- **Large UAV:** Operates at an altitude above 5,500 meters, and a range above 200 kilometers.

Studies have mainly identified multirotor or multicopter crafts as the most used form of UAV, with variances from tricopters, quadcopters, hexacopters, and octocopters, their names indicating the numbers of rotors. Other ways of classifying UAVs include weight, wing-span, payload capacity, power source, and type of engine. An important advance-
ment in UAV technology is the development of “drone-in-a-box” systems. While traditional drones are manually operated, drone-in-a-box solutions deploy autonomously from a docking and charging station to carry out preprogrammed instructions. They offer much greater efficiency than manual drones, as a single operator can control multiple devices.56 Another area of innovation is in the area of tethered drones, which receive their power and connectivity from a terrestrial base station and thus allowing for much longer flight times.57 These include hybrid tethered/untethered drones that can release the tether and continue in free flight for a limited timeframe.58

Current UAVs can perform various complex tasks. For example, the X-47B aircraft used by the U.S. army can support military operations, while also being able to perform aerial refueling and collaboration with human operators of other aircrafts.59 Other systems can operate both as solitary UAVs and as swarming systems. Shield AI’s new V-BAT UAVs have been designed to carry out surveillance and can “classify, track, read, and react to targets,” with the capability to operate as a swarm.60 During their demonstration in August 2023, Shield AI tasked a team of three V-BAT systems to detect, identify, locate, and report (DILR), even in GPS-denied environments.61 Unlike satellite imagery, UAVs can avoid cloud cover as they gather and transmit data.62

Opportunities

Autonomous aerial vehicles can fulfill many functions, the most significant being carrying and transportation, aerial imagery capture, and aerial data gathering, with applications across...
numerous civilian sectors. These include agriculture, construction, emergency services, energy and utilities, humanitarian aid and disaster relief, insurance, local administration, last and middle mile delivery, manufacturing, security, and telecommunications. Drone technologies provide transportation and delivery of commercial and medical goods, monitoring and inspection of sites and key assets, aerial photography and videography of events, crop spraying, and many other services. Because they can operate in harsh weather conditions, UAVs can perform more efficiently than satellite imagery. An emerging area of UAV deployment is the context of smart cities, fulfilling a breadth of urban management functions such as traffic management, inspecting and maintaining urban infrastructure, environmental monitoring, and public space video surveillance.

AUTONOMOUS GROUND VEHICLES

Autonomous ground vehicles (AGVs) are cars and other systems that can operate on- or off-road with little or no human intervention, using sensors, actuators, communication, and AI components. An academic review of AGV configurations for underground applications identifies three main types: wheeled, tracked, and what the authors term ‘bio-inspired robots’, the former ranging from four-wheeled designs to multi-wheeled configurations that can be better suited to cargo transportation or traversing uneven terrain. Tracked AGVs, while slower in speed, are a useful alternative to wheeled AGVs on uneven and soft-soiled terrain. The bio-inspired robots identified in the research are typically small in size and employ locomotive mechanisms borrowed from the natural world.

Key Takeaways- (Autonomous Ground Vehicles)

AGVs
- These are vehicles with capabilities for self-driving.
- They have mostly been developed for road transportation and have 6 levels of autonomy.

Uses for Security
- Offroad logistics (transporting security equipment).
- Detection and disposal of explosives.
- Firearm response.
- Surveillance & securing of premises.
- Rescue missions and personnel transport.

Uses for other sectors
Fire-fighting, passenger transportation, explosive ordnance, agriculture, military logistics, health sector logistics etc.

Future Uses
- Transportation of and securing high-value goods (this requires future AGVs to be safe from hacking and to have full defensive capabilities that are fail-safe).
- Coordination with other systems (aerial, maritime, and human).
in order to fulfill a wide variety of functions. They include legged, snake-like, earthworm-inspired, climbing, rolling, jumping, and hybrid motion robots.

The first self-driving car was showcased at the 1939 World Fair. With the advent of AI and machine learning techniques, autonomous cars have become abundant, with different levels of autonomy in almost all cars being developed. Examples of autonomous behavior in cars include advanced cruise control, obstacle avoidance mechanisms, anti-lock brake systems, emergency stopping, convoying, and lane tracking, among other behaviors. Companies like Motional, Cavnue, and Zoox, amongst others, are heavily invested in developing fully autonomous cars, particularly for civilian use. Recent estimates suggest that there will be more than eight million fully autonomous or semi-autonomous vehicles by 2025. Companies like Motional, Cavnue, and Zoox, amongst others, are heavily invested in developing fully autonomous cars, particularly for civilian use. Recent estimates suggest that there will be more than eight million fully autonomous or semi-autonomous vehicles by 2025. Perhaps the most well-known modern autonomous ground vehicles are those produced by Tesla. All new Tesla models have “autopilot” or “full self-driving” capabilities, enabling them to operate using cruise control, autosteer, change lanes, identify and react to traffic lights, and autopark. However, Tesla warns that there should always be an “attentive (human) driver.” Consequently, the vehicles are not yet fully autonomous although their development is meant to achieve full autonomy in the near future. Google’s autonomous vehicle, now known as Waymo One, is also well-known for being the first autonomous ride-hailing service/taxi. Levels of autonomy pertinent to AVs as a whole are further discussed later in the chapter.

Opportunities

The opportunities provided by AGVs are numerous. Their primary uses include passenger and cargo transport, delivery, and surveillance, offering many current and potential applications in smart cities, with other urban applications including cleaning and autonomous wheelchairs. A 2023 study of ridehail cars by General Motors (GM), Cruise LLC, the University of Michigan Transportation Research Institute (UMTRI), and the Virginia Tech Transportation Institute (VTTI) suggests that AI-driven cars have the potential to perform more safely on the roads, causing fewer accidents than human-driven cars. Autonomous cars have the potential to impact lifestyle choices, ranging from the reduction of private car ownership, elimination or reduction of fixed-route transit, changes in land use and design, and changes in market conditions. While there are new opportunities with new products, there is also the potential disadvantage of decreasing sales of automobiles if autonomous capability increases overall cost of cars and other ground vehicles.

The off-road capabilities of some autonomous ground vehicles also make them ideal for a variety of functions. In an industrial context, they can be useful for large-scale agricultural jobs like sowing seeds and spraying pesticides, and accessing harsh and unexplored landscapes for mapping, mining, or scientific purposes, including space, as in the case of the Mars Rover. Their numerous military, humanitarian, and security applications include logistics in environments with obstructive vegetation, transporting personnel, securing premises, search and rescue, explosive ordnance detection and disposal, and firefighting, and they can be especially useful in contexts and terrains that are risky to human drivers, such as areas populated with landmines.

AUTONOMOUS MARITIME VEHICLES

There are two types of autonomous maritime vehicles (AMV): autonomous underwater vehicles (AUVs) and autonomous surface vehicles (ASVs). AMVs are systems that can operate independently of a host vessel, with various capabilities like the ability to carry payloads including imaging and oceanographic instruments.
These systems can be used for scientific, exploratory, commercial, security, and military purposes. AUVs are especially advantageous when environments are unknown and dangerous. They have been used for cooperative transportation, surveillance, and interception.

**Opportunities**

AUVs have existed since at least 1953, when Dimitri Rebikoff developed a remotely operated vehicle named POODLE. Because of safety concerns, AUVs present a cheaper and safer option for ocean expeditions, rescue missions, the protection of ocean resources from pollution, scientific expeditions, and enhancing national and border security through surveillance. The security and defense sectors can also benefit from the early identification, defense, and retrieval of assets lost at sea. Autonomous systems can be used as defense systems capable of offensive missions where they probe enemy targets in forward-sea areas and defensive missions where they react to enemy intrusion by air, land, and sea. With the potential of autonomous systems being acquired by terrorists and malicious actors, autonomous underwater vehicles are also useful in the defense of underwater and port infrastructure from attacks by such actors. In addition, autonomous systems can acquire data from underwater environments that humans cannot access, such as underneath ice sheets.

---

**Key Takeaways- (Autonomous Maritime Vehicles)**

**AMVs**
- AMVs can be in the form of surface (ASVs) or underwater (AUVs) vehicles.
- AMVs can operate independently of a host vehicle and can carry payloads.

**Uses for Security**
- Identification and retrieval of lost assets.
- Rescue missions.
- Personnel security.
- Securing port infrastructure.
- Securing ships, boats, and other sea equipment.
- Sea-land communications.

**Uses for other sectors**
Scientific exploration, expeditions, protection of marine environments, national security, surveillance, maritime recreational activities.

**Future Uses**
- AMVs are projected to have the potential of improving research, transportation, environmental sustainability, energy efficiency, and various other sectors. It is essential that security professionals learn from and harness these advances.
AUTONOMOUS WEAPONS SYSTEMS

Autonomy in weapons has been used to enable machines to move, target, survey, and engage objects using sensors and without human intervention. Importantly, autonomous weapons can only function as part of larger technological and human systems. Most of the autonomous weapons in existence are defensive, with loitering munitions the only offensive systems currently available. However, only 89 states across the world are operating air defense systems. SIPRI’s dataset on autonomy in weapons shows that the largest share of autonomous weapons (at least 27.7 percent) are made by the United States, with Israel, China, South Korea, India, France, Italy, Germany, and Russia also contributing more than a combined 50 percent of the autonomous weapons in existence. Figure 2.1 shows the distribution of the countries of origin of various autonomous weapons systems. Although autonomous weapons systems have been classified separately in this study, they exist in various forms, including but not limited to all forms of AVs.

<table>
<thead>
<tr>
<th>Country of origin</th>
<th>% of existing autonomous weapons</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>27.7%</td>
</tr>
<tr>
<td>Israel</td>
<td>13.2%</td>
</tr>
<tr>
<td>Russia</td>
<td>10.2%</td>
</tr>
<tr>
<td>France</td>
<td>9.5%</td>
</tr>
<tr>
<td>Italy</td>
<td>7.7%</td>
</tr>
<tr>
<td>China</td>
<td>7.5%</td>
</tr>
<tr>
<td>India</td>
<td>6%</td>
</tr>
<tr>
<td>Germany</td>
<td>5.2%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>5%</td>
</tr>
<tr>
<td>Sweden</td>
<td>3%</td>
</tr>
<tr>
<td>South Korea</td>
<td>3%</td>
</tr>
<tr>
<td>Japan</td>
<td>1.5%</td>
</tr>
<tr>
<td>Norway</td>
<td>0.5%</td>
</tr>
</tbody>
</table>

Figure 2.1: Distribution of Countries of Origin of autonomous weapons systems (adapted from SIPRI Dataset on autonomy in weapons)

Key Takeaways- (Autonomous Weapons Systems)

**AWS**
- These are weapons that operate with high levels of autonomy to move, target, survey, and engage objects with little or no human intervention.
- AWS cut across UAVs, Maritime AVs, and AGVs.

**Uses for Security**
- Premise/asset security (defence).
- Detection and disposal of explosives.
- Firearm response.
- Surveillance.
- Used in all environments.

**Uses for other sectors**
National defence, surveillance, engaging enemies, logistics, refuelling, blood transportation etc.

**Future Uses**
- AWS are expected to increase speed and accuracy in engaging targets and to decrease human costs for the user.
- However, AWS are expected to reduce the threshold of war and the rates of proliferation are likely to be high.

© Ishmael Bhila
CLASSIFICATION AND LEVELS OF AUTONOMY

The levels of autonomy in cars have largely been standardized by SAE International, formerly the Society of Automobile Engineers, and are summarized in Figure 2.2. Its classification has been used or adapted by the IEEE, US NHTSA, the EU, and others. SAE has been developing its “Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles” for over a decade. Over four iterations of the taxonomy, SAE International has been clarifying concepts, updating definitions, and providing a robust framework with the aim of being “useful across disciplines, including engineering, law, media, and public discourse.” In addition, this example has the potential to be adapted and adopted across multiple AV domains beyond automobiles.95

Classification of road-going or any other type of AV can have important legal and ethical ramifications. In 2022, the European Union Technical Committee on Motor Vehicles approved regulations for the sale and use of AVs at Level 3 and higher.96 It uses the phrase “automated driving systems” throughout, rather than “autonomous

Figure 2.2: SAE levels of driving automation
vehicles. The US National Highway Traffic Safety Administration (NHTSA) uses the SAE taxonomy for autonomy levels for its reporting of accidents and incidents involving automobiles.

Many AVs are comparatively cheap, accessible, and modifiable to suit the needs of a wide range of potential users.

The NHTSA uses the SAE classifications to move towards standardization of accident reporting and data gathering from automobile manufacturers. For example, it refers to automated driving systems (ADS), which are classified as SAE levels 3 through 5. These are still at various stages of development, whereas Level 2 advanced driver assistance (Level 2 ADAS) assists a driver during normal driving operations when the system is engaged but still requires a human to do the driving at all times. In both instances, the NHTSA requires manufacturers to gather data and report accidents which occur within 30 seconds if a vehicle was equipped with either ADS or Level 2 ADAS. In the case of ADS, a crash must be reported if it results in “property damage or injury.” In the case of Level 2 ADAS, a crash must be reported if it “involved a vulnerable road user or resulted in a fatality, a vehicle tow-away, an airbag deployment, or any individual being transported to a hospital for medical treatment.”

The United States and the European Union combined provide the largest joint market for AVs in the world, and, in terms of classification of AVs, it is pragmatic for manufacturers and end users to use the same SAE levels of driving automation.

Figure 2.3: Levels of autonomy in weapons (adapted by Ishmael Bhila from Warren 2023)
adopted by both. However, in the security and military domains, these levels are usually contested as they also determine the interpretation of international law and other related existing regulations. The idea of “meaningful human control” has dominated discussions in military, academic, and nongovernmental organizations. It has been a key strand of debate around autonomous weapons systems at the United Nations Convention on Certain Conventional Weapons (CCW) discussions in Geneva and is largely contested. Warren classified the levels of autonomy, according to the current global discourse, into three categories: human in the loop, human supervised, and fully autonomous systems.101

SUMMARY

The development and manufacture of autonomous vehicles are expanding rapidly for aerial, ground, and maritime use. Many AVs are comparatively cheap, accessible, and modifiable to suit the needs of a wide range of potential users. Autonomy, which in itself is a spectrum rather than a rigid class of systems, brings with it various opportunities for different categories of AVs. These potential benefits are still being realized and more potential advantages will be identified as AVs become more secure and efficient.
CHAPTER 3: THREATS AND RISKS POSED BY AUTONOMOUS VEHICLES

INTRODUCTION

While the positive impacts and potential opportunities for AVs are numerous, their production and use, particularly at these early stages of their evolution, present various challenges, including the safety and security of AV systems, unlawful uses, hardware and performance issues, the explainability of the AI that powers autonomy, ethical concerns, and public mistrust. The sections to follow look at these in turn.

THREATS TO AUTONOMOUS VEHICLES

Key threats to the safety and security of AVs relate to their safe operation and their cybersecurity, since they are based on a combination of digital technologies, sensory techniques, and AI platforms. The primary focus of the regulation of civilian AVs, explored in chapter four, is safety, and the proliferation of AVs requires robust safety and quality standards. Kobaszyńska-Twardowska, et al., identify six sources of potential hazards to a UAV operation, which are equally applicable to other types of AVs. These are:

• Human error (due to such factors as poor communication among the operating team, insufficient training of personnel, fatigue, or pressure from a supervisor to deploy in inappropriate conditions)

• Failure to comply with procedures

• Failure of the vehicle or system

• The appearance of another vehicle on a collision course

• Rapid deterioration in weather conditions

• Deterioration in the performance of systems used in steering or navigation, such as GPS

Cybersecurity of AVs is also a significant concern, since they communicate through wireless channels that are not secure by default. These platforms are liable to cyberattack by actors who intend to disrupt, damage, or tamper with AVs. Threat actors, which range from individual, autonomous attackers to organized groups operating as part of a criminal enterprise or on behalf of a nation state, all work towards the infiltration, destabilization, and attack of computer systems on which AVs operate.

Cybersecurity of AVs is also a significant concern, since they communicate through wireless channels that are not secure by default.

Cyberattacks come in the form of malware attacks, jamming, unauthorized access, spoofing, data breaches, denial of service, and phishing, inter alia. Attack entry points can be via radio channel, message, or on-board system. Cyberattacks represent financial costs in the case of loss of control of systems and pose serious security threats in the event of the weaponization, accidental harm, or incompetent use of lost systems.
While some AVs are designed to operate independently of GPS and Internet connectivity, others remain susceptible to cyberattack because of that connectivity, automation, and the knowledge gaps that exist in the nature and number of vulnerabilities in autonomous systems.\textsuperscript{113} Civil GPS signals do not typically have the level of secure encryption employed in military GPS signals, hence they can be spoofed and counterfeited.\textsuperscript{114, 115} However, it is not feasible to find geographical, functional, or any other uses of AVs that simply avoid security threats.

### THREATS FROM AUTONOMOUS VEHICLES

Autonomous vehicles have recently become widely accessible and commercialized. This accessibility makes it possible for individuals and non-state groups to use them illegally. In the absence of any global, legally binding standards and regulations on the development and use of AVs, there is a likelihood that criminals, terrorists, and other malicious actors will gain access to these technologies and use them for malevolent purposes.

**In the absence of any global, legally binding standards and regulations on the development and use of AVs, there is a likelihood that criminals, terrorists, and other malicious actors will gain access to these technologies and use them for malevolent purposes.**

The threat presented by UAVs is described by the U.S. government as the reasonable belief that the activity of an unmanned aircraft or unmanned aircraft system may, if unabated:

1. Cause physical harm to a person
2. Damage property, assets, facilities, or systems
3. Interfere with the mission of a covered facility or asset, including its movement, security, or protection
4. Facilitate or constitute unlawful activity
5. Interfere with the preparation or execution of an authorized government activity, including the authorized movement of persons
6. Result in unauthorized surveillance or reconnaissance
7. Result in unauthorized access to, or disclosure of, classified, sensitive, or otherwise lawfully protected information\textsuperscript{116}

A classification by Jackman and Hooper\textsuperscript{117} divides the threats into four categories:

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Image and video capture (of critical or sensitive infrastructure, commercial sites or activities, or emergency service operations; for reconnaissance; to invade privacy; or as a means of abuse or stalking of individuals, e.g., ex-partners)</td>
</tr>
<tr>
<td>2.</td>
<td>Transport and carrying (of weaponry or contraband)</td>
</tr>
<tr>
<td>3.</td>
<td>Data collection (for cyberattacks or corporate espionage)</td>
</tr>
<tr>
<td>4.</td>
<td>Disruption (of sites, events, and activities, such as airports, political events, sporting events, and emergency service operations)</td>
</tr>
</tbody>
</table>

Many UAS incidents are caused by “careless or reckless”\textsuperscript{118} operators, while malicious uses include hostile surveillance, smuggling or
contraband delivery, disruption of business, and weaponization.119

The burgeoning popularity of drones is a particular challenge for the aviation industry. The U.S. Federal Aviation Administration (FAA) receives over 100 reports per month of UAV sightings from pilots, law enforcement personnel, or citizens concerned about the threat of potential collisions or other risks to civil aviation.120 Some incidents have proven to be extremely costly. At the Dubai International Airport in 2015, a recreational drone interference brought air traffic to a standstill and cost the United Arab Emirates' economy over USD 55 million.121

Bad actors with reasonable technical awareness have the capacity to manipulate multipurpose drones to execute attacks using simple methods, such as through smartphones.122 The Islamic State launched Trojan Horse weaponized drones against Kurdish fighters and French troops in 2016, and carried out further drone attacks in Syria against U.S. soldiers in 2017.123 Reports indicate the Islamic States has employed intelligence gathering drones for years, and experts fear it has developed the capability to disperse chemical weapons.124 By 2017, Hamas and Hezbollah had already used small armed drones with varying levels of autonomy,125 as had the Houthi terrorist group in Yemen,126 which stepped up its drone and missile strikes within Yemen and into Saudi Arabia in 2019.127 The use of small, off-the-shelf commercial drones is now a significant dimension of warfighting in Yemen, Ukraine, and Israel and Gaza. The low-cost vehicles are used for reconnaissance, situational awareness, and the deployment of small explosives or grenades. In evidence given to a UK Parliamentary inquiry on the Domestic Threat of Drones in 2019, Rogers argued that the technical proficiency for weaponizing civilian drones is not as specialized as might be expected, making it easy for terrorists to adapt these technologies for their own purposes.128

Such capability building by terrorist groups has increased the potential threat to national infrastructure and other buildings and objects.129 Small UAVs can be fast, agile, and difficult to identify and track, and harder still to forcefully remove from the sky. Notable drone attacks on critical infrastructure, each attributed to Houthi terrorists, including the following:

- A swarm attack of 25 drones and missiles130 on Saudi Aramco oil processing facilities at Abqaiq and Khurais in Saudi Arabia disrupted production by around 5 million barrels per day, equivalent to 5 percent of global production (2019).131
- Attacks on oil tankers near Abu Dhabi International Airport killed three people and injured six others (2022).132
- Multiple attacks on commercial shipping vessels in the Red Sea disrupting one of the world’s most important trade routes.133

A report by Deloitte discusses the plausible risk scenarios presented by UASs to critical infrastructure and assets from both malicious and unintentional actors, and these are summarized in Table 3.1.134 Most scenarios relate to malicious actors only, with the exception of flight operations interference, infrastructure damage, and facility trespassing. The report points out that access control measures are typically designed to detect and prevent unauthorized ground- and cyber-based access, while almost none are designed to prevent unauthorized aerial-based access.
The diverse uses of UAVs for criminal, terrorist and antisocial activities have given rise to the need for effective counter UAV technology. The autonomous systems likely to be developed by these less scrupulous actors will likely not live up to security, safety, and international legal standards. The threats are so serious that in 2022 the U.S. government published its Domestic Counter-Unmanned Aircraft Systems National Action Plan. The plan addresses UAV-related challenges that all countries face, including detection and mitigation capabilities, physical defensive systems, training, legal frameworks, incident tracking, and international cooperation, while also attempting to balance rights, privacy, the spectrum of communication frequencies, and nondisruption of commercial activities.

Unfortunately, the challenges of counter-UAV, or counter-drone, technology are significant. Israel and Ukraine, for example, have both kinetic counter-UAV systems, which fire bullets or missiles to destroy drones, and nonkinetic systems, which rely on electronic disruption of control signals. Kinetic systems can work effectively against military grade, aircraft-sized drones, but are ineffective against small, maneuverable, off-the-shelf hobby drones that have been modified to carry, say, a grenade or a small amount of explosive. Such weaponized systems would pose a danger to the public outside of battle zones. Signal-disrupting signals can be effective, but not against a small drone that has been programmed with instructions that enable it to function in a highly automated way. If such a drone was programmed with a specific, disruptive flight plan over an international airport, there would be no signal to disrupt and the use of kinetic weapons to shoot it down would endanger lives. Effective systems to counter-small drone threats are not keeping up with advances in drone technology.

<table>
<thead>
<tr>
<th>SECTORS MOST LIABLE TO BE AFFECTED</th>
<th>MILITARY</th>
<th>GOVERNMENT</th>
<th>LAW ENFORCEMENT</th>
<th>HEALTHCARE</th>
<th>ENERGY &amp; OIL/GAS</th>
<th>MANUFACTURING</th>
<th>TELECOM</th>
<th>TRANSPORTATION</th>
<th>OTHER BUSINESSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flight operations interference</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Infrastructure damage</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Facility trespassing</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Information gathering</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Illicit materials smuggling</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Explosives insertion</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Chemical biological insertion</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Personnel assassination</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Table 3.1: UAS risk scenarios
HARDWARE AND PERFORMANCE

The performance of AVs in practice is a key challenge. Much of the engineering and computer science literature researched was intended to fix technical problems. Technical challenges related to the “size, endurance, speed, recoverability, survivability, altitude, or depth range” and “communication, intelligence, and situational awareness” problems have been identified in the development and use of AVs.139

One high-profile system malfunction is the 2016 Tesla autopilot failure. The Tesla Model S’s autopilot failed to apply the autonomous emergency brake system, although “human error” was blamed for the driver’s failure to override the autopilot.140 With the proliferation of AVs and technological advancement, the probability of machine or technical errors also grows.141 Although AVs, particularly road vehicles, are meant to reduce accidents, there is no guarantee that they will achieve this as their use comes with social and behavioral changes in both the users and pedestrians. The complex real-life scenarios within which these systems are used also make it hard to verify the performance standards.142

BLACK-BOX CHALLENGES AND EXPLAINABILITY

Systems that rely on AI and machine learning do so through black-box algorithms. A black box is a system whose inputs and outputs are known but whose functional process is unexplainable.143 It is, however, hard to explain how an AI system works and why it makes the decisions it does in a way that can be easily understood by humans.144 AI’s decision-making processes are not always clear and can be difficult to interpret. This leads to a lack of transparency, which, in turn, can make it difficult to debug and improve a system. In addition, the reliability and trustworthiness of the AI can therefore be called into question, leading to the need for explainable artificial intelligence (XAI).145 To establish and improve decision-making in human-machine collaboration and teaming, the AI elements need to be understood and explainable.146 The black box dilemma follows that algorithms are opaque, making it difficult for humans to understand how the algorithms make their decisions, and in turn raising ethical questions on whether autonomous systems would act in good faith and within the remit of ethical and legal regulations.147 There are indications that scientists are beginning to overcome this challenge but it is likely to persist in the medium term.148

In the military field, explainable AI systems are very problematic. Developers make their systems with high levels of secrecy, enabling unpredictability and deception which give the owner of a system a strategic and tactical advantage.149 Christie, et al., argued that, if a system becomes explainable, transparent, and predictable, it loses its effectiveness as a weapon against an adversary.150 This makes most military developments of AVs problematic because the black box is deliberately maintained to ensure military advantage if it falls into the hands of an adversary.

The problem of explainability in AVs gets more complicated when and if a system can evolve using machine learning. China’s 2022 working paper submitted to the Group of Governmental Experts on Lethal Autonomous Weapons Systems (GGE on LAWS) recommended that systems with the capability to evolve on interaction with an environment, and which can learn new things without human input, should be prohibited.151 If a system can develop new characteristics after deployment beyond what the developer and user know about its internal functionality, then it presents high risks and becomes ethically questionable.152 However, the GGE on LAWS—the UN talks in Geneva—has not adopted that recommendation.
AUTONOMY LEVELS, SYSTEM FUNCTION, AND DEGREES OF RISK

When different levels of autonomy are combined with increasingly complex system functions, the risk involved can shift significantly. The two columns on the left of Table 3.2 illustrate the levels of autonomy for civilian autonomous systems based on the SAE autonomy levels. Column 3 shows levels of autonomy using the terminology of “human in the loop” for autonomous weapon systems commonly used to describe autonomy in military systems. Underneath columns 4 through 8 are descriptions of AI functions, from routine to high risk. The color-coded risk matrix is derived from the combination of levels of autonomy and the functions for which AI-enabled systems will be used. This applies to both civilian security applications and military applications.

<table>
<thead>
<tr>
<th>Autonomy Level</th>
<th>SAE Definition (Civilian)</th>
<th>Military Applications</th>
<th>AI system functions and degrees of autonomy</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No Driving Automation</td>
<td>Human in loop.</td>
<td>No risk from system</td>
</tr>
<tr>
<td>1</td>
<td>Driver Assistance</td>
<td></td>
<td>Low</td>
</tr>
<tr>
<td>2</td>
<td>Partial Driving Automation</td>
<td></td>
<td>Moderate</td>
</tr>
<tr>
<td>3</td>
<td>Conditional Driving Automation</td>
<td>Human on loop.</td>
<td>Medium</td>
</tr>
<tr>
<td>4</td>
<td>High Driving Automation</td>
<td>Human out of loop.</td>
<td>High</td>
</tr>
<tr>
<td>5</td>
<td>Full Driving Automation</td>
<td></td>
<td>Extreme, Extreme, Critical</td>
</tr>
</tbody>
</table>

Routine Administrative tasks. System AI-informed routine decisions. AI-based complex decision support to human operators in benign environments. Autonomous system uses AI-based decision-making in high risk environments with human input available. Autonomous system uses AI-based decision-making in high risk environments and lethal environments with no human input available.

Table 3.2: Risk matrix: autonomous vehicles and autonomous weapons systems
The most controversial use of autonomy in systems will be the intentional taking of human life by an autonomous weapon system using AI-based decision making with no human input. There are currently no fully autonomous self-learning weapon systems operated by major powers that are capable of nuanced judgments on when to use lethal force. The risk only manifests if a state is willing to use fully autonomous weapons without any ethical constraint. In civilian applications, high levels of autonomy are available in cars already, but the risks increase in line with those autonomy levels.

**ETHICAL CHALLENGES**

With developments in AI moving at an unprecedented pace, emerging technologies in the form of AVs have brought with them new ethical challenges, including privacy considerations. For example, if autonomous systems include video surveillance or facial recognition, the right to privacy of private citizens may be violated if they are used in public places. This could be further compounded if the AI which powers the autonomous system is not sufficiently explainable to provide reasons why the violation of privacy occurred.

Small drones are proving to be particularly problematic with regard to privacy, security, and safety, and legislation is not keeping pace with technological advances. In the United States, citizens with a small drone with a first-person, live view video camera can carry out counter-police or counter-security surveillance. If police drones are observing rioters, for example, a well-coordinated group could similarly use small drones to observe police movements. Drones can also be used to spy on neighbors, observe children in schoolyards, or track the movements of rival gangs. While the law requires them to be flown in line-of-sight of the operator, criminals will not be deterred by that regulation. Plus, small drones are so cheap they can be considered disposable.

Military use of drones highlights some challenges and ethical issues that civilian security may eventually have to face. Most significantly, this includes the ways in which they can be adapted for the deliberate taking of human life. This leads to concerns about digital dehumanization and questions about the ethics of ascribing the responsibility to make lethal decisions to machines. For them to be able to comply with International Humanitarian Law (IHL), AV systems should be able to understand and apply the key principles of IHL: proportionality, distinction (between combatants and civilians), necessity, unnecessary suffering, and identification of hors de combat. It remains a question of ongoing international debate whether autonomous weapons systems can or will be able to satisfy these criteria and comply with IHL.

The attribution of ethical and legal responsibility when it comes to the use of autonomous weapon systems presents challenges. The greatest concern arises if an autonomous system were to attack civilians and a human operator failed to stop it. Bo argues that criminal responsibility for “commission by omission” in international law should be interpreted to apply to such usage of autonomous weapons, with the principle of “meaningful human control,” or human in the loop, being key to this understanding. The introduction of autonomous weapon systems into military arsenals raises new ethical questions that challenge historical norms of ethical responsibility.

The Canberra Working Group demonstrates the ethical implications for military command structures when introducing and deploying autonomous weapon systems. They compare the authorization and sign out process for three types of aircraft: a conventional bomber, a remotely piloted aircraft (drone) with bomb-
ing capability, and an autonomous aircraft (drone) with bombing capability. The drones referred to here are aircraft-sized with a wing-span over 20 meters and able to carry over 1,000 pounds of bombs and missiles.

Table 3.3 sets these command structures side-by-side for comparison.

<table>
<thead>
<tr>
<th>Conventional military bomber aircraft preflight checks, authorizations, and sign-out</th>
<th>Military RPA preflight checks, authorizations, and sign-out</th>
<th>Military autonomous aircraft pre-flight checks, authorizations, and sign-out</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>System</strong></td>
<td><strong>System</strong></td>
<td><strong>System</strong></td>
</tr>
<tr>
<td>• Engine serviceability and service record</td>
<td>• Engine serviceability and service record</td>
<td>• Engine serviceability and service record</td>
</tr>
<tr>
<td>• Fuel Status</td>
<td>• Fuel status</td>
<td>• Fuel status</td>
</tr>
<tr>
<td>• Airframe serviceability</td>
<td>• Airframe serviceability</td>
<td>• Airframe serviceability</td>
</tr>
<tr>
<td>• Avionics</td>
<td>• Avionics</td>
<td>• Avionics</td>
</tr>
<tr>
<td>• Sensor systems (including cameras)</td>
<td>• Sensor systems (including cameras)</td>
<td>• Sensor systems (including cameras)</td>
</tr>
<tr>
<td>• Communications systems</td>
<td>• Communications systems</td>
<td>• Communications systems</td>
</tr>
<tr>
<td>• Control systems</td>
<td>• Control systems</td>
<td>• Control systems</td>
</tr>
<tr>
<td>• Navigation systems</td>
<td>• Navigation systems</td>
<td>• Navigation systems</td>
</tr>
<tr>
<td>• IT updates confirmed</td>
<td>• IT updates confirmed</td>
<td>• IT updates confirmed</td>
</tr>
<tr>
<td><strong>Mission</strong></td>
<td><strong>Mission</strong></td>
<td><strong>Mission</strong></td>
</tr>
<tr>
<td>• Weapon payload</td>
<td>• Weapon payload</td>
<td>• Weapon payload</td>
</tr>
<tr>
<td>• Meteorology report for operational area</td>
<td>• Meteorology report for operational area</td>
<td>• Meteorology report for operational area</td>
</tr>
<tr>
<td>• Operations intelligence update</td>
<td>• Operations intelligence update</td>
<td>• Operations intelligence update</td>
</tr>
<tr>
<td>• Aircraft tasking (ISR/weapon strike)</td>
<td>• Aircraft tasking (ISR/weapon strike)</td>
<td>• Aircraft tasking (ISR/weapon strike)</td>
</tr>
<tr>
<td>• Special instructions (warnings about other aircraft activities in the area)</td>
<td>• Special instructions (warnings about other aircraft activities in the area)</td>
<td>• Special instructions (warnings about other aircraft activities in the area)</td>
</tr>
<tr>
<td>• Aircraft “signed out” to the captain (pilot) by the authorizing officer</td>
<td>• Aircraft “signed out” to the captain (pilot) by the authorizing officer</td>
<td>• Aircraft “signed out” to the captain (pilot) by the authorizing officer</td>
</tr>
<tr>
<td>• Crew walks to the aircraft</td>
<td>• Crew walks to the ground control station</td>
<td>• Operation parameters programmed into operating system, incorporating engagement criteria</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Aircraft “signed out” to the captain (pilot) by the authorizing officer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Crew walks to the ground control station</td>
</tr>
</tbody>
</table>

Table 3.3: Authorization and sign out process for conventional, remotely piloted and autonomous bomber aircraft
Each hierarchy is ethically, legally, and operationally responsible for decision making. In the case of an autonomous, weaponized drone, there is no human to make the final decision to deploy lethal force. In that case, ethical responsibility does not simply disappear. Even an autonomous weaponized drone will not be able to operate independently of a large human infrastructure. Political leaders will decide if they are to be deployed and under what rules of engagement (that is, when lethal force can be deployed); commanders will decide on operational matters; legal advisors will still be needed; and coders will need to write programs and update systems. Engineers will still need to maintain the airframes (the body of the aircraft), engines, controls, radar, and other sensing equipment. Armorers will still fit weapons, others will refill the fuel tanks, and so on.

In the case of an autonomous, weaponized drone, there is no human to make the final decision to deploy lethal force. In that case, ethical responsibility does not simply disappear.

Moving to a civilian domain, if an AV, rather than a weapon system, is fully autonomous, the ascription of criminal responsibility in the event of a breach of international law or the laws of humanity becomes highly elusive. Weigend suggests that, because of this “responsibility gap,” new obligations that are specific to autonomous weapons systems (and AVs by extension) should be put in place to address these problems. Practitioners should be aware that specific international norms for AVs are not yet in place. Until then, military doctrine and regulations regarding AVs, and civil liability cases in the automobile sector, can provide insights to inform decision making in other sectors.

In autonomous road vehicles, the problem of liability in case of an accident has been raised in several cases. For example, in San Francisco in 2023, a Cruise driverless car drove over—and stopped on top of—a woman who had just been knocked over by a human hit-and-run driver. Analysis of cases like this will help users understand where system vulnerabilities and responsibilities lie.

PUBLIC PERCEPTIONS

Around the world, public perceptions of the trustworthiness of AVs and autonomous systems overall will significantly influence government decision making on the licensing of new systems and industry uptake of the technology. Research on public perceptions has focused in particular on the use of drones and autonomous passenger vehicles.

There have been numerous studies examining public opinion on drone technologies, one of the most recent at the time of writing being a systematic review of 30 studies undertaken in 15 countries. The review identified “socio-cultural aspects,” the main perceived risks, and the main expected benefits as being the main influences on public opinion, the former encompassing personal factors such as geographic location, technological expertise, and familiarity with drone-related terminology. The main perceived risks identified included drone misuse, privacy disrespect, malfunction, damage, safety, noise, and legal liability, while the main expected benefits included flexibility of application, emergency response and monitoring, cost reduction, and safety.

A systematic review of 158 research articles from around the world on applications, impacts, and public perceptions of autonomous vehicles in road transportation systems suggested that public perceptions about autonomous vehicles differ markedly between countries. Key determi-
nants of public opinion towards AV technologies were found to include gender, cost of AV technology, trust, legal liabilities, safety, control, consequences regarding the use of AV technology, loss of vehicle control, liability, and equipment failure. The study concluded that AV incorporation into public transportation is dependent on public perception and acceptability, and that public attitudes and how they vary by demographic and geographic group must be better understood, to inform public education and outreach programs to boost AV acceptability.

SUMMARY

Threats or potential threats from AVs come in many forms. The cyber element alone poses multiple threats: damage can render a system unusable, hacking could result in control of an AV being taken over by criminals or terrorists, while spoofing—confusing the system—could have similarly disastrous consequences. Hardware failures will have similar consequences to failures in other nonautonomous fields.

New ethical challenges will continue to emerge as autonomy develops in sophistication and application, from the explainability of the AI that powers autonomy, to the way individuals and their rights are affected. Public perceptions of the trustworthiness of AVs and autonomous systems overall will have significant impact on whether governments will take social and economic risks to license new systems. Manufacturers and developers will also need to make careful risk calculations about systems that may be less predictable than their analog forebears. It is no surprise that the regulatory environment faced by manufacturers and users of autonomous vehicles, the focus of the next chapter, is rapidly evolving.
CHAPTER 4: REGULATORY ENVIRONMENT

INTRODUCTION

The existence of AVs in different domains (sea, land, and air) has led to disparate attempts to regulate them. While international regulations concerning AVs are still hugely dependent on archaic civil aviation and transportation legal standards, efforts have been made to update laws relating to the various systems that are being developed. Faced by the significant opportunities as well as the risks presented by AI systems and the autonomous systems supported by AI, the global community is now engaged not only in a race to AI but also a race to AI regulation. In the case of AV regulation, the challenge is balancing the enablement of technological innovation while considering safety, privacy, security, and environmental concerns.

Efforts to regulate AI in its application to AVs have been disparate and fragmented. Büthe and colleagues have characterized efforts to govern AI as an exercise similar to “herding cats,” especially if policy makers focus on the nature of technologies instead of the risks and opportunities presented by AI. AVs and AI in general are evolving at a very fast pace, so the developments in the regulatory landscape have reflected this. The purpose of this chapter is to show what has been done so far in order to provide a platform from which future developments can be understood.

While international regulations concerning AVs are still hugely dependent on archaic civil aviation and transportation legal standards, efforts have been made to update laws relating to the various systems that are being developed.

Calls for a more coordinated global governance framework for AI have been growing. The United Nations Secretary General, together with the Secretary-General’s Envoy on Technology, called for the establishment of a High-Level Advisory Body on Artificial Intelligence to draft...
regulations for global AI governance. This began operating in October 2023, made up of 38 experts from different fields tasked with making recommendations on the international governance of AI, key risks and challenges, and key opportunities and enablers, to inform a proposed Digital Global Compact. Its interim report calls for the establishment of international norms that are more in step with the pace of AI in development and application, identifying five principles that should guide the formation of new global AI governance institutions: inclusivity; public interest; centrality of data governance; universal and multistakeholder buy-in through a networked approach; and anchoring in international law. It also sets out seven critical functions of AI governance, including horizon scanning for risks; harmonizing standards; safety and risk management frameworks; promoting international multistakeholder collaboration to empower the Global South; and developing binding accountability norms.

Despite some private companies' attempts to oppose and fend off regulation, others are "engaging and pushing, and leading and inspiring" in the development of ethical standards for AI.

The European Union proposed a risk-based policy framework for the regional governance of AI in Europe, an approach that has been supported by scholars in AI governance. Several intergovernmental organizations, including UNESCO and the Organization for Economic Cooperation and Development (OECD), have developed ethics-based frameworks for AI governance. UNESCO’s recommendations are centered on the principles of human rights, dignity, transparency, fairness, and the human in the loop principle that stipulates that a human should always have oversight over an AI system. So far, 193 UNESCO member states have adopted UNESCO’s AI ethics global standard. The OECD has put forward a set of AI principles based on values such as inclusion (and sustainable development), humanity and fairness, transparency and explainability, security and safety, and accountability, which is recognized by the 38 member states of the OECD and a further eight nonmember states. These and other lists of ethics principles have a direct bearing on AVs and autonomous weapon systems if AI is limited in its practical application.

In 2019, a comprehensive review by Jobin, Ienca, and Vayena mapped existing global AI ethics codes and listed 84 different sets of principles published by international organizations of different types. In addition to multilateral organizations, several thinktanks and other organizations have come up with frameworks and guidelines for AI governance. Also in 2019, the U.S. National Institute of Standards and Technology (NIST) put forward its Artificial Intelligence Risk Management Framework (AI RMF 1.0) to address risks, impacts, and harms posed by artificial intelligence. Firms and not-for-profit stakeholders are now finding incentives to develop codes of practice in AI-related areas such as autonomous vehicles, data privacy, software development, health, finance, and others.

Despite some private companies' attempts to oppose and fend off regulation, others are "engaging and pushing, and leading and inspiring" in the development of ethical standards for AI. Maas and
Villalobos\textsuperscript{182} classified existing institutional models for AI governance into the following categories: scientific consensus-building; political consensus-building and norm-setting; policy coordination and regulation; enforcement of standards or restrictions; stabilization and emergency response; international joint research; and distribution of benefits and access. There are at least 208 ongoing initiatives globally for the understanding and development of rules, laws, and directives on the regulation of emerging technologies in the field of AI.\textsuperscript{183}

Figure 4.1 shows the distribution of these initiatives.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{figure41.png}
\caption{Distribution of AI regulation initiatives. Graph adapted from OECD\textsuperscript{184}}
\end{figure}
Table 4.1 lists many of the key regulations globally that are relevant to AI.

<table>
<thead>
<tr>
<th>CATEGORY</th>
<th>AVAILABLE/POSSIBLE REGULATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>GENERAL AI</td>
<td>• 127 states have bills that refer to AI.</td>
</tr>
<tr>
<td></td>
<td>• OECD AI Principles (2019)</td>
</tr>
<tr>
<td></td>
<td>• UNESCO AI Ethics Recommendations (2021)</td>
</tr>
<tr>
<td></td>
<td>• UN High-Level Advisory Body on AI (2023)</td>
</tr>
<tr>
<td></td>
<td>• EU AI Act (2024)</td>
</tr>
<tr>
<td>UNCREWED AERIAL VEHICLES</td>
<td>• UN Resolution 2309 (2016)</td>
</tr>
<tr>
<td></td>
<td>• EU Regulation 2019/947</td>
</tr>
<tr>
<td></td>
<td>• UK Air Traffic Management and Unmanned Aircraft Act 2021</td>
</tr>
<tr>
<td>AUTONOMOUS GROUND VEHICLES</td>
<td>• Vienna Convention on Road Traffic (1968, 2016 amendment)</td>
</tr>
<tr>
<td></td>
<td>• SAE International Std J3016 (2021)</td>
</tr>
<tr>
<td>AUTONOMOUS MARITIME VEHICLES</td>
<td>• International Regulations for Preventing Collisions at Sea (COLREGs) (1972)</td>
</tr>
<tr>
<td></td>
<td>• International Convention for the Safety of Life at Sea (SOLAS) (1974)</td>
</tr>
<tr>
<td></td>
<td>• San Marenò Manual on International Law Applicable to Armed Conflicts at Sea (1994)</td>
</tr>
<tr>
<td></td>
<td>• International Humanitarian Law (IHL)</td>
</tr>
<tr>
<td>AUTONOMOUS WEAPONS SYSTEMS</td>
<td>• UN Convention on Certain Conventional Weapons (1980)</td>
</tr>
<tr>
<td></td>
<td>• UN Human Rights Council Resolution A/HRC/51/L.25 (2022)</td>
</tr>
<tr>
<td></td>
<td>• Belén Communiqué (2023)</td>
</tr>
<tr>
<td></td>
<td>• Caribbean Community (CARICOM) Declaration on Autonomous Weapons Systems (2023)</td>
</tr>
<tr>
<td></td>
<td>• UN Resolution on Lethal Autonomous Weapons Systems A/C.1/78/L.56 (2023)</td>
</tr>
<tr>
<td></td>
<td>• International Humanitarian Law (IHL)</td>
</tr>
</tbody>
</table>

Table 4.1: Regulations applicable to AI governance
UNCREWED AERIAL VEHICLE REGULATIONS

UAVs are subject to several regulatory obligations mainly related to risks and safety concerns. One industry commentator describes their regulation as moving through three phases, from the establishment of simple flight rules with exemptions, to supporting advanced applications of drones by industry stakeholders through simplified processes for authorizing exemptions, to the standardization of risk assessment and certification. Initial frameworks have focused on the user rather than the developer. These include the U.S. FAA Small Unmanned Aircraft Systems (UAS) Regulations (Part 107) (2016), and EU regulation 2019/947, in which systems in the “open” category cover the majority of leisure drone activities and low-risk commercial activities, which do not require any specific approvals. Open category systems have weight limitations (not over 25 kilograms) and height restrictions (not above 120 meters from the surface), and must operate within visual line of sight, be authorized by aviation authorities, have passed safety risk assessments for specified risks and limits, and be certified. The current EU regulatory regime anticipates that beginning in 2026 UAVs must demonstrate safety and security in design, not just deployment, for them to be used in the open category.

Using drones beyond these parameters includes extended visual line of sight (EVLOS) and beyond visual line of sight (BVLOS) operations, necessary for many industrial uses. The two other user categories are “specific,” requiring an authorization by the competent authority or a declaration by the UAS operator; and “certified,” requiring the certification of the UAS in accordance with Delegated Regulation (EU) 2019/945, the certification of the operator, and, where applicable, the licensing of the remote pilot.

AUTONOMOUS GROUND VEHICLE REGULATIONS

There are no global, legally binding regulatory frameworks specifically designed for AGVs. The minimum operating requirement is that they should follow traffic rules within the jurisdictions in which they operate. However, when it comes to ethical reasoning, the use of AGVs creates unique ethical dilemmas that should be addressed in legal and ethical frameworks, namely: decision-making in cases where loss of life is unavoidable and the attribution of responsibility, liability, and accountability in cases of failure. SAE International provides authoritative guidance for the engineering field, working in conjunction with the International Organization for Standardization (ISO) in the development of international standards.

The Institute of Electrical and Electronics Engineers (IEEE) have also developed several standards, most importantly IEEE Std 2846-2022: the IEEE Standard for Assumptions in Safety-Related Models for Automated Driving Systems (2022), to address the safety and behaviors of both machine systems and human road users. This standard recommends that for automated cars to be regarded as safe, the safety-related models on which they are based should be verifiable and demonstrable through inspection and validation, developed through a systematic process, compliant with acknowledged reference architecture, utilize mathematically rigorous methods, and be based on data-driven analysis, simulated testing, closed-course testing, and public road testing.

In international law, 2016 amendments to the Vienna Convention on Road Traffic of 1968 allow automated vehicles to drive legally on roads, as well as requiring that vehicle systems should be terminable or capable of being overridden by a human driver (Article 8, Paragraph 5). The
United States—the state of Nevada specifically—became the first jurisdiction in the world to develop legislation for autonomous cars, and in 2016 the U.S. NHTSA provided guidelines for the safe development of autonomous cars. These guidelines were adopted from standard J3016 put forward by SAE International.

**AUTONOMOUS MARITIME VEHICLE REGULATIONS**

AMVs do not have a dedicated regulatory framework. As with autonomous weapons systems, scholars and policy makers have so far attempted to situate the use of AMVs within existing international law. Some have attempted to bring the use of emerging disruptive technologies in the sea under the United Nations Convention on the Law of the Sea (UNCLOS) of 1982, yet this presents challenges. Most significantly, this is because when UNCLOS was developed, the main assumption about sea vessels was that they would be operated by human beings.

Several attempts have been made to interpret the use of AMVs using civilian and military regulatory frameworks. In addition to the UNCLOS, the International Humanitarian Law (IHL) and the San Remo Manual on International Law Applicable to Armed Conflicts at Sea (1994) have been used to make sense of the rules that can be used for AMVs. Others have called for the updating and amendment of other regulations like the International Regulations for Preventing Collisions at Sea (COLREGs) of 1972, as these do not apply to autonomous systems, including autonomous ships and underwater vehicles.

**AUTONOMOUS WEAPONS SYSTEMS REGULATIONS**

Autonomous weapons systems (AWS) can be in the form of any of the above-mentioned AVs, with the capability to be a weapon or used as a weapon delivery system. They can be defined loosely as weapons that can select, target, and engage a target without human intervention. The discussions on the regulation of AWS have been ongoing at the United Nations Convention on Certain Conventional Weapons (UNCCW) in Geneva through the Group of Governmental Experts on Lethal Autonomous Weapons Systems (GGE on LAWS) since at least 2013.

The discussions have been slow but have yielded Communities that are more likely to be negatively affected by disruptive technologies, particularly security applications of those technologies, are not part of the three dominant regulatory regimes, and are only encouraged to stand the avoidance of collisions at sea through algorithms. However, others have called for the updating of supplementary regulations like the International Regulations for Preventing Collisions at Sea (COLREGs) of 1972, as these do not apply to autonomous systems, including autonomous ships and underwater vehicles.

As a result of the vacuum in international law on AMVs, the International Maritime Organization is developing a regulatory framework for the use of Maritime Autonomous Surface Ships (MASS). Researchers have also situated the use of AMVs within the Convention on the International Regulations for Preventing Collisions at Sea (1972), arguing that the regulations can be used to understand the avoidance of collisions at sea through algorithms. However, others have called for the updating of supplementary regulations like the International Regulations for Preventing Collisions at Sea (COLREGs) of 1972, as these do not apply to autonomous systems, including autonomous ships and underwater vehicles.
learn from these regimes and simply harness technology. Several global milestones, starting with the Human Rights Council Resolution (A/HRC/51/L.25) tabled on 30 September 2022 by Austria, Costa Rica, Ecuador, Panama, Peru, and Uruguay. Regional agreements followed in the form of the Belén Communiqué, which was an outcome document for the February 2023 discussions among Latin American and Caribbean states on autonomous weapons systems. Caribbean states also adopted their own CARICOM Declaration on Autonomous Weapons Systems in September 2023. In October 2023, Austria and several other states tabled the UN Resolution on Autonomous Weapons Systems at the First Committee meetings, with the understanding that the UN Charter, international humanitarian law (IHL), and human rights law (HRL) all apply to autonomous weapons systems. Some 163 states voted in favor of the resolution, giving way to more directed efforts to regulate autonomous weapons systems.

REPRESENTATIONAL GAPS

Bradford argues in Digital Empires that the global digital order is structured according to interests and values based on three identifiable models: market-driven (U.S.), rights-based (EU), and state-driven (China). The U.S. model prioritizes the protection of national security through technological innovations, while at the same time allowing the market to be as innovative as possible with few government restrictions. By contrast, China’s model utilizes technology to control its citizenry, enhance surveillance, and fuel economic and industrial growth, while the EU model aims to harness technology to protect the human rights of digital citizens.

What is evident from Bradford’s analysis is that the Global South, which in practical terms includes the rest of the world, is barely represented, yet technologies like autonomous vehicles have been rolled out in most parts of the world and are being tested on populations with no say in how they will be regulated. During the Tigray War in Ethiopia (2020 to 2022), the leaders of the Tigray People’s Liberation Front (TPLF) claimed that they were being used as guinea pigs for testing new war technologies like autonomous drones. Communities that are more likely to be negatively affected by disruptive technologies, particularly security applications of those technologies, are not part of the three dominant regulatory regimes, and are only encouraged to learn from these regimes and simply harness technology. Africa and Latin America have only three countries apiece with adequate regulations for AI. With an autonomous weapons arms race ongoing, it is essential that all regions develop regulatory regimes that will safeguard them against excesses of AI development and use.

SUMMARY

Governments and international organizations are wrestling with how to regulate AVs in ways that will maximize social, economic, and military benefit while minimizing harm. Different approaches have emerged, with some focusing on technical aspects and capabilities, while other approaches concentrate on the risks and opportunities involved. However, guidance and regulations can best be described as patchy, rapidly developing, and not yet robust enough. Such efforts are yet to fully address the needs and risks presented by emerging technologies in the area of AVs or employ a holistic approach to regulation. A multisectoral and integrated regulatory framework is needed that governs the development and use of the five strands of AV technologies more comprehensively.
CHAPTER 5: IMPLICATIONS FOR THE SECURITY SECTOR

INTRODUCTION

This chapter discusses the practical implications of AVs for the security sector, showing how the findings from the previous chapters can be applied. AVs have tremendous potential in many industries and for various purposes. AVs have the potential to enhance security, but organizations deploying the technology must understand the requisite risks and threats. It is essential that, when considering the use of any technology, necessary analysis of its dangers is undertaken first, and guidelines and legal frameworks are put in place regardless of the advantages presented by the technology. We therefore provide an overview of what security practitioners can gain from using AVs, while also suggesting coordinated frameworks that will guide the use of those emerging technologies.

The technology industry’s increasing adoption of flexible consumption, or as-a-service business models should make such technologies even more cost-effective, facilitating their usage on a pay-per-use or pay-as-you-go basis.

Important innovations in the UAV market herald the arrival of what Bill Edwards, an industry expert and frequent media commentator on drone opportunities and challenges for the security sector, describes as “drone-as-a-security-service,” including the development of “drone-in-a-box” systems. These systems cover much greater areas than ground-based equipment and personnel, and provide an additional layer of security for patrol and quick reaction. He also noted the development of tethered drone systems, which have theoretically unlimited flight times.

Chapter 2 detailed numerous AV applications, which include a wide variety of current and potential applications in safety and security domains. These opportunities will only increase with the rapid development of emerging technologies, and security practitioners should be ready to harness them while mitigating risks and threats and complying with appropriate standards. Key safety and security applications include:

- Accessing remote and challenging terrains
- Acoustic sensors to detect loud noises
- Asset inspection
- Carriage and transportation of goods
- Data collection for security operations
- Detection and disposal of explosives
• Firearm response
• Identification and retrieval of lost assets
• Personnel transportation
• Risk assessment
• Search and rescue of personnel
• Securing infrastructure
• Securing personnel
• Security communications and information exchange
• Thermal imaging
• Video surveillance

AVs present opportunities for those considering the expansion of their business into new markets, and can be an essential addition to the security arsenal for those who operate in remote locations, since they can be used in virtually any environment, including under the sea, in the desert, in the mountains, or in the coldest places on the planet. Such resilience in the harshest of conditions is complemented by the ability of emerging AVs to operate without the need for connectivity. The potential benefits are still being realized and more potential advantages will be identified, including those based on human-machine collaboration and teaming to bring together the best of both, as AVs become more secure and more efficient.

MANAGING THE THREATS TO AUTONOMOUS VEHICLES

The management of safety and security threats to AVs needs to address both the operational and technical aspects. Management of safety risk should be embedded throughout the design, testing, demonstration, and deployment stages of AV development and operation. In the case of UAVs, they have arrived in a world in which strict regulations for aircraft already exist, and the need to adapt to a regulatory regime with a very low tolerance for risk is limiting their commercial deployment.\(^{217}\) Well developed regulatory regimes such as that of the U.S. FAA provide detailed guidance and resources for individual and organizational users.\(^{218}\)

Managing the cybersecurity threats to AVs involves ensuring the confidentiality, integrity, and authenticity of information handled by AVs, and the availability of services for which AVs are used. Weaknesses in the firmware, software, and wireless communication channels of AVs make them vulnerable to cyberattack. There is a considerable and fast-evolving body of literature on the cybersecurity of autonomous vehicles, including several systematic reviews,\(^{219}\)\(^{220}\)\(^{221}\)\(^{222}\) highlighting the key concerns that users need to consider and manufacturers must address.

A simple overview of the various countermeasures that may be deployed to protect drones from cyberattacks is provided by Kong, who divides these into the three categories of prevention, detection, and mitigation, as summarized in Table 5.1.\(^{223}\) Preventative countermeasures such as access control, information security measures, or the selection of components without exploitable vulnerabilities can stop a cyberattack from happening. If these fail, detection countermeasures provide warnings of the presence of an attack agent, which vary based on the type of attack (e.g. a strong interfering radio signal for channel jamming, or a malicious computer program for a virus attack), or of anomalies in areas like on-board resource usage pattern, radio signal, communication traffic, or flight movement. Mitigation countermeasures serve to limit the impact and damage of attacks, with Kong recommending five key methods:
Neutralizing the attacker by jamming the channel of a malicious eavesdropper

Avoiding the attack agent by switching to a different channel from the one being attacked, or changing the flight path of the UAV

Providing redundancy by installing multiple receivers, each for a different global navigation satellite system (GNSS), so that the targeted UAV can receive messages from another GNSS if one is jammed

Exploiting uncertainty by making a UAV’s behavior less predictable

Implementing a fail-safe protocol as a measure of last resort, by returning or forwarding the UAV to a safe state

Autonomous passenger vehicle countermeasures are even less technologically mature, since the vehicles themselves are far less so. Through a literature survey, Gupta, et al., provide a classification of attack countermeasures for autonomous passenger vehicles, based on the type of attack they protect against.

These are:

- Identity-based, using identity attributes such as AV ID-number, AV IP address, and AV registration number to protect a vehicular ad-hoc network (VANET), which provides connectivity between groups of vehicles
- Key-based, employing symmetric (single key) or asymmetric (public and private keys) to encrypt and decrypt communications
- Trust-based, relating to the degree of trust between AVs forming part of a VANET, as a result of previous communications, with each AV having a different degree of trust
- Misbehavior detection-based, using the trust value ascribed to an AV by roadside transportation infrastructure (RSI) (e.g., road sensors, radar, and other AVs) on the basis of past activity data
- Machine learning-based, which extend beyond previously collected information, and can learn and predict attacks according to attack patterns

The authors discuss the use of blockchain, a distributed database system that maintains all records or transactions relating to the AVs in linked lists of records (blocks) within an encrypted business network, as a means of enhancing such privacy and security measures. While acknowledging that blockchain-based AV systems are still in their infancy, they summarize the benefits

<table>
<thead>
<tr>
<th>Prevention</th>
<th>Detection</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Control access</td>
<td>- Presence of attack agent</td>
<td>- Neutralize attacker</td>
</tr>
<tr>
<td>- Protect information</td>
<td>- Presence of anomaly</td>
<td>- Avoid attack agent</td>
</tr>
<tr>
<td>- Select components without exploitable vulnerabilities</td>
<td>- Signal physical characteristic</td>
<td>- Provide redundancy</td>
</tr>
<tr>
<td></td>
<td>- Communication traffic</td>
<td>- Exploit uncertainty</td>
</tr>
<tr>
<td></td>
<td>- Flight behaviour</td>
<td>- Fail-safe protocol</td>
</tr>
<tr>
<td></td>
<td>- UAV environment</td>
<td></td>
</tr>
</tbody>
</table>

Figure 5.1 UAV countermeasures (source: Kong, 2021224)
Autonomous Vehicles: Threats, Risks, and Opportunities

they can bring as including immutability (the inability to modify stored records), traceability (recording all activities of all AVs in the block), reliability (with each node in the network having copies of the same data), and transparency (with each participant member having a copy of all unmodifiable data). The authors highlight key areas for future research to support the development of such solutions.

MANAGING THE THREATS FROM AUTONOMOUS VEHICLES

A more immediate concern for the larger proportion of security practitioners is, of course, the management of risks and threats presented by AVs. In chapter 3, Table 3.1 sets out the plausible risk scenarios by sector of UASs, according to a report by Deloitte, given that most access control measures address unauthorized ground- and cyber-based access and not aerial-based access. The risk matrix in Table 3.2 can be used as a tool to help security practitioners make a basic risk estimate, before that initial estimate is further refined according to the specific kind of AV and how it will be used. As a rough guide, when a system only provides assistance to human operators for routine activities, the risk level is low. In contrast, a combination of high levels of automation and lethal or potentially lethal activities carries extremely high risk.

As noted in the Deloitte report, the relatively low cost of UASs, their technological capabilities, and their ability to overcome aerial barriers with ease make them a distinct and pressing challenge to organizations. It therefore emphasizes the importance of comprehensive risk management frameworks that address both external and internal UAS risks. The report highlights key aspects of such frameworks in the assessment and management of UAS risk, much of which is pertinent to AVs in general. Dimensions of risk assessment include:

- Studying the risks, by keeping abreast of emerging technologies and the potential threats they present, determining the risk environment and the level of risk that the organization is willing to accept, identifying the potential risks, and evaluating overall risk by probability and severity of consequence
- Ecosystem mapping, recognizing stakeholders and relevant risks, identifying organizations’ responsibilities within the ecosystem, and determining points of collaboration with key stakeholders
- Risk management program maturity assessment, based on such activities as stakeholder interviews, round table discussions, and survey analysis to ascertain which solutions can be integrated into organizational business processes and existing risk management activities

Another useful guide for security practitioners by Edwards outlines the key requirements of a drone threat and vulnerability risk assessment for protecting critical infrastructure:

- Detailed threat analysis
- UAV and commercial drone capability review
- Identification of critical assets
- Vulnerabilities of those assets
- Risk mitigation recommendations and measures

The latter, he argues, require “layered zones of interest, a defense in depth mindset, mutual aid agreements and partnerships, and knowledge of applicable laws and regulations that support a comprehensive plan,” and “the ability to employ technology to detect, monitor, interdict, and even destroy.”
Edwards goes on to detail what he presents as the minimum parameters of a drone emergency response plan, all of which are explained in more detail in his journal article:

1. Identify the area you will defend

2. Form response teams and identify their functions and reporting procedures

3. Identify laws and regulations that limit the effect of the plan

4. Identify zones of interest and influence, and develop a listening and observation post array for deployment

5. Develop reporting standards and templates, such as the technological package to be deployed and operations center standard operating procedures

6. Formulate individual munitions, biohazard, and chemical response plans, and organize quick reaction forces, communications plans, and medical and HAZMAT (hazardous materials) response planning

7. Develop evacuation plans

8. Stock emergency supplies, such as water, food, and medical

9. Coordinate with local public support agencies and emergency services

10. Consider cyber implications and protect crucial data and information

11. Establish business continuity options and plans and form mutual aid agreements for support

In addition to these elements, the Deloitte report advocates war gaming and modelling, through simulated risk events and decision-making processes to test risk responses and crisis management plans, and stress testing of risk management plans.\(^{228}\)

It also emphasizes that because of the complexity of the risk environment, the extent of the opportunities and risks, and the pace of technological advancement, the responsibility falls upon multiple stakeholders to understand and mitigate risks and recognize the opportunities presented. Thus, it is stressed that industry, government, and academia need to come together in an integrated and collaborative effort.\(^{229}\) The wider literature on governing complexity offers recommendations on the necessary adaptations to organizational and professional practice. These include enhancing problem understanding through better modeling and analysis tools; drawing on big and open data; transparency to prevent information hoarding and increase stakeholder accountability; effective deliberative mechanisms that are collaborative and inclusive; adaptive policy responses that enable continuous learning; and adaptive system design that mitigates uncertainties, such as responding to unintended consequences, and rebalancing power differentials.\(^{230,\ 231}\)

**ETHICAL, LEGAL, AND REGULATORY CONSIDERATIONS**

It is evident that the practical and ethical challenges presented by AVs are highly complex and will continue for the foreseeable future. The degree of complexity, in turn, is influenced by the level of autonomy within a particular vehicle or system. This is happening across both civilian and military contexts, and extends to include autonomous weapon systems. Security professionals will need to keep fully abreast of developments in the legal and safety frameworks to which they must comply. This means taking the time and making the effort to remain up to date with necessary legislation.
and regulatory requirements in the jurisdictions where AVs and autonomous systems are designed and built, as well as where they may be used or sold. With regulations proliferating, this challenge will only grow.

The security sector could benefit from developing its own ethical and operational guidelines that would make the adoption and utilization of AVs safe, efficient, and acceptable. Organizations like ASIS International can play a key role in bringing stakeholder communities together and sharing expertise. Taking one of their more advanced current and future applications—the deployment of UAVs in smart cities—a systematic review of smart city applications for safety and security purposes identified privacy challenges, regulatory challenges, public acceptance issues, physical and cybersecurity vulnerabilities, and interoperability and standardization challenges.232

**SUMMARY**

The management of risks and threats presented by AVs are a pressing concern for security practitioners, especially as the technologies become more ubiquitous, with UASs being a key area of focus. This requires the recognition of such risks in organizational risk management frameworks, as well as a collaborative approach to security in recognition of the pace of technological advancement and the complexity of the risk environment. Security practitioners must also be cognizant of the security risks and threats to AVs being employed by their organizations or clients, as part of the growing cyber-physical organizational landscape. This requires an understanding of prevention, detection, and mitigation countermeasures, as well as an awareness of challenges on the horizon and key areas of future innovation. In contributing to the protection of such systems, such practitioners can also capitalize on the benefits of AVs that are transforming other sectors and incorporate them more actively in the security arsenal. Such technologies have never been cheaper or more accessible.
CHAPTER 6: CONCLUSION

Autonomous vehicles are proliferating rapidly for use in land, sea, and air environments. This has been transformative in many sectors and also had a dramatic impact on markets, user behavior, and attitudes towards the services provided. Unmanned aerial system (UAS) technologies are the most mature and can be applied most widely and cheaply, but there is now considerable investment taking place in autonomous ground vehicles (AGV) that can carry passengers and significant cargo. At the same time, autonomous weapons are continually being developed by countries with the expertise and infrastructure to support their development.

The AI upon which autonomous vehicles and systems will operate is under intense political, legal, and ethical scrutiny. Governments and international organizations are wrestling with how to regulate AVs in ways that will maximize social, economic, and military benefit while minimizing harm. However, guidance and regulations can best be described as patchy, rapidly developing, and not yet robust enough. In addition, new ethical and legal questions are emerging on a regular basis. The technical challenges are considerable and expensive. Liability costs for system error are likely to be huge, depending on the sector. An unavoidable reality is that no major government can afford to cede technical or economic ground to opponents in what will be a highly significant race for technology.

Users of autonomous vehicles and systems will need to focus on what autonomous vehicles they require and why, as well as adapt rapidly to new legal, ethical and practical challenges as they emerge. Security practitioners need to be able to support their organizations and clients in harnessing such technologies effectively, responsibly, and securely, with a grasp of the regulatory environment and public attitudes, both of which vary immensely across jurisdictions. They also must consider the security requirements of a widening cyber-physical organizational landscape and attack surface. Finally, they need to recognize AV risk to critical infrastructure and other assets from both malicious and unintentional actors, and ensure that adequate risk management frameworks are in place. Looking to the future, the following trends are anticipated:

- Security concerns will escalate as commercial AVs are increasingly adapted by criminal organizations and terrorist groups as lessons are learned from war zones like Ukraine and Gaza.

- The relatively low cost of sophisticated surveillance capabilities will challenge security, police, and military organizations.

- The interconnectedness of AVs in air, land, and sea surface and subsurface domains will further test security capabilities.

- Where commercial AVs rely on a live signal to operate, these will become increasingly vulnerable to hacking and spoofing.

- Where AVs incorporate higher and higher levels of autonomous capability, signal disruption becomes less of a threat, but the AI involved in such systems bring their own challenges to ensure consistency, safety, and reliability.

As security practitioners’ familiarity with AV technology grows, their potential to transform and improve security practice can also be realized, supporting such functions as surveillance, rescue missions, defense, firearms response, securing premises, communications; operating in remote areas or harsh conditions; and increasingly as a tool for public safety, security, and
law enforcement purposes in smart cities. The security community needs to anticipate and adapt to such changes, while at the same time being prepared to contribute to the harmonization of service provision in accordance with multisectoral needs, national and international guidelines and laws, and public perceptions of the use of emerging technologies. Organizations like ASIS International have a key role in bringing stakeholder communities together, sharing expertise, and driving best practice.
RECOMMENDED READING LIST

CHARACTERIZATION, CATEGORIZATION, & OPPORTUNITIES


RISKS & THREATS


REGULATIONS


Nathalie A Smuha, ‘From a “Race to AI” to a “Race to AI Regulation”: Regulatory Competition for Artificial Intelligence’ (2021) 13 Law, Innovation and Technology 57.
Anna Jackman and Louise Hooper, ‘Drone incidents and misuse: legal considerations’ (December 2023) University of Reading.

Matthijs Maas and Jose Jaime Villalobos, 'International AI Institutions: A Literature Review of Models, Examples, and Proposals' (Legal Priorities Project 2023)


MANAGING THE RISKS


Rico Merkert and James Bushell, ‘Managing the drone revolution: a systematic literature review into the current use of airborne drones and future strategic directions for their effective control’ (2020) Journal of Air Transport Management, 89.


RESEARCHER BIOGRAPHIES

ISHMAEL BHILA is a doctoral candidate in the School of Law at the University of Portsmouth, researching in/exclusion in the making of norms relating to autonomous weapons systems. Ishmael’s work looks at the interface of emerging technologies, power, and marginality. Ishmael has been involved in global advocacy on issues relating to disarmament and autonomy in weapons systems since 2022. His work includes engagement with and analysis of the discussions surrounding autonomous weapons systems in the Group of Governmental Experts on Lethal Autonomous Weapons Systems (GGE on LAWS). He is also currently involved in projects looking at (1) meaningful human control and accountability in security assistance in Africa, and (2) systems of cooperation in autonomous weapons systems discourse and their impact on vulnerable populations whose lives are seen as “lose-able,” “injurable” and “disposable.” Ishmael is undertaking these projects through Research Fellowships in the BMBF-competence network Meaningful Human Control – Autonomous Weapon Systems between Regulation and Reflexion (MEHUCO) project at Paderborn University and in the Collaborative Research Center (CRC) 1187 “Media of Cooperation” at the University of Siegen.

PROFESSOR ALISON WAKEFIELD is Co-Director of the Cybersecurity and Criminology Centre at the University of West London. She is an academic criminologist and security studies specialist with an international profile in both the academic and practitioner communities. Alison’s research interests are in all matters security, and her latest book Security and Crime: Converging Perspectives on a Complex World (Sage, 2021) examines security trends across multiple dimensions, including chapters on international, regional, national, local, individual, cyber, corporate, and maritime perspectives. Alison’s current research is focused on security convergence and managing complexity in security risk management. She holds a number of pro bono roles, including those of Senior Associate Fellow at the Royal United Services Institute, a London-based security and defense think tank; Commissioner on the UK’s National Preparedness Commission; Academic Advisor to the Chartered Security Professionals Registration Authority; Chair Emeritus of the Security Institute, having served as Chair from 2018 to 2020; Advisory Board member for Resilience First, the London Cyber Resilience Centre, and the International Security and International Cyber Expos; and Editorial Board member for several international journals including Security Journal. Alison has been an ASIS member since 2021.

PROFESSOR PETER LEE is a Professor of Applied Ethics and the Director, Security and Risk Research and Innovation at the University of Portsmouth. His research has spanned the politics and ethics of war, the ethical, operational, and other human aspects of UK Remotely Piloted Aircraft Systems (drone) operations, and the ethics of AI and autonomous weapon systems. In 2014 Peter was an expert ethics contributor to the first International Committee of the Red Cross Conference on “Autonomous Weapon Systems: Technical, Military, Legal and Humanitarian Aspects.” In 2015/2016, he was a member of the UK Department for Transport Oversight Committee for the public dialogue on “The Use and Development of Remotely Piloted Aircraft Systems and Small Drones in the United Kingdom,” which addressed issues including privacy, ethics and legality, flight safety, policing, and public education. From 2016-2018 he was granted unprecedented research access to the two RAF Reaper (drone) squadrons for his book, Reaper Force. In 2020 Peter led two research projects which explored legal, ethical, and moral perspectives on advanced technology and emerging weapon systems (DSTL-funded) and, separately, moral injury in police online child sex crime investigators and RAF Reaper (drone) operators (CREST-funded). In
April 2023 he commenced a collaborative EPSRC-funded project to create a Trustworthy Autonomous Robotic Drone System to Support Battlefield Casualty Triage. Peter has delivered 100+ keynotes/invited talks to academic, military, and humanitarian organizations in 10 countries and 4 continents, plus ongoing radio and TV engagements. He is a founding member of the UK Ministry of Defense Artificial Intelligence Ethics Advisory Panel and in 2022 contributed to the UK MOD's now-published AI Ethics Principles. He is an Expert Adviser of the All-Party Parliamentary Group on Drones and Modern Conflict.
END NOTES


⁴Civil Aviation Authority (UK) ‘CAP 2569: Call for Input- Review of UK UAS Regulation’ (CAA 2023).


⁹Ibid.


¹¹Jackman and Hooper (n 41).

13 Natasa Turak, ‘How Saudi Arabia Failed to Protect Itself from Drone and Missile Attacks Despite Billions Spent on Defense Systems’ (September 23 2019) CNBC.


17 Nathalie A Smuha, ‘From a “Race to AI” to a “Race to AI Regulation”: Regulatory Competition for Artificial Intelligence’ (2021) 13 Law, Innovation and Technology 57.


22 Faisal et al. (n 1)


24 ASIS uses gender-neutral language whenever possible and substitutes “uncrewed” for “unmanned.” When quoting directly from sources, the term used by the cited source is used.

EU Regulation 2019/945 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems.


Xiong and Xie (n 3).


ibid.


Civil Aviation Authority (UK) ‘CAP 2569: Call for Input- Review of UK UAS Regulation’ (CAA 2023).

Fard, Selmic and Khorasani (n 5).


Neshat Elhami Fard, Rastko R Selmic and Khashayar Khorasani, ‘Public Policy Challenges, Regu-

42Taylor, Sean Joe, Farhan Ahmad, Hoang Nga Nguyen, and Siraj Ahmed Shaikh. 2023. ‘Vehicular Plato-

43Parlov (n 4).

44Iva Parlov, ‘Can the International Regulatory Framework on Ships’ Routing, Ship Reporting, and 
Vessel Traffic Service (VTS) Accommodate Marine Autonomous Surface Ships (MASS)?: Exploring the 
Autonomy-Neutral Character of the Existing Regulations’ (2023) 54 Ocean Development & International 
Law 163.

45Shaopeng Zhong, Ao Liu, Yu Jiang, Simon Hu, Feng Xiao, Hai-Jun Huang, and Yan Song, ‘Energy and 
environmental impacts of shared autonomous vehicles under different pricing strategies’ (2023) npj 
Urban Sustainability 3(1): 8.


47Catherine T Lawson and Karthik Soundara Rajan, ‘Unmanned Aircraft Systems (UAS): Applications 
and Integration into Hazard Mitigation Planning’ (2023) Journal of Homeland Security and Emergency 
Management 20(3).


49See Syed Agha Hassnain Mohsan and others, ‘Unmanned Aerial Vehicles (UAVs): Practical Aspects, 
Applications, Open Challenges, Security Issues, and Future Trends’ (2023) 16 Intelligent Service Robotics 
109.

50Yousef Alghamdi; Arslan Munir; Hung Manh La, ‘Architecture, Classification, and Applications of Con-

51Yousef Alghamdi; Arslan Munir; Hung Manh La, ‘Architecture, Classification, and Applications of Con-

52Georgia Lykou, Dimitrios Moustakas, and Dimitris Gritzalis, ‘Defending Airports from UAS: A Survey on 

53Ashleigh Townsend, Immanuel N. Jiya, Christiaan Martinson, Dmitri Bessarabov, and Rupert Gouws, 
‘A Comprehensive Review of Energy Sources for Unmanned Aerial Vehicles, Their Shortfalls and Oppor-
tunities for Improvements’ (2020) Heliyon 6(11).

54Yavinaash Naidu Saravanakumar, Mohamed Thariq Hameed Sultan, Farah Syazwani Shahar, Wojciech 
Giernacki, Andrzej Łukaszewicz, Marek Nowakowski, Andriy Holovaty, and Sławomir Stepień, ‘Power 
Autonomous Vehicles: Threats, Risks, and Opportunities


62 Lawson and Rajan (n 11).

63 Anna Jackman and Louise Hooper, ‘Drone incidents and misuse: legal considerations’ (December 2023) University of Reading.

64 Elsayed and Mohamed (n 5).


74 Carol Flannagan, Andrew Leslie, Raymond Kiefer, Scott Bogard, Geoff Chi-Johnston, Laura Freeman, Rayman Huang, David Walsh, Antony Joseph, ‘Establishing a Crash Rate Benchmark Using Large-Scale Naturalistic Human Ridehail Data’ (2023) https://deepblue.lib.umich.edu/handle/2027.42/178179.

75 Marek Nowakowski and Jakub Kurylo, ‘Usability of Perception Sensors to Determine the Obstacles of Unmanned Ground Vehicles Operating in Off-Road Environments’ (2023) 13 Applied Sciences 4892.

76 Thakur and Mishra (n 20).


83 Vedachalam and others (n 1).


85 ibid.


91 The remainder of the report will refer to ‘autonomous weapons’ but this should be understood as shorthand for ‘autonomous weapon systems’.

92 ibid.


94 The data mentioned here and the graphic below were created from SIPRI's dataset on autonomy in weapons systems available publicly at https://docs.google.com/spreadsheets/d/1C9ewqFQ53ehRaEmGy-H9bl6xMsxFmhu/edit#gid=1786183935

95 J3016_202104: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - SAE International'.

96 EU, 'New EU Type Approval rules for automated vehicles Level 3 and beyond - Connected Automated Driving'.

97 The following includes information from the report 'The era of Highly and FULLY AUTOMATED DRIVERLESS VEHICLES is rapidly approaching' by J3016_202104: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - SAE International'.

98 EU, 'New EU Type Approval rules for automated vehicles Level 3 and beyond - Connected Automated Driving'.

99 The following includes information from the report 'The era of Highly and FULLY AUTOMATED DRIVERLESS VEHICLES is rapidly approaching' by J3016_202104: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles - SAE International'.


100 National Highway Traffic Safety Administration.


106 Ibid.


111 Kong (n 31)

112 Ibid.


114 Humphreys (n 5).

115 Todd Humphreys and others ‘Resilience and Validation of GNSS PNT Solutions’ (Center for Automated Vehicles Research with Multimodal Assured Navigation (CARMEN+) Tier-1 University Transportation Center, 2023).


117 Jackman and Hooper (n 41).

118 The terminology of the US Code of Federal Regulations, Title 14, Aeronautics and Space, section 91.13: Careless or reckless operation.


Autonomous Vehicles: Threats, Risks, and Opportunities

brary.un.org/record/1639536> accessed February 20 2024.


128Rogers (n 97).


130Natasha Turak, 'How Saudi Arabia Failed to Protect Itself from Drone and Missile Attacks Despite Billions Spent on Defense Systems' (September 23 2019) CNBC.


135Ibid.

136Altmann and Sauer (n 99).


146 ibid.


150 ibid.

Some researchers have questioned whether ascription of such qualities to AI systems are helpful considering that AI does not have human-like agency. See for example Arthur Holland Michel, ‘The Black Box, Unlocked: Predictability and Understandability in Military AI’ (2020) United Nations Institute for Disarmament Research <https://unidir.org/black-box-unlocked>, p.21.


Warren (n 8).

Hors de combat refers to individuals who are incapacitated/out of action due to injury. The question remains whether AVs that are fully autonomous can distinguish between combatants who are out of action and those who are not. The ICRC uses the Martens Clause of the 1899 Hague Convention to include the ‘Principle of Humanity’ as a fundamental principle in war, a general principle that protects ‘inhabitants and belligerents' according to the 'laws of humanity and the dictates of public conscience'. See https://casebook.icrc.org/a_to_z/glossary/martens-clause for more information on the Martens Clause.


Ibid.


Isaac Oyeyemi Olayode, Bo Du, Alessandro Severino, Tiziana Campisi, Frimpong Justice Alex, Systematic Literature Review on the Applications, Impacts, and Public Perceptions of Autonomous Vehicles in
164 Nathalie A Smuha, 'From a “Race to AI” to a “Race to AI Regulation”: Regulatory Competition for Artificial Intelligence' (2021) 13 Law, Innovation and Technology 57.


166 Tim Büthe and others, 'Governing AI – Attempting to Herd Cats? Introduction to the Special Issue on the Governance of Artificial Intelligence' (2022) 29 Journal of European Public Policy 1721.


171 Carlos I Gutierrez, ‘Multilateral Coordination for the Proactive Governance of Artificial Intelligence Systems’ [2023] SSRN.


174 Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts 2021 (2021/0106 (COD)).

175 Jonas Schuett, ‘Defining the Scope of AI Regulations’ (2023) 15 Law, Innovation and Technology 60.

22 August 2023.


180Carlos Ignacio Gutierrez, ‘Uncovering Incentives for Implementing AI Governance Programs: Evidence From the Field’ (2023) 4 IEEE Transactions on Artificial Intelligence 792.


184OECD data for this graph can be found at https://oecd.ai/en/dashboards/policy-instruments/Emerging_technology_regulation.


188Although regulations for certification are not yet available in Europe, the UK uses ‘aviation principles’ of licensing, airworthiness, and operations to determine whether a system is certified/certifiable or not.

190 Contissa, Lagioia and Sartor (n 19).


196 ibid.


200 See the outcome of the regulatory scoping exercise done in 2021 here and the information on the proposed MASS Code here.


203 Therese Tärnholm and Hans Liwång, ‘Military Autonomous Underwater Vehicles: An Implementation

Ibid.


Informal discussions were conducted from 2013 to 2016, when the Group of Governmental Experts was then formed through a mandate, with its first sitting taking place in 2017.


219 Rico Merkert and James Bushell, 'Managing the drone revolution: a systematic literature review into the current use of airborne drones and future strategic directions for their effective control' (2020) Journal of Air Transport Management, 89.


229 Ibid.

230 Tom Pegram and Julia Kreienkamp, ‘Governing Complexity: Design Principles for Improving the
