Vehiculos Autónomos

AMENAZAS, RIESGOS, y OPORTUNIDADES

Researchers: Ishmael Bhila, Peter Lee, and Alison Wakefield

ASIS FOUNDATION™

Vehículos Autónomos: amenazas, riesgos y oportunidades

Investigadores: Ishmael Bhila, Peter Lee y Alison Wakefield

Spanish translation of Autonomous Vehicles: Threats, Risks & Opportunities Executive Summary.

Mario Arroyo provided this translation as a volunteer service project for the ASIS Foundation.
Mario Arroyo elaboró esta traducción como un servicio voluntario para la Fundación ASIS.

Resumen ejecutivo

El potencial de vehículos autónomos (VA) ha ido creciendo desde la década de 1990. Aunque los defensores de los VA a menudo han prometido demasiado y no han cumplido lo suficiente en el pasado, los avances en inteligencia artificial (IA), ahora permiten que las aplicaciones autónomas se desarrollen a un ritmo más rápido. Las oportunidades para el uso de vehículos autónomos abarcan los sectores comercial, militar y de seguridad, cubriendo los dominios terrestre, aéreo, marítimo y submarino. Estas nuevas tecnologías ofrecen beneficios logísticos, operativos y técnicos, pero también traen consigo una variedad de amenazas, riesgos y desafíos que pueden limitar su uso o ralentizar su implementación.

Este informe documenta las amenazas, riesgos, desafíos y oportunidades que presentan los AV en varios campos para brindar recomendaciones para su uso por parte de los profesionales de la seguridad. Muestra cómo los profesionales pueden beneficiarse de los avances en las tecnologías AV y al mismo tiempo evitar consecuencias inesperadas o no deseadas.

Los AV pueden caracterizarse como sistemas que pueden funcionar con grados mínimos de intervención humana o ninguna. La automatización en vehículos implica la sustitución de parte o todo el control humano de un sistema por dispositivos electrónicos, mecánicos o sensoriales.[1] La autonomía en los sistemas se ha aplicado para la movilidad (retorno a la

base, navegación, despegue y aterrizaje), control remoto de sistemas por parte de operadores humanos (realización de actividades pre programadas), focalización (reconocimiento y seguimiento de objetivos), inteligencia (detección de objetos, dispositivos, intrusión, disparos de armas, generación de mapas, evaluación de amenazas y análisis de *big data*), interoperabilidad (cooperación con otros sistemas militares/de seguridad) y gestión del estado de los sistemas (autorrecarga/reabastecimiento de combustible, diagnóstico y reparación).[2]

Para los profesionales de la seguridad, existe una desconcertante variedad de regulaciones nacionales e internacionales, marcos industriales y estándares y guías emergentes que deben seguir. Incluso el término "autónomo" es problemático porque se utiliza para significar muchas cosas diferentes, desde automatización programada hasta sistemas con capacidades de autoaprendizaje. El objetivo de esta investigación fue ayudar a los profesionales de la seguridad a comprender mejor este campo complejo y dispar para gestionar mejor las amenazas, los riesgos y las oportunidades asociadas.

Características y oportunidades de los vehículos autónomos existentes

El desarrollo y la fabricación de vehículos autónomos se están expandiendo rápidamente para uso marítimo, terrestre y aéreo. Los desafíos prácticos y éticos que generan son altamente complejos y continuarán en el futuro previsible. El grado de complejidad, a su vez, está influenciado por el nivel de autonomía dentro de un vehículo o sistema en particular. Esto está sucediendo en contextos tanto civiles como militares y se extiende para incluir sistemas de armas autónomos. Los profesionales de la seguridad deberán mantenerse al tanto de los desarrollos en los marcos legales y de seguridad a los que deben cumplir. Sin embargo, las posibles recompensas son significativas, dada la amplia gama de aplicaciones actuales y potenciales, que incluyen:

- Acceso a terrenos remotos y desafiantes
- Sensores acústicos para detectar ruidos fuertes como explosiones
- Inspección de activos
- Transporte de mercancías

● Recopilación de datos para operaciones de seguridad

● Detección y eliminación de explosivos

● Respuesta con armas de fuego

● Identificación y recuperación de activos perdidos

● Transporte de personal

● Evaluación de riesgos

● Búsqueda y rescate de personal

● Protección de infraestructuras

● Protección de personal

● Comunicaciones de seguridad e intercambio de información

● Imágenes térmicas

● Videovigilancia

Los avances en el desarrollo de los VA presentan nuevas e importantes oportunidades comerciales para las empresas.[3][4] En comparación con los vehículos convencionales, los sistemas autónomos pueden ser menos costosos, más confiables, más rápidos en la ejecución de tareas y más sostenibles desde el punto de vista ambiental, reducen los costos laborales, aumentan la seguridad debido a la ausencia de errores humanos y permiten la ejecución simultánea de tareas. Los modelos de consumo flexible (MCF), también llamados modelos "como servicio" (XaaS), aportan más beneficios al proporcionar servicios sin propiedad y con pago por uso. Estos se adaptan al ritmo del avance tecnológico, ya que evitan que el usuario potencial invierta en tecnología que rápidamente se vuelve obsoleta; son más sostenibles desde el punto de vista ambiental y pueden ser significativamente más rentables.[5] Las innovaciones de "drones como servicio de seguridad" incluyen el desarrollo de sistemas de drones en una caja, que pueden cubrir áreas mucho mayores que los equipos y el personal terrestre, proporcionan una capa adicional de seguridad para patrullas y reacciones rápidas y sistemas de drones unidos, con tiempos de vuelo teóricamente ilimitados.[6]

Amenazas y riesgos que plantean los vehículos autónomos

Los impactos positivos y las oportunidades potenciales para los vehículos autónomos son numerosos. Sin embargo, su producción y uso, en particular en estas primeras etapas de su evolución, presentan diversos desafíos para la seguridad de los sistemas de vehículos autónomos, incluidos usos ilegales, problemas de hardware y rendimiento, la explicabilidad de la IA que impulsa la autonomía, preocupaciones éticas y desconfianza pública. Las principales amenazas a la seguridad de los vehículos autónomos se relacionan con su funcionamiento seguro y la ciberseguridad, ya que se basan en una combinación de tecnologías digitales, técnicas sensoriales y plataformas de IA. El enfoque principal de la regulación de los vehículos autónomos civiles es la seguridad, y la proliferación de vehículos autónomos requiere estándares de seguridad y calidad sólidos.

Kobaszyńska-Twardowska, et al., identifican seis fuentes de peligros potenciales para la operación de vehículos aéreos no tripulados, que son igualmente aplicables a otros tipos de vehículos autónomos. Estos son:

● Error humano (debido a factores como la mala comunicación entre el equipo operativo, la capacitación insuficiente del personal, la fatiga o la presión de un supervisor para desplegarse en condiciones inadecuadas)
● Incumplimiento de los procedimientos
● Falla del vehículo o sistema
● La aparición de otro vehículo en curso de colisión
● Deterioro rápido de las condiciones climáticas
● Deterioro en el rendimiento de los sistemas utilizados en la dirección o la navegación, como el GPS.[7]

La ciberseguridad de los VA también es una preocupación importante, ya que se comunican a través de canales inalámbricos que no son seguros por defecto.[8] Estas plataformas son propensas a ciberataques por parte de actores que intentan interrumpir, dañar o manipular los VA.[9] Los actores de amenazas, que van desde atacantes individuales y autónomos hasta grupos organizados que operan como parte de una empresa criminal o en nombre de un

estado nacional, trabajan para infiltrarse, desestabilizar o atacar los sistemas informáticos en los que operan los VA.[10] Una clasificación de Jackman y Hooper[11] divide las amenazas de los sistemas AV en cuatro categorías:

● Captura de imágenes y videos (de infraestructura crítica o sensible, sitios o actividades comerciales u operaciones de servicios de emergencia; para reconocimiento; para invadir la privacidad; o como medio de abuso o acecho de individuos, por ejemplo, ex parejas).
● Transporte y porte de armamento o contrabando
● Recopilación de datos (para ciberataques o espionaje corporativo)
● Interrupción (de sitios, eventos o actividades, como aeropuertos, eventos políticos, eventos deportivos u operaciones de servicios de emergencia)

El uso de pequeños drones comerciales listos para usar como arma es ahora una dimensión significativa de la lucha bélica en Yemen, Ucrania y Gaza. Estos drones de grado comercial se utilizan para reconocimiento, conocimiento de la situación y el despliegue de pequeños explosivos o granadas. Los terroristas que desarrollan una capacidad similar aumentan la amenaza potencial a la infraestructura nacional y otros edificios y objetos.[12] Los vehículos aéreos no tripulados pequeños pueden ser rápidos, ágiles y difíciles de identificar y rastrear, y aún más difíciles de eliminar del cielo por la fuerza. Entre los ataques notables con drones a infraestructuras críticas, cada uno atribuido a terroristas hutíes en Yemen, se incluyen:

● Un ataque en enjambre de 25 drones y misiles[13] a las instalaciones de procesamiento de petróleo de Saudi Aramco en Abqaiq y Khurais en Arabia Saudita, que interrumpió la producción en alrededor de 5 millones de barriles por día, equivalente al 5 por ciento de la producción mundial (2019)[14]
● Ataques a petroleros cerca del Aeropuerto Internacional de Abu Dhabi, que mataron a tres personas e hirieron a otras seis (2022)[15]
● Múltiples ataques a buques de transporte comercial en el Mar Rojo, una de las rutas comerciales más importantes del mundo.[16]

Cuando los vehículos autónomos incorporan niveles cada vez más altos de capacidad autónoma, la interrupción de la señal se convierte en una amenaza menor, pero la IA involucrada en dichos sistemas trae sus propios desafíos para garantizar la consistencia, la

seguridad y la confiabilidad. El elemento cibernético por sí solo plantea múltiples amenazas: los daños pueden dejar un sistema inutilizable, la piratería informática puede hacer que delincuentes o terroristas se apoderen del control de un VA, mientras que la suplantación de identidad (confundir el sistema) puede tener consecuencias igualmente desastrosas. De cara al futuro, se prevén las siguientes tendencias:

● Las preocupaciones en materia de seguridad aumentarán a medida que las organizaciones delictivas y los grupos terroristas adapten cada vez más los vehículos autónomos comerciales, a medida que se aprendan las lecciones de zonas de guerra como Ucrania y Gaza.

● El costo relativamente bajo de las capacidades de vigilancia sofisticadas supondrá un desafío para las organizaciones de seguridad, policiales y militares.

● La interconexión de los vehículos autónomos en los dominios aéreo, terrestre, de superficie y submarino pondrá a prueba aún más las capacidades de seguridad.

● Cuando los vehículos autónomos comerciales dependen de una señal en vivo para funcionar, serán cada vez más vulnerables a la piratería y la suplantación de identidad.

Las percepciones públicas de la fiabilidad de los vehículos autónomos y los sistemas autónomos en general tendrán un impacto significativo en la decisión de los gobiernos de asumir riesgos sociales y económicos para licenciar nuevos sistemas. Los fabricantes y desarrolladores también tendrán que hacer cálculos de riesgo cuidadosos sobre los sistemas que pueden ser menos predecibles que sus antecesores analógicos. Seguirán surgiendo nuevos desafíos éticos a medida que la autonomía se desarrolle en sofisticación y aplicación. Por ejemplo, si los sistemas autónomos incluyen CCTV o reconocimiento facial, el derecho a la privacidad de los ciudadanos privados puede verse violado si los sistemas se utilizan en lugares públicos. Esto podría agravarse aún más si la IA que impulsa el sistema autónomo no es lo suficientemente explicable como para proporcionar razones por las que se produjo la violación de la privacidad.

Entorno regulatorio

Ante los riesgos que presentan los sistemas de IA y los sistemas autónomos que `la respaldan`, la comunidad global está involucrada en una "carrera hacia la regulación de la IA".[17] Los esfuerzos para regular la IA en su aplicación a los vehículos autónomos han sido

dispares y fragmentados. Algunos han caracterizado los esfuerzos para gobernar la IA como un ejercicio similar a arrear gatos *(Expresión idiomática anglosajona para describir el desafío de organizar o gestionar una situación caótica o incontrolable)*, especialmente si los responsables de las políticas se centran en la naturaleza de las tecnologías en lugar de los riesgos y las oportunidades que presenta la IA.[18] Los vehículos autónomos terrestres, aéreos y marítimos han recibido un trato diferente en lo que respecta al desarrollo de regulaciones, aunque algunos sistemas, por ejemplo los sistemas de enjambre, operan en todos esos dominios y pueden utilizar los mismos modelos para su funcionamiento. Por lo tanto, la regulación de los vehículos autónomos se divide en cinco ejes:

1. Regulación general de la IA a través de iniciativas internacionales, nacionales e institucionales: es probable que la mayoría de los vehículos autónomos utilicen tecnologías basadas en IA, especialmente con los avances en el aprendizaje automático.

2. Regulación de los vehículos aéreos no tripulados.

3. Regulación de los vehículos terrestres autónomos.

4. Regulación de los vehículos marítimos autónomos.

5. Regulación de los sistemas de armas autónomas

Los gobiernos y las organizaciones internacionales están debatiendo cómo regular los vehículos autónomos de manera que se maximicen los beneficios sociales, económicos y militares y se minimicen los daños. Los distintos organismos adoptan distintos enfoques, algunos de los cuales se centran en los aspectos técnicos y las capacidades, mientras que otros se concentran en los riesgos y las oportunidades que implican. Estos esfuerzos no han abordado plenamente las necesidades y los riesgos que presentan las tecnologías emergentes en el ámbito de los vehículos autónomos ni han empleado un enfoque holístico de la regulación. Se necesita un marco regulatorio multisectorial e integrado que regule el desarrollo y el uso de los cinco ejes de las tecnologías de los vehículos autónomos de manera más integral.

Implicaciones para el sector de la seguridad

La gestión de los riesgos y amenazas que presentan los vehículos autónomos es una preocupación apremiante para los profesionales de la seguridad, especialmente a medida que las tecnologías se vuelven más omnipresentes, siendo los sistemas de aeronaves no tripuladas un área clave de atención. Deben ser conscientes de los riesgos y amenazas de seguridad para los vehículos autónomos que utilizan sus organizaciones o clientes, como parte del creciente panorama ciber-físico organizacional. Esto requiere el reconocimiento de dichos riesgos en los marcos de gestión de riesgos organizacionales, sobre la base de una sólida comprensión de las contramedidas de prevención, detección y mitigación, así como de una conciencia de los desafíos en el horizonte y las áreas clave de innovación futura. También se necesita un enfoque colaborativo para la seguridad, en reconocimiento del ritmo del avance tecnológico y la complejidad del entorno de riesgo. Organizaciones como ASIS International pueden desempeñar un papel clave a la hora de reunir a las comunidades de partes interesadas y compartir conocimientos. Al contribuir a la protección de dichos sistemas, los profesionales de la seguridad pueden aprovechar los beneficios de los vehículos autónomos que están transformando otros sectores e incorporarlos de forma más activa en el arsenal de seguridad: estas tecnologías nunca han sido más baratas ni más accesibles. También deben mantenerse al día con la legislación y los requisitos reglamentarios necesarios en las jurisdicciones donde se diseñan y construyen los vehículos autónomos y los sistemas, así como donde pueden utilizarse o venderse. Con la proliferación de regulaciones, este desafío no hará más que crecer.

Conclusión

Los VA presentan desafíos de seguridad urgentes, tanto como un riesgo que debe gestionarse como herramientas organizativas cada vez más importantes que forman parte del paisaje ciber-físico que necesita protegerse. Este informe destaca las consideraciones clave para brindar seguridad en estos dos aspectos. Los vehículos autónomos también tienen el potencial de transformar y mejorar la práctica de seguridad. El uso de vehículos autónomos ha sido transformador en muchos sectores y ha tenido un impacto dramático en los mercados, el comportamiento de los usuarios y las actitudes hacia los servicios prestados. El sector de la seguridad debe anticipar estos cambios, al mismo tiempo que debe estar preparado para

contribuir a la armonización de la prestación de servicios de acuerdo con las necesidades multisectoriales, las directrices y leyes nacionales e internacionales y las percepciones públicas sobre el uso de tecnologías emergentes.

Metodología de la investigación

La investigación fue encargada por la Fundación ASIS y se llevó a cabo entre agosto de 2023 y febrero de 2024. Se empleó la metodología de una revisión de alcance: una síntesis de conocimientos adecuada para proyectos de investigación exploratoria. Basada en un enfoque sistemático para mapear la evidencia sobre un tema e identificar conceptos clave, teorías, hallazgos, fuentes de evidencia y brechas de conocimiento. Al igual que una revisión sistémica, es un proceso sistemático, transparente y replicable que proporciona un enfoque útil para examinar la evidencia emergente cuando las preguntas más específicas que se pueden abordar a través de una revisión sistémica más precisa aún no están claras. Una revisión de alcance puede extenderse a la literatura gris que no es publicada por editoriales comerciales o indexada en bases de datos de investigación, como investigaciones gubernamentales o del sector privado o libros blancos, disertaciones y artículos de conferencias.

En el caso de los vehículos autónomos, la vasta y rápidamente cambiante literatura abarca las diferentes dimensiones y categorías tecnológicas de los vehículos autónomos; abarca varias disciplinas académicas; incluye una extensa literatura gris junto con la académica, incluidos documentos gubernamentales y libros blancos de la industria; e incluye leyes y marcos regulatorios existentes y futuros en múltiples jurisdicciones. La metodología elegida refleja la dificultad de captar una gama tan amplia de dimensiones a través de la investigación empírica y la necesidad de sintetizar el conjunto de conocimientos existentes en primera instancia para identificar los parámetros y dimensiones clave del campo.

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

[4]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.

[5]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.

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

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

[8] Ibid.

[9] 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

[10] Jackman and Hooper (n 41)

[11] 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).

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

[13] Michael Safi and Graeme Wearden, 'Everything you need to know about the Saudi Arabia oil attacks' (September 16 2019) The Guardian <https://www.theguardian.com/world/2019/sep/16/saudi-arabia-oil-attacks-everything-you-need-to-know> accessed February 20 2024.

[14] Martin Chulov, 'Suspected drone attack in Abu Dhabi kills three and raises tensions' (January 17 2022) The Guardian <https://www.theguardian.com/world/2022/jan/17/drones-explosions-three-oil-tankers-airport-abu-dhabi> accessed February 20 2024.

[15] 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.

[16] Patrick Wintour and agencies, 'Red Sea crisis: UN security council demands immediate end to Houthi attacks' (January 11, 2024) The Guardian <https://www.theguardian.com/world/2024/jan/11/red-sea-shipping-crisis-un-security-council-yemen-youthi-rebels-attacks> accessed February 20 2024

[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.