THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 69-78
https://doi.org/10.55682/cdr/m9d9-5ee5

PROFESSIONAL COMMENTARY

Autonomous Vehicles in Critical Infrastructure: Technologies, Vulnerabilities, and Implications

Donna Artusy

Autonomous vehicles (AVs) are quickly emerging as a critical component of the Transportation Systems Sector (TSS), one of the essential infrastructure sectors designated by the Department of Homeland Security (DHS). While autonomy is not a new concept, advancements in artificial intelligence (AI), real-time data processing, and sensor fusion have accelerated the deployment of AV technology in both military and commercial civilian sectors. These technologies enable AVs to operate with varying levels of autonomy but also introduce significant cybersecurity, legal, and ethical challenges. As AV integration into critical infrastructure scales and military reliance on interconnected autonomous systems grows, ensuring cyber and operational resilience becomes a national security imperative to guard against cyber-physical threats. This article explores the technological foundation of AVs, their military and commercial applications, and the cybersecurity risks impeding safe deployment. We examine specific frameworks, such as the commercial SAE autonomy levels (1-5) and military adaptations like the Robotic Combat Vehicle (RCV) program, alongside key cybersecurity threats, including remote hacking, GPS spoofing, and Denial-of-Service (DoS) attacks. This analysis highlights the immense potential and inherent vulnerabilities of AV technology as it becomes more deeply integrated into civilian and military systems. The paper concludes by addressing critical cybersecurity measures, including strong encryption and AI model training, to mitigate these risks and enhance AV security in commercial and defense applications.

Keywords: critical infrastructure, autonomous vehicles, autonomy level, transportation systems sector, cybersecurity

INTRODUCTION

Autonomous vehicles (AVs) are integral components of the Transportation Systems Sector (TSS)-one of the Department of Homeland Security's (DHS) sixteen critical infrastructure sectors (CISA 2022). TSS consists of various modes of transportation essential for the movement of both people and goods, and autonomous ground vehicles are now among them. Although the concept of autonomously operated vehicles is not novel per se, their commercial applications and implementation into military systems have introduced both clear efficiencies and significant vulnerabilities. AVs include a number of complex and robust integrations of artificial intelligence (AI), real-time data processing, and geospatial mapping. These foundational technologies, however, expand the attack surface and introduce new cybersecurity threats. Algorithmic limitations and a growing dependence on existing infrastructure become critical vulnerabilities. Furthermore, the deployment of AVs raises novel legal and ethical concerns.

As AVs become increasingly embedded within both civilian and military transportation networks, they function not only as vehicles but as cyber-physical platforms deeply dependent on the integrity and reliability of other critical infrastructure systems and data that support their operation. This reliance creates strategic vulnerabilities, exposed to the disruption of digital enablers such as Global Positioning System (GPS), mobile 5G communications, and cloud-based control architectures. Threats can directly impair mobility operations, logistical continuity, and broader defense readiness. Cybersecurity and operational resilience are therefore not ancillary concerns: they are foundational requirements for the secure deployment of AVs within national infrastructure.

Technological advances are double-edged swords. In this particular case, the advent of autonomous technology in both military and civilian settings presents many potential benefits along with new vectors of vulnerability ripe for exploitation by U.S. adversaries (Guttieri 2025, 95). AVs expand the national cyber-physical attack surface by linking AI-driven decision-making systems, sensors, and cloud-connected infrastructure, thereby intertwining transportation with other critical infrastructure sectors (National Counterintelligence and Security Center 2022). Because AVs rely on the continuous exchange of data and constant connectivity, a 'successful' cyberattack could cascade across logistics and emergency services, underscoring the need to integrate AV cybersecurity into broader national resilience and infrastructure protection frameworks (NHTSA, n.d.). Accordingly, it would make logical sense to conceptualize cyber resilience as integral to a sustained national strategic posture (Demchak 2021). This framework of considering cyber resilience will help position the U.S. in a more strategically favorable position on the world stage, where progressively sophisticated cyber threats are constantly emerging.

This article provides a high-level overview of the technologies underpinning AV systems and examines their use in commercial and military contexts. The article then analyzes the impact

of AVs on critical infrastructure and discusses key cybersecurity vulnerabilities, concluding with a high-level snapshot of the legal and policy landscapes for the technology.

Levels of Autonomy

The Society of Automotive Engineers (SAE) provides a helpful standardized taxonomy of levels of vehicle automation. According to this framework, Levels 1 and 2 necessitate driver assistance features and are not classified as fully autonomous systems. Levels 3-5 represent higher levels of automation that culminate with full autonomy. Vehicles classified at either Level 4 or 5 are capable of operating without human intervention when automated systems are engaged; however, Level 4 systems still allow for human oversight in specific conditions (SAE 2021). Commercially available technologies such as Google's Waymo cars are currently considered Level 4: they are fully autonomous in the sense that humans are not directly driving the vehicle, but can still provide guidance for the vehicle in new or unknown situations (Ackerman 2021). As of this writing, Level 5 autonomy—representing full automation without any human intervention in all driving conditions—has not yet been achieved.

Technologies Used in Autonomous Vehicles

AVs integrate a diverse range of technologies and computational systems to operate with varying levels of autonomy. These technologies typically include AI, high-definition real-time geospatial mapping, advanced perception systems such as LiDAR (Light Detection and Ranging), radar, and Vehicle-to-Everything (V2X) communication. Most AVs employ a combination of LiDAR, radar, GPS, cameras, high-definition maps (including Simultaneous Localization and Mapping (SLAM)), sensor fusion, and Inertial Navigation Systems (INS) to accurately perceive their surroundings, determine their position, and navigate within their environment. However, certain AV systems prioritize camera-based perception and AI-driven computer vision over LiDAR, relying on deep learning algorithms and real-time image processing to interpret the driving environment and make navigation decisions.

Each of these technologies contributes to the vehicle's capacity for operating with greater levels of autonomy and accuracy, as well as its ability to adapt to unexpected environmental changes. By integrating AI, advanced sensor systems, high-definition mapping, and real-time data processing, AVs can more effectively perceive, interpret, and react to dynamic road conditions. Consequently, this causes a reduction in reliance on human intervention and increases operational reliability. AI serves as the basis for the 'intelligence' of AVs, leveraging subfields of AI, including machine learning (ML), neural networks, and generative AI (genAI) to process sensory data and make real-time driving decisions. AI significantly improves the vehicle's ability to predict and react to dynamic road conditions (Bojarski et al. 2016). LiDAR enhances both object detection and depth perception, creating a high-resolution 3-dimensional model of the AV's surroundings. This is critical for obstacle avoidance and precise

navigation in complex, evolving environments (Shan and Englot 2018). Radar can add an additional layer of perception, particularly in adverse weather conditions where LiDAR and cameras are less effective.

GPS and INS work together to maintain accurate vehicle positioning: GPS provides more precise global location data, while INS compensates for GPS signal disruptions by tracking motion and orientation through accelerometers and gyroscopes (Groves 2013). SLAM algorithms allow AVs to build and refine maps of their environment in real-time, improving localization and adaptation to previously unknown geographies (Durrant-Whyte and Bailey 2006). Sensor fusion rapidly combines and processes incoming sensor data to improve the accuracy, reliability, and robustness of the autonomous system. This helps AVs detect obstacles, road conditions, pedestrians, and infrastructure signals more accurately than relying on a single sensor modality. Lastly, V2X communication enhances vehicle decision-making by enabling AVs to exchange real-time data with other vehicles and infrastructure. This improves efficiency and safety through cooperative maneuvering and collision avoidance (Papadimitratos et al. 2009). The collective use of all of these technologies reduces the need for human intervention, bringing AVs closer to achieving full autonomy.

MILITARY AND COMMERCIAL APPLICATIONS OF AUTONOMOUS VEHICLES

While the commercial development of AVs has garnered public attention for decades, the U.S. Army has simultaneously pursued its own applications through various initiatives. Autonomous combat vehicles offer the potential to reduce casualties on the battlefield, where over 50% of casualties historically occur during the transport and delivery of supplies in combat zones (Muller 2019). The Army's initial endeavor focused on the "leader-follower" robotic vehicle deployment program, which utilized AV technologies to enhance force protection and sustainment. In March 2023, the "leader-follower" program was replaced by the Autonomous Vehicle Transport System, which aims to expand these autonomously driven capabilities further (Luckenbaugh 2023).

A few months later, the Army shifted its focus to leveraging commercial autonomous driving technologies for implementation in convoy operations (Eversden 2023). The shift was driven by a desire to accelerate the adoption of emerging capabilities readily available in the commercial sector. This new direction included a prototyping competition managed by the Defense Innovation Unit (DIU)—the Ground Expeditionary Autonomy Retrofit Systems (GEARS). GEARS sought vendors to equip existing military vehicles with reliable unmanned operational capabilities (Harper 2023). The program's goal was to integrate both hardware and software to enable autonomous functions, including convoy operations and navigation, while maintaining an open architecture to facilitate future upgrades.

The Army is also developing a Robotic Combat Vehicle (RCV) program as part of its "Next Generation Combat Vehicle" series, designed to function directly in combat scenarios (Feickert 2025). This ongoing program aims to develop a family of unmanned, combat-ready vehicles that can operate collaboratively with manned vehicles. The RCV's mission set has been expanded to include reconnaissance, execution of complex tactical maneuvers, and direct self-defense when attacked. As of October 2024, the Army planned to select one vendor from a 2023 Army Request for Prototype Proposal (RPP) to proceed with the platform prototype design and build phase of the RCV program (John 2023). Although current RCVs incorporate advanced sensors, they remain dependent on soldiers for operation; testing in 2024 revealed that one control vehicle with a crew of five soldiers was necessary for the deployment of two RCVs. The progression toward greater autonomy will be heavily influenced by funding considerations and how well RCVs perform in battle-simulated environments. While the aforementioned SAE standards apply to commercial automotive applications, it is reasonable to infer from publicly available information that the RCVs currently operate at an equivalent of approximately Level 3 autonomy.

CRITICAL INFRASTRUCTURE IMPLICATIONS

AVs have become more embedded within critical infrastructure due to their reliance on and integration with interconnected cyber-physical systems that underpin modern transportation networks. The security of such networks extends well beyond individual vehicles, encompassing mobile communication protocols such as 5G, GPS navigation systems, cloud-based command and control systems, and the physical infrastructure that supports these technologies. Such dependencies magnify the potential negative impact of cyber and physical disruptions, which can cascade through many sectors, thereby threatening broader national resilience. The breadth of this exposure necessitates robust risk management and mitigation strategies, combined with cross-sector coordination to safeguard these interdependent systems from increasingly sophisticated threats. Effective risk management for AVs within critical infrastructure involves continuous threat identification, timely vulnerability assessments, and implementation of layered cybersecurity controls. Collaboration across interdependent critical infrastructure sectors will proactively mitigate emerging threats, ensure reliability, and lead to increased resilience.

In military operations, AVs play critical roles in autonomous logistics, reconnaissance, and force mobility. To simultaneously reduce personnel risk while also enhancing operational flexibility and responsiveness, the resilience of these platforms is vital. Disruptions may impair mission-critical capabilities and strategic mobility. Addressing these vulnerabilities requires adherence to established cybersecurity frameworks from the National Institute of Standards and Technology (NIST), such as NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations* (Joint Task Force 2018), and NIST SP 800-82 Revision

3, *Guide to Operational Technology (OT) Security* (Stouffer et al. 2023), alongside integrated policies that unify civilian and military cybersecurity efforts. This comprehensive approach helps to ensure that the deployment of AVs strengthens, rather than jeopardizes, national security objectives across both civilian and defense domains.

CYBERSECURITY VULNERABILITIES AND MITIGATION STRATEGIES

As has been an evident trend over the last decade, cybersecurity attacks are becoming increasingly prevalent, and malicious actors are becoming more sophisticated. AVs are not immune to such attacks. Although autonomous technologies are not yet widespread and remain limited to select commercial applications, their expansion to buses and other public transportation will increase the vulnerabilities of related critical infrastructure. Understanding potential threat vectors will significantly mitigate potential damages and threats to human life, while also raising awareness of legal liability issues. Some of the potential vulnerabilities for both commercial and subsequently military AVs include data breaches and privacy concerns, remote hacking and unauthorized access, GPS spoofing and sensor manipulation, and Denial of Service (DoS) attacks. Although each of these present significant potential harm to users and those around them, mitigating measures can be taken to reduce such risks considerably.

Data Breach and Privacy Considerations

There are clear legal concerns around AVs, including liability, data breaches, and potential exposure of user data. This particular topic is broad and has been extensively examined in academic analyses, articles, and books. To remain within the scope of this article, the analysis here will provide a high-level overview rather than engaging in an in-depth legal examination. In constantly evolving and multi-faceted environments with AVs, the information security considerations impact not only the integrity of data, but also the physical security of the passengers and those around them. Consequently, robust security practices are critical to both informational and physical safety by securing the information and data. A primary security objective is to maintain the confidentiality, integrity, and availability of data.

AVs may generate and collect substantial amounts of data during operation: while not an exhaustive list, this may include real-time and geolocation data, synced device data, and driving habits. AVs are also vulnerable to malware infections via over-the-air software updates. Mitigating strategies can be implemented at several levels, including multi-layer authentication, intrusion detection systems (IDS), robust encryption practices, multi-factor authentication, and AI model training to ensure the security of deep learning models. Typically, AVs utilize Advanced Encryption Standard (AES) 256 and secure communication protocols, including Transport Layer Security (TLS), to protect data transmitted between the vehicle, infrastructure, and cloud environments (Rossi, Tiffiny 2019). AVs increasingly incorporate generative AI (genAI) models to enhance decision-making, communication with operators, and further

advance autonomous capabilities. Such models rely on a vast amount of training data to 'learn' and subsequently make effective decisions during the deployment of the technology (Muller 2024). Ensuring that genAI models are trained on high-quality and integrity-verified data provides safeguards for reducing biases, improving real-world adaptability, and mitigating safety risks associated with unpredictable driving conditions. Curated datasets further help AVs respond accurately to edge cases, diverse environmental conditions, and complex scenarios, ultimately enhancing reliability and trust in autonomous systems.

Remote Hacking, Unauthorized Access, GPS Spoofing, and Denial of Service

Remote hacking involves exploiting security vulnerabilities in an AV's communication networks, such as the Controller Area Network (CAN), to gain unauthorized access and manipulate critical vehicle functions, including steering, braking, and acceleration (Adly et al. 2023). Malicious actors may also exploit vulnerabilities in internet-to-vehicle commands. This was evidenced by a Kia vulnerability exposed in 2024, where attackers could send unauthorized commands to other vehicles simply by substituting a victim's identifier (e.g. an email address) into an Application Programming Interface (API) request, which the backend system failed to authenticate before routing the command to the victim's vehicle (Greenberg 2024).

When cars rely on GPS for navigation, sending false location data to an AV can be detrimental: inaccurate or manipulated location data compromises the vehicle's ability to navigate correctly. Not only is this disruptive and potentially harmful to the passengers in the AV, it can also disrupt the integrity of vehicle-to-vehicle (V2V) communications, vehicle-to-network (V2N) communications (which enable AVs to connect to the cloud for navigation and real-time updates), and vehicle-to-pedestrian (V2P) communications which enable AVs to interact with pedestrians through mobile devices or sensors. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks can target the AV's network bandwidth or processing capacity, potentially impacting all of these safety-critical services and functions. The degradation of the AV's ability to properly receive, interpret, or transmit data and interface with external systems can result in severe consequences (Durlik et al. 2024).

THE LEGAL AND POLICY LANDSCAPE

The proliferation of AVs introduces critical legal and policy challenges. Examining these implications is crucial for a comprehensive understanding of the emerging AV landscape.

Legal Liability Standards

At a high level, legal liabilities for AVs follow in part traditional paths of product liability, strict liability, negligence, and, of course, breach of contract. While software embedded in commercial vehicles is not new in itself, the autonomous component alters the nature of risks and may impact the legal framework of responsibilities. Increasing levels of autonomy seem

to necessitate a shift in this legal framework, but is that necessary? Proponents of change may argue that responsibility and control no longer stem directly from a human decision-maker, as in a traditional vehicle. Additionally, causation becomes more attenuated and removed with increasing levels of autonomy. Conversely, some legal scholars argue that traditional legal frameworks are sufficiently robust to resolve the liability question. Regardless of the type of human control technology, is it not still true that the car manufacturer is responsible for its platforms, including embedded technology (joint liability considerations aside)?

The courts are still grappling with the conundrum of how to address AVs as more cases come to the fore. Many such cases have settled out of court, removing the opportunity for courts to set precedent where applicable. This question will undoubtedly become more critical as the levels of autonomy in commercially available vehicles increase and the number of such vehicles in use proliferates.

Policy

At the policy level, although federal legislation regarding autonomous vehicles has been proposed, no such framework currently exists. There is no single federal law that explicitly regulates AVs, though the National Highway Traffic Safety Administration (NHTSA, n.d.) provides guidance for best practices around AV safety . Many states have adopted legislation attempting to address AVs but this mirrors the piecemeal state-by-state approach that is present in privacy laws today (Baker Donelson 2024).

NIST has provided guidance on the evolving topic, although it does not create a binding set of standards as of this writing. Several relevant frameworks apply to the technology within AVs, including the NIST Cybersecurity Framework (CSF), to help address cyber risk and vulnerability management for the technologies within the AVs. NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations* (NIST 2020), provides a comprehensive catalog of security and privacy controls. Although not directly written for AVs, this document offers guidance on cyber risk management to support system resilience for such vehicles. NIST Internal Report (IR) 8534, *Feature Description for Assessing Autonomous Vehicle Performance* (Hajjaj et al. 2024), provides a standardized framework for evaluating AV features, specifically to help support consistent assessment of performance, safety, and cybersecurity. While there are other relevant publications and guidance, it is worth acknowledging that a specific framework for AVs could be a worthwhile endeavor.

CONCLUSION

AVs represent a significant technological advancement with far-reaching implications for both commercial and military operations. The implementation of AI, LiDAR, GPS, SLAM, and other emerging technologies continues to push AVs toward greater autonomy, yet fundamental challenges remain, particularly regarding security vulnerabilities and operational limitations.

While the commercial sector has made strides in deploying AVs for public and private use, the military's approach, as evidenced by initiatives like the leader-follower program and its successors, demonstrates a commitment to leveraging AVs for combat and logistics applications that strive for higher levels of autonomy.

As AVs become more integrated with and reliant upon critical infrastructure sectors and networks, their security is intricately linked to the resilience of these interconnected systems. Consequently, cybersecurity threats such as data breaches, remote hacking, and GPS manipulation pose mounting risks that must be addressed through AI-driven security models and real-time monitoring systems. Along with a more robust and transparent legal landscape, this will undoubtedly bolster cyber resilience. Ensuring the safe and ethical deployment of AVs requires continued investment in security infrastructure and AI governance to shape the future of autonomy across industries. Such coordinated efforts will enhance U.S. cyber resilience and mitigate vulnerabilities, playing a vital role in defining the evolution of autonomous technologies across both civilian and military domains.

ABOUT THE AUTHOR

Donna Artusy is an attorney at a cybersecurity public company in Silicon Valley and non-resident fellow in Cyber Law, Policy, and Strategy at the Army Cyber Institute at West Point. She is also an area editor for The Cyber Defense Review Journal. She was previously a non-resident fellow at the Center for Security and Emerging Technology for CyberAI. Prior to earning her J.D., Donna received her graduate degree from Georgetown University's Walsh School of Foreign Service, and dual undergraduate degrees from the University of California, Berkeley. Previously, she completed the International Security and Intelligence program at the University of Cambridge. Donna's other professional experiences include co-founder of a health tech startup with multi-patented technology, Center for Strategic International Studies (CSIS), the United States Department of Justice, Santa Clara County Superior Court (civil and criminal), and Wilson Sonsini Goodrich and Rosati. She has numerous publications and speaking engagements around cybersecurity policy, law, and emerging tech.

REFERENCES

Ackerman, Evan. 2021. "What Full Autonomy Means for the Waymo Driver." IEEE Spectrum, March 4, 2021. https://spectrum.ieee.org/full-autonomy-waymo-driver.

Adly, Salah, Ahmed Moro, Sherif Hammad, and Shady A. Maged. 2023. "Prevention of Controller Area Network (CAN) Attacks on Electric Autonomous Vehicles." *Applied Sciences* 13 (16): 9374. https://doi.org/10.3390/app13169374.

Baker Donelson. 2024. "Autonomous Vehicle Statutes and Regulations Across the 50 States," September 20, 2024. https://www.bakerdonelson.com/autonomous-vehicle-statutes-and-regulations-across-the-50-states.

Bojarski, Mariusz, et al. 2016. "End to End Learning for Self-Driving Cars." *arXiv preprint,* 1–9. https://arxiv.org/pdf/1604.07316.

CISA (Cybersecurity and Infrastructure Security Agency). 2022. *Autonomous Ground Vehicles Security Guide: Transportation Systems Sector.* http://www.cisa.gov/sites/default/files/publications/Autonomous%2520Ground%2520Vehicles%2520Security%2520Guide.pdf.

Demchak, Chris. 2021. "Achieving Systemic Resilience in a Great Systems Conflict Era." *The Cyber Defense Review* 6 (2).

Durlik, Irmina, Tymoteusz Miller, Ewelina Kostecka, Zenon Zwierzewicz, and Adrianna Łobodzińska. 2024. "Cybersecurity in Autonomous Vehicles - Are We Ready for the Challenge?" *Electronics* 13 (13): 2654. https://doi.org/10.3390/electronics13132654.

Durrant-Whyte, Hugh, and Tim Bailey. 2006. "Simultaneous Localization and Mapping: Part I." *IEEE Robotics and Automation Magazine* 13 (2): 99–110. https://doi.org/10.1109/MRA.2006.1638022.

Eversden, Andrew. 2023. "Army Closing Down 'Leader-Follower' Robotic Truck Development, Eyeing Commercial Solutions," June 5, 2023. https://breakingdefense.com/2023/06/army-closing-down-leader-follower-robotic-truck-development-eyeing-commercial-solutions/.

Feickert, Andrew. 2025. *The Army's Robotic Combat Vehicle (RCV) Program.* Technical report. Congressional Research Service, May 20, 2025. https://crsreports.congress.gov/product/pdf/IF/IF11876.

Greenberg, Andy. 2024. "Millions of Vehicles Could Be Hacked and Tracked Thanks to a Simple Website Bug." Wired, September 26, 2024.

Groves, Paul. 2013. *Principles of GNSS, Inertial, and Multi-sensor Integrated Navigation Systems.* Boston: Artech House.

Guttieri, Karen. 2025. "Fighting Through Disruption: Reframing Cyber Resilience for Power Projection and Strategic Credibility." *The Cyber Defense Review* 10 (1): 93–114. https://doi.org/10.55682/cdr/egvf-mkys.

Hajjaj, H., T. T. Gamage, E. R. Griffor, T. P. Roth, and W. W. Guo. 2024. *Feature Description for Assessing Autonomous Vehicle Performance.* Technical report NIST IR 8534. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8534.

Harper, Jon. 2023. "DIU Issues Solicitation for GEARS Program to Convert Older Vehicles into Unmanned Systems," May 26, 2023. https://defensescoop.com/2023/05/26/diu-issues-solicitation-for-gears-program-to-convert-older-vehicles-into-unmanned-systems.

John, Ashley. 2023. "Army Selects Four Companies for Robotic Combat Vehicle Prototypes," September 20, 2023. https://www.army.mil/article/270093/army_selects_four_companies_for_robotic_combat_vehicle_prototypes.

Joint Task Force. 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.* Technical report 800-37 Rev. 2. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2.

Luckenbaugh, Josh. 2023. "Army Pressing Forward With Autonomous Vehicle Transport System." National Defense Magazine, March 1, 2023. https://www.nationaldefensemagazine.org/articles/2023/3/1/army-pressing-forward-with-autonomous-vehicle-transport-system.

Muller, Joann. 2019. "The U.S. Army Is Looking to Autonomous Vehicles to Cut Casualties," April 12, 2019.

Muller, Joann. 2024. "Generative AI Could Power the Next Wave of Self-Driving Cars," June 18, 2024. https://www.axios.com/2024/06/18/self-driving-cars-generative-ai.

National Counterintelligence and Security Center. 2022. *Autonomous Automotive Vehicles Supply Chain Risk.* Technical report. Washington, DC: U.S. Department of Homeland Security.

NHTSA (National Highway Traffic Safety Administration). n.d. *Automated Driving Systems.* https://www.nhtsa.gov/vehicle-manufacturers/automated-driving-systems. U.S. Department of Transportation.

NIST (National Institute of Standards and Technology). 2020. *Security and Privacy Controls for Information Systems and Organizations.* Technical report 800-53, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5.

Papadimitratos, Panagiotis, et al. 2009. "Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation." *IEEE Communications Magazine* 47 (11): 84–95. https://doi.org/10.1109/MCOM.2009.5307471.

Rossi, Tiffiny. 2019. "Fast, Secure File Systems for Autonomous Vehicles from Tuxera," January 3, 2019. https://community.arm.com/arm-community-blogs/b/embedded-and-microcontrollers-blog/posts/fast-secure-file-systems-for-autonomous-vehicles-from-tuxera.

SAE (Society of Automotive Engineers). 2021. *SAE J3016 Levels of Driving Automation Update.* SAE International, June. https://www.sae.org/blog/sae-j3016-update.

Shan, Tianyu, and Brendan Englot. 2018. "LeGO-LOAM: Lightweight and Ground-Optimized LiDAR Odometry and Mapping on Variable Terrain." In *IEEE/RSJ International Conference on Intelligent Robots and Systems,* 4758–4765. https://arxiv.org/pdf/1805.03766.

Stouffer, Keith, et al. 2023. *Guide to Operational Technology (OT) Security.* Technical report 800-82 Rev. 3. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3.