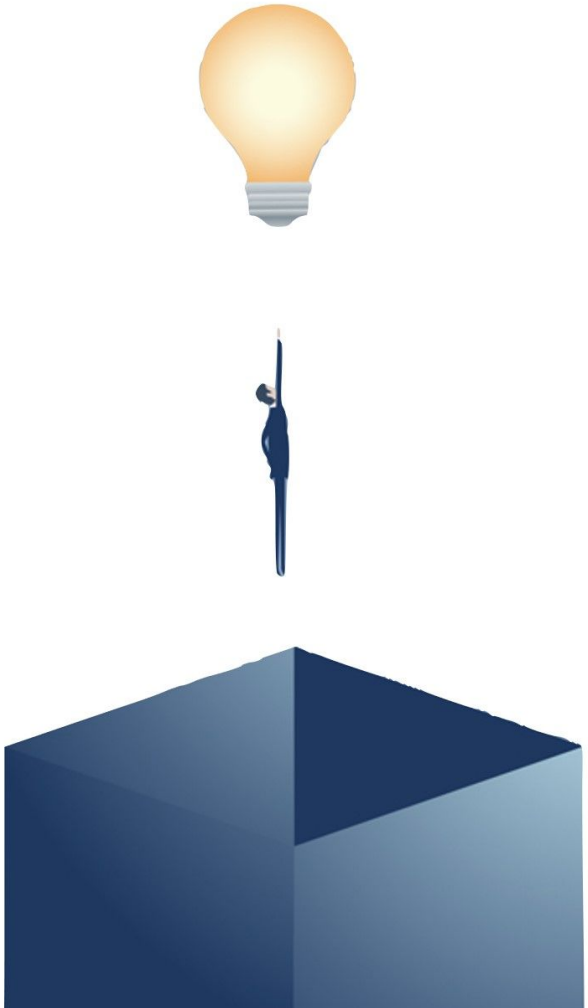
The Singularity group

Here Comes the Internet of Cars, Part II

A Singularity Snapshot



Research Takeaways

- **The autonomous vehicle (AV) landscape today** comprises autonomous trucks, driverless robotaxis, and privately owned cars that sometimes drive themselves. Also making gains are suppliers of advanced driver-assistance systems (ADAS).

- **TSG sees significant opportunity in the autonomous trucking segment.** Demand for autonomous trucks has accelerated with the post–pandemic demand for shipping. The global autonomous truck market is projected to reach $US 1.7 billion by 2025.[1]

- **Connected and automated vehicles may help pave the way for net-zero emissions.** Autonomy may increase vehicle energy efficiency between 5 and 20%.[2] Other aspects of connectivity, such as truck platooning, could potentially compound this increase.

- TSG portfolio companies such as **Daimler (DAI; Singularity Score (SC): 23)[3], Waymo (GOOGL; SC: 87), Velodyne (VLDR; SC: 100)**, **Luminar Technologies (LAZR; SC: 100),** and **NVIDIA (NVDA; SC: 100)** are among the core players in the autonomous truck –– and overall autonomous vehicle –– market. TSG is exposed to these dynamics through our **artificial intelligence, IoT, big data,** and **robotics Singularity Sectors.**

- **TSG believes the bottom–up approach to autonomy** pursued by ADAS providers also positions them to capture a significant share of the global autonomous vehicle market. TSG companies **Aptiv (APTV; SC: 16), Magna (MG CN; SC: 12), Intel (INTC; SC: 42)** and **TomTom (TOM2 NV; SC: 26)** are among those poised for growth.

- **Underpinning demand for AVs is the need for automotive cybersecurity.** TSG believes automotive cybersecurity is an overlooked sector in the autonomous and connected vehicle market. The automotive cybersecurity market is likely to be valued around $US5.6 billion in 2025, a 21.4% CAGR.[4] This opportunity should continue to expand as new products emerge.

[1]Allied Market Research, 'Global Self–Driving Truck Market Expected to Reach $1,669 Million by 2025.' Available online: https://www.alliedmarketresearch.com/press-release/self-driving-truck-market.html
[2]Institution of Mechanical Engineers, Automated Vehicles: Automatically Low Carbon. June 2016.
[3]The TSG Singularity Score is an indicator of a company's applied innovation, based on the revenues it generates by leveraging TSG Singularity Sectors. It is calculated on a standardized scale of 0—100, where 0 indicates no applied innovation and 100 denoted a company that fully applies innovative technologies.
[4]Million Insights, 'Automotive Cyber Security Market Size to Advance at 21.4% CAGR by 2025.' Available online: https://prn.to/3v61qwb

Introduction

Transportation –– the moving of people and goods from place to place –– serves a fundamental economic function. Historically transportation innovations have heralded and enabled profound economic transformations. The success of catalog retailers like Sears in the United States and Littlewoods in the United Kingdom, for example, could not have been possible without the railroad. The expansion of global cities into suburbs would not have happened in the absence of expansive highway systems and relatively inexpensive and accessible automobiles.

As we explored in our previous Singularity Snapshot, 'Here Comes the Internet of Cars,' transportation is entering another period of innovation that involves connected and autonomous vehicles. The Singularity Group (TSG) believes that superior economics, technological advancements, and increased convenience will encourage the adoption of autonomous vehicles, with some industry segments scaling faster than others. This will likely propel efficiency gains in many adjacent industries – logistics, agriculture, retail among them – helping to pave the way to net-zero emissions.

The autonomous vehicle (AV) landscape today comprises autonomous trucks, driverless robotaxis, and privately owned cars that sometimes drive themselves. Also making gains are suppliers of advanced driver–assistance systems (ADAS) that are taking a bottom–up approach, gradually adding new features to their products until they can achieve full self–driving capability. We expect that, in the near–to–medium term, autonomous trucks and ADAS suppliers should grow to dominate the autonomous vehicle sector.

Of course, autonomous driving is not without its challenges. Primary among them is cybersecurity. Advancements in autonomous technologies have transformed modern vehicles into data centers on wheels, creating ample vulnerabilities and opportunity for cyberattacks. While this poses a risk, we believe it is also an opportunity. The automotive cybersecurity market is anticipated to advance at a compound annual growth rate (CAGR) of 21.4% between 2021–2025 to reach $US 5.6 billion.[5] Among the key factors propelling this growth is the increasing sophistication of two of our Singularity Sectors: artificial intelligence (AI) and blockchain technology.

[5]Million Insights, 'Automotive Cyber Security Market Size to Advance at 21.4% CAGR by 2025.' Available online: https://prn.to/3v61qwb

1. Autonomous Technology Is Not New

The development of autonomous vehicles began decades ago when automakers started to introduce semi–autonomous technologies into private cars. Chrysler first introduced power–steering in 1951. Toyota released a car with adaptive cruise control in 1997. Audi introduced the first car with automated braking features in 2006. These advancements helped relieve various elements of a driver's responsibility, but they fall short of creating a fully autonomous vehicle. The Society of Automotive Engineers (SAE) defines five different levels of vehicle autonomy, as depicted in Figure 1.

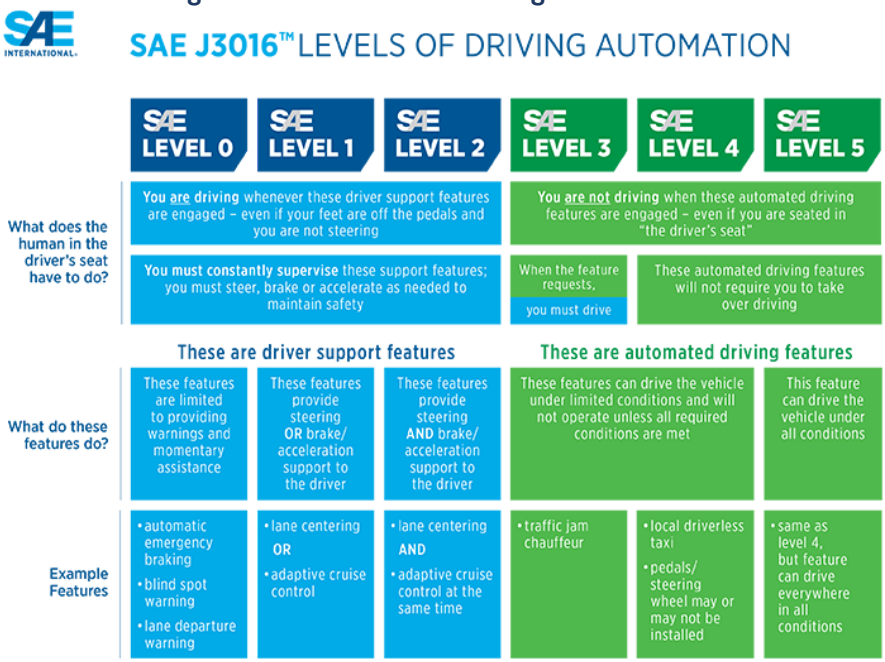
Today, ADAS players led by suppliers including Mobileye – and Intel (INTC; SC:42)[6] company – Aptiv (APTV; SC:16), Magna (MG CN; SC: 12), and Bosch work with all major automakers, which means most new vehicles already have partial automation –– Levels 1 and 2, including cruise control and automated braking. For example, Irish mobility company, Aptiv, supplies ADAS like autonomous emergency braking, blind spot warning, and lane assist to a broad customer base that includes General Motors, Volkswagen (VOW3 GR; SC:14), Fiat, and Hyundai (005380 KS; SC: 16).

It has been developing ADAS for over 20 years, gradually scaling its technology from active safety systems to greater levels of automation.

In March 2021 Honda (7267 JP; SC:10) launched the world's first L3 autonomous car, 'Legend,' in which acceleration, braking, and steering can be system–controlled.[7] In the event that a driver becomes unresponsive, the system will assist with an emergency stop and alert surrounding vehicles by activating the car's hazard lights and horn.

L4 - in which a driver cedes all responsibilities to the robotic car –– would be a significant step–change in the economics and utility of vehicle transport. Of the better–known L4 developments is the robotaxi project spearheaded by Alphabet's (GOOGL; SC: 87) self–driving car initiative, Waymo. Waymo has been offering driverless rides in the Phoenix, Arizona, area since October 2020.[8] It uses Pacifica minivans made by partner Fiat Chrysler. The company has additionally signed agreements with Volvo (VOLVB; SC: 3), Nissan–Renault, Fiat, and Jaguar Land Rover to integrate its L4 autonomous technology in their vehicles.[9] Waymo has also partnered with Daimler to develop L4 trucks.

Figure 1: SAE levels of driving automation



[6]Companies mentioned in the report alongside their ticker are Singularity Fund portfolio companies.
[7]Reuters, "Honda's part self–driving Legend a big step for autonomous tech." March 4, 2021, https://www.reuters.com/article/us-honda-autonomous-legend-idUSKBN2AW0TZ
[8]Joseph White, "Waymo opens driverless robo–taxi service to the public in Phoenix." Reuters, October 8, 2020, https://www.reuters.com/article/us-waymo-autonomous-phoenix-idUSKBN26T2Y3
[9]Andrew J. Hawkins, "Volvo will use Waymo's self–driving technology to power a fleet of electronic robotaxis." The Verge, June 25, 2020, https://www.theverge.com/2020/6/25/21303324/volvo-waymo-l4-deal-electric-self-driving-robot-taxi

Demand for autonomous trucks has accelerated as the explosion of e–commerce since the pandemic has created an increased demand for shipping and, subsequently, for drivers. In the first half of 2021, investors pumped US$5.6 billion into autonomous trucking companies such as TuSimple, Plus,[10] and Embark. Trucks should become cheaper and more convenient, and we expect distributed trucking networks to form along fixed and predictable transportation routes in the next 2–3 years, giving the logistics industry a boost. Advances in trucking automation should also greatly reduce the volume of greenhouse gas emissions that originate from road freight transport.

2. Autonomous Trucks And Adas Suppliers Show Most Promises

TSG sees evidence that autonomous trucks and lower level (L1–L3) autonomous systems captured by ADAS suppliers are poised for significant near–and–medium term growth.

The American Trucking Association estimates the trucking industry needs more than 60,000 additional drivers in the U.S. alone to meet growing demand, with the number increasing to 160,000 drivers by the end of the decade.[12] TSG expert Lukas Schleuniger points to this shortage as a key factor propelling the autonomous trucking segment.[13]

From a technological standpoint the case for autonomous trucking is also encouraging. Both autonomous cars and autonomous trucks rely on similar underlying technologies: sensors (Singularity Sector: Robotics) –– typically cameras, lidars, and radars – feed data (Singularity Sector: Big Data) to a computer (Singularity Sector: IoT), which in turn controls the vehicle using skills learned through a massive amount of training and simulation (Singularity Sector: AI). In principle, developing an autonomous truck can be easier than developing an autonomous car.

Unlike passenger vehicles, trucks –– in particular long–haul tractor trailers –– generally follow fixed routes and spend more time on highways that are overall more predictable and easier to navigate than surface streets.[14] Trucks are also a better platform for autonomy. Their large size provides more power for AI computations and an improved field of view for sensors, which can be mounted higher off the ground.

TSG portfolio companies including Velodyne (VLDR; SC: 100) and Luminar Technologies (LAZR; SC:100) are active players in the autonomous trucking industry. Luminar has partnered with Daimler (DAI; SC: 23) and Volvo (VOLVB; SC: 3) to deliver its lidar sensor solutions for the rollout of their highway autonomy solutions. Velodyne cooperates with Beijing Truck Technology Co. (Trunk.Tech) to develop next–generation autonomous heavy trucks for China's logistics market. Trunk.Tech is the first company in China to develop L4 driverless trucks.[15] China's logistics market is expected to generate revenues worth RMB 15 trillion by 2025[16], in turn driving demand for advanced transport solutions. In June, Chinese e–commerce giant Alibaba (9988 HK; SC: 13) announced that it is working with its logistics arm, Cainiao, to develop self–driving trucks to support its e–commerce business. Chinese internet company, Baidu (9888 HK; SC: 88), and auto manufacturer NIO (NIO US; SC: 95), are also engaged in this sector –– as are a growing number of ADAS players.

In contrast to the 'go big or go home' - full autonomy or nothing at all – solutions pursued by some driverless groups including Trunk.Tech, Baidu, and Waymo, ADAS players are taking a step–by–step approach that allows them to improve their existing driver–assistance technologies as a step–change toward greater automation. For example, Canadian mobility company, Magna, is building on its long legacy of driver-assistance to develop semi–to–full–autonomous solutions.

[12]American Trucking Association, Truck DriverShortage Analysis 2019, July 2019.
[13]Lukas Schleuniger, Email communication, 2 September 2021.
[14]Rodney Brooks, 'The big problem with self–driving cars is people,' IEEE Spectrum, July 27, 2017, https://spectrum.ieee.org/the-big-problem-with-selfdriving-cars-is-people
[15]Velodyne Lidar, 'Velodyne Lidar and Trunk.Tech announce strategic partnership in autonomous trucking," January 19, 2021, https://velodynelidar.com/press-release/trunk-tech-in-autonomous-trucking/
[16] Markets Insider, 'Chinese logistics industry is expected to generate revenues worth 15 RMB trillion by 2025,' July 13, 2021. Available online: http://markets.businessinsider.com/news/1030602208

Its Max4 driving platform builds on its cruise control, sensor, and emergency services to allow for up to Level 4 autonomous driving. Magna supplies over 50 global original equipment and trucking manufacturers, including Caterpillar (CAT; SC: 5), Hyundai, and CNH Industrial (CNHI; SC: 9). This network, together with the millions of vehicles around the world that are already equipped with some form of Magna's driver–assistance technology, allows the company to quickly scale its advanced autonomy solutions.

Other ADAS providers benefit from similar advantages, which is why TSG believes they are likely to accelerate their performance and capture a critical share of the autonomous vehicle market. The global ADAS market was worth US$25 billion in 2020 and is projected to reach US$69 billion by 2027.[17] Due to stricter regulations on L4 features, Europe is expected to lead all other regions in ADAS penetration by 2025.[18] TSG expert Sebastian Guenther additionally points to the continent's more complex traffic patterns as a potential challenge for L4 and L5 automation, and an opportunity for ADAS.[19]

3. Self-Driving Vehicles Are Vulnerable To Cyberattacks

Underpinning all of this is the need for driver and vehicle safety and security. Sebastian notes, "key to the autonomous opportunity is getting cybersecurity right."[20]

Autonomous vehicles employ a combination of high-tech sensors and innovative algorithms to detect and respond to their surroundings, including radar, lidar, drive–by–wire control systems, odometry, and computer vision. In other words, at its core, a self–driving vehicle is a blend of networked components (known as electronic control units, or ECUs), some existing within the vehicle and others existing outside of it. These complex systems provide AVs the data and intelligence to make autonomous decisions – but they also create attack vectors for hackers.

If, for instance, hackers manage to gain access to a vulnerable, peripheral ECU – for instance, a vehicle's infotainment – from there they may be able to take control of safety critical ECUs like its brakes or engine.

In 2015, security researchers Miller and Valasek demonstrated exactly this, and showed how a Jeep Cherokee can be hacked remotely via its internet connection.[21] The team was able to take over the Jeep's steering unit, causing it to mimic the braking system and paralyze the car on a highway. In a series of additional experiments, Miller and Valasek exploited the rudimentary (L1–L2) automated features of the targeted vehicles. For example, they used Toyota's collision avoidance system to apply brakes on a Toyota Prius; the Jeep's cruise control to accelerate, and its automated parking system to turn the steering wheel by tricking the car into thinking that it was parking when in fact it was going 80 miles per hour during the test. In other words, the hacks were limited in scope to a few functions controlled by the on–board computers in standard cars.

Now, every aspect of an AV can theoretically be hacked as all control systems are administered by computers. White–hat and black–hat hackers have already started to implement a wide range of attacks against moving and stationary AVs, sometimes with the aim of stealing them, their cargoes or data, and other times to upset their proper performance. An analysis of all publicly reported automotive cyber incidents in 2020 found that 36% of incidents involved data and privacy breaches, and 28% vehicle theft.[22]

[17]Blue Weave Consulting, 'Global advanced driver assistance systems (ADAS) market set to flourish,' April 2019, https://www.blueweaveconsulting.com/advanced-driver-assistance-systems-adas-market
[18]Konstantin Shirokinskiy, Wolfganga Bernhart, and Stephan Keese, 'Advanced driver–assistance systems: A ubiquitous technology for the future of vehicles.' Roland Berger, March 31, 2021, https://www.rolandberger.com/en/Insights/Publications/Advanced-Driver-Assistance-Systems-A-ubiquitous-technology-for-the-future-of.html
[19]Sebastian Guenther, Telephone communication, 31 August 2021.
[20]Ibid.
[21]Andy Greenberg, 'Securing driverless cars from hackers is hard. Ask the ex-Uber guy who protects them,' Wired, April 12, 2017, https://www.wired.com/2017/04/ubers-former-top-hacker-securing-autonomous-cars-really-hard-problem/
[22]Upstream Security, Global Automotive Cybersecurity Report 2021

4. Cybersecurity For Trucks To Occupy Largest Automotive Cyber Segment

Malicious commands can arise from a number of different sources. Vehicle accessories are a big source of risk. Autonomous vehicles increasingly ship with USB ports and WiFi, Bluetooth, or other communication protocols intended to make it easy for vehicles to communicate with accessories. This increases the risk that malware–infected applications could be introduced to the vehicle. A simple example is an attack against the wireless link used for electronic keys, with theft of a vehicle or its cargo as the goal.

Autonomous trucks may be at particular risk. Trucks share a common communications standard, SAE J1939, that makes it possible for hackers to devise a one–size–fits–all attack that could potentially access an entire trucking fleet. As ransomware attacks also become more common, trucks may be in even greater danger. Because they are relied on to transport goods and services, holding a fleet of trucks for ransom is likely to yield a quicker payment than in the case of other AVs as the cost of not delivering goods is in most cases too high. This is why TSG believes cybersecurity solutions for autonomous trucks will occupy the largest segment of the automotive cybersecurity market.

Self-driving vehicles can also be hacked from external vectors. Vehicle–to–vehicle (V2V) and vehicle–to–external (V2X) are evolving paradigms that automakers have started to introduce in connected and autonomous vehicles, including autonomous trucks. V2V allows vehicles to communicate with others on the road to share data on traffic flow, accidents, or poor weather, while V2X enables communication with other connected devices like smart home systems and traffic lights. These communication channels are an invaluable source of data for the guidance and control systems of autonomous vehicles, but also make them more susceptible to being attacked or tracked.

5. Machine Learning And Blockchain Provide Security

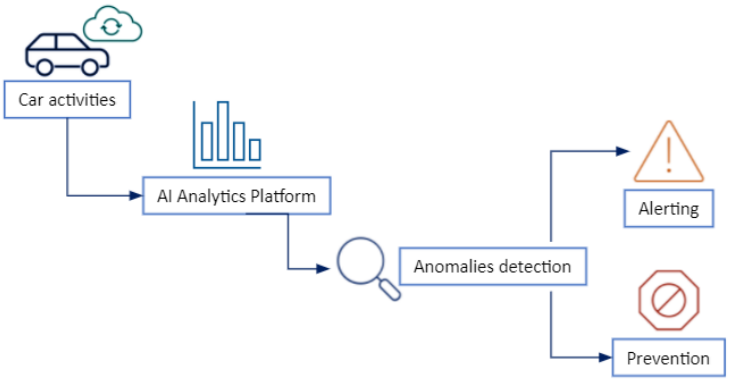
We believe machine learning and the blockchain technology offer promising security solutions for autonomous vehicles, with growth potential. The AI in cybersecurity market is projected to grow at a CAGR of 23.6% during 2020–2027 to reach US$46.3 billion.[23] Most blockchain for security solutions are in the research and development phase, with the global blockchain market expected to reach US$72 billion by 2026.[24]

The best mental model for understanding how automotive cybersecurity solutions work is to envision them as having several layers of defense. Starting at the foundation, defensive software solutions can be housed locally on individual ECU's –– for instance, a vehicle's brakes –– to reinforce these ECUs against attacks. Israeli cybersecurity provider Argus and Germany's Siemens (SIE GR) are among the companies that provide security software solutions that can be embedded directly in ECUs. Private blockchain players like Cube, based out of the U.K., and the U.S.' NXM Labs are also early players in this market. In this case, blockchain could potentially be used to secure AV systems by decentralizing their administration, giving individual ECUs the ability to make their own decisions. Normally, hackers gain access to an autonomous vehicle by penetrating one ECU which then gives them full control of all others. By decentralizing an AV's authority systems, blockchain could likely ensure such attacks are harder to execute.

Moving up a level, machine learning software can protect a vehicle's overall internal network by monitoring all network communications, flagging any changes in standard in–vehicle network behavior, and stopping attacks from advancing in the network. Figure 2 illustrates how a vehicle's data logs could flow into such a database, allowing for detection of potential security exploits.

[23]Meticulous Research, Artificial Intelligence (AI) in Cybersecurity Market, June 2020.
[24]KBV Research, Global Blockchain Technology Market, 2021–2027, April 2021.

Figure 2: Example of vehicle data log flows with AI



Next, solutions exist to defend the particular electronic units that are involved in V2V and V2X operations. This is an important layer in the overall cybersecurity defense system, because it represents the border between a vehicle's internal network and the external world. For example, Japan's Denso Corporation (6902 JP; SC:13) will monitor an AV's in–vehicle technology to ensure authentication of external connections, as well as authentication to improve in–vehicle network security. Nvidia's (NVDA; SC:100) Drive AGX AI–powered security platform similarly processes data from a vehicle's camera, radar, and lidar sensors to perceive a vehicle's real–time environment, localize it to a map, and support and protect driver monitoring. Nvidia's deep learning systems are used by automakers including Tesla (TSLA; SC: 85), Toyota (7203 JP; SC:9), and Volkswagen (VOW3 GR; SC:14).

Finally, cloud security services can detect and correct threats before they reach a vehicle. They can also send the vehicle over–the–air (OTA) updates and intelligence in real time. Cloudflare's (NET; SC: 100) Orbit is a leading solution in this area. It creates a secure and authenticated connection between an autonomous vehicle and its origin server. ADAS providers are also engaged in this space. Aptiv, Magna, and Mobileye all provide security architecture for OTA updates to their advanced driver–assistance systems.

Conclusion

We believe there is a big wave coming in the autonomous vehicle industry that is not necessarily well appreciated. While there has been much focus on the expansion of autonomous vehicles for shared mobility, the trucking sector has so far received less attention. Yet a variety of factors combine to position autonomous trucks for growth, including their potential to reduce shipping expenses not only when compared with those of traditional trucking but also with those of rail, while at the same time offering the door–to–door service that rail cannot. The relationships that companies like Waymo, Velodyne, Luminar are making within the trucking industry are in this regard notable.

The likelihood that driver–assistance systems continue to advance, even if slowly, is also high. As more vehicles become equipped with the technology, the faster the systems learn. Here, the vast and established customer networks maintained by ADAS players are a big advantage. Navigation specialist TomTom (TOM2 NV; SC: 26), for example, has equipped more than three million vehicles with its high–definition maps accurate to a few centimeters that receive near real–time updates. The continuous stream of data generated by the maps has allowed the company to develop its own AV.[25] Like other ADAS suppliers, TomTom works closely with a network of cybersecurity partners to ensure the integrity of its systems. Cyberspace has met the road and automotive cybersecurity is paramount.

In both the development of autonomous vehicle solutions and in ensuring their security, Singularity Sectors – AI, big data, IoT, robotics, and blockchain – and TSG companies are at the forefront. This is no longer a science project; it is applied innovation –– proven that it can be done. The impact of autonomous vehicles will reverberate across industries and the environment.

[25]Paul Sawers, 'TomTom launches a fully autonomous test car to develop HD maps,' Venture Beat, September 5, 2019, https://venturebeat.com/2019/09/05/tomtom-launches-a-fully-autonomous-test-car-to-develop-hd-maps/