Autonomous Vehicles

THREATS, RISKS, AND OPPORTUNITIES

Researchers: Ishmael Bhila, Peter Lee, and Alison Wakefield

ASIS FOUNDATION™

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.[3] [4] 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.[5] '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.[6]

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.[7]

Cybersecurity of AVs is also a significant concern, since they communicate through wireless channels that are not secure by default.[8] These platforms are liable to cyberattack by actors who intend to disrupt, damage, or tamper with AVs.[9] 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.[10]

A classification by Jackman and Hooper[11] 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.[12] 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."[17] 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.

END NOTES

[1]Asif Faisal, Tan Yigitcanlar, Md. Kamruzzaman, and Graham Currie, 'Understanding Autonomous Vehicles: A Systematic Literature Review on Capability, Impact, Planning and Policy' (2019) Journal of Transport and Land Use, 12: 1.

[2]Vincent Boulanin and Maaike Verbruggem, 'Mapping the Development of Autonomy in Weapon Systems' (Stockholm International Peace Research Institute (SIPRI) 2017) <https://www.sipri.org/sites/default/files/2017-11/siprireport_mapping_the_development_of_autonomy_in_weapon_systems_1117_1.pdf> accessed 26 October 2023.

[3]Neshat Elhami Fard, Rastko R Selmic and Khashayar Khorasani, 'Public Policy Challenges, Regulations, Oversight, Technical, and Ethical Considerations for Autonomous Systems: A Survey' (2023) 42 IEEE Technology and Society Magazine 45.

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

[5]Deloitte, 'The shift to flexible consumption: how to make an "as a service" business model work' <https://www.deloitte.com/global/en/our-thinking/insights/topics/business-strategy-growth/as-a-service-business-model-flexible-consumption.html> accessed February 2 2024.

[6]Bill Edwards, 'Drone as a Security Service: Is It Right for Your Business?' (October 1 2021) Security Technology <https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2021/october/drone-as-a-security-service-is-it-right-for-your-business/> accessed February 23 2024.

[7]Anna Kobaszyńska-Twardowska, Jędrzej Łukasiewicz, and Piotr W. Sielicki, 'Risk Management Model for Unmanned Aerial Vehicles during Flight Operations' (2022) Materials 15(7): 2448.

[8]Kong, 'A Survey of Cyberattack Countermeasures for Unmanned Aerial Vehicles' (2021: 148246).

[9]Ibid.

[10]Aiden Warren, 'Disruptive Technologies and New Threat Multipliers' in Elizabeth Kath, Julian CH Lee and Aiden Warren (eds), The Digital Global Condition (Springer Nature 2023) <https://doi.org/10.1007/978-981-19-9980-2_3> accessed 26 October 2023.

[11]Jackman and Hooper (n 41).

[12]For further insights into potential drone threats in a rapidly changing security environment please see Peter Lee, 'Drones – Opportunities, Threats and Challenges' in Robert Dover, Huw Dylan and Michael S. Goodman, Eds., Palgrave Handbook of Security, Risk and Intelligence (Basingstoke: Palgrave Macmillan, 2017).

[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.

[18]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.

Note: Endnote numbers are skipped in the Executive Summary because the references are repeated in the full report and are numbered in the order they appear in the full report.