Cybersecurity and the Adoption of Self-Driving Cars

Pedro dos Santos Braz

Dissertation written under the supervision of Professor Peter V. Rajsingh and Professor Damien Forterre

Dissertation submitted in partial fulfilment of requirements for the MSc in International Management at CLSBE, at Universidade Católica Portuguesa and for the Master in Management at ESCP Business School, September 2024.

Abstract

This dissertation investigates the impact of cybersecurity concerns on adopting autonomous vehicles (AVs). As AV technology becomes increasingly prevalent in modern transportation systems, it faces potential cybersecurity threats such as data breaches, remote hijacking, and unauthorized data access. While these issues pose challenges, they are not inevitable barriers to consumer acceptance and widespread adoption.

This study employs a mixed-methods approach, combining quantitative data from consumer surveys of a sample of 239 respondents with qualitative insights from 12 expert interviews from the automotive and cybersecurity sectors to assess public perceptions and the effectiveness of current cybersecurity measures. The results show that most consumers do not unthinkingly oppose the adoption of AVs despite the significant cybersecurity risks as long as robust cybersecurity protections are implemented.

The research underscores the importance of transparent communication and the development of comprehensive regulatory frameworks to build and sustain public trust. Proactive cybersecurity strategies, continuous technological updates, and solid regulatory oversight can effectively mitigate risks and encourage the adoption of AV technologies. This study offers insights into the dynamic interplay between technology adoption, public perception, and cybersecurity, providing strategic guidance for policymakers and industry stakeholders to navigate these challenges.

Keywords: Autonomous Vehicles, Cybersecurity, Consumer Acceptance, Innovation Diffusion, Public Perception, Risk Mitigation

Title: Cybersecurity and the Adoption of Self-Driving Cars

Author: Pedro dos Santos Braz

Resumo

Esta dissertação investiga o impacto das preocupações com a cibersegurança na adoção de veículos autónomos (VAs). À medida que a tecnologia VA se torna cada vez mais prevalente nos sistemas de transporte modernos, esta enfrenta potenciais ameaças à cibersegurança, como violações de dados, sequestros remotos e acesso não autorizado a dados. Ainda que estas questões representem verdadeiros desafios, elas não são barreiras intransponíveis para a aceitação dos consumidores e para a adoção generalizada.

Este estudo utiliza uma abordagem de métodos mistos, combinando dados quantitativos de inquéritos a consumidores de uma amostra de 239 inquiridos com perceções qualitativas de 12 entrevistas com especialistas dos setores automóvel e de cibersegurança para avaliar as perceções públicas e a eficácia das medidas de cibersegurança atuais. Os resultados mostram que a maioria dos consumidores não se opõe de forma irrefletida à adoção dos VAs, apesar dos riscos significativos de cibersegurança, desde que sejam implementadas proteções robustas.

A pesquisa sublinha a importância da comunicação transparente e do desenvolvimento de quadros regulatórios abrangentes para construir e sustentar a confiança pública. Estratégias proativas de cibersegurança, atualizações tecnológicas contínuas e uma supervisão regulatória sólida podem mitigar eficazmente os riscos e encorajar a adoção das tecnologias VA. Este estudo oferece insights sobre a interação dinâmica entre a adoção de tecnologia, a perceção pública e a cibersegurança, fornecendo orientações estratégicas para os decisores políticos e as partes interessadas da indústria de forma a navegar por estes desafios.

Palavras-chave: Veículos Autónomos, Cibersegurança, Aceitação do Consumidor, Difusão da Inovação, Perceção Pública, Mitigação de Risco

Título: Cibersegurança e a Adoção de Carros Autónomos

Autor: Pedro dos Santos Braz

Acknowledgements

This document signifies the culmination of my academic journey, including my Double Degree Master's program at Católica-Lisbon and ESCP. It has been an enriching experience.

First and foremost, I am deeply grateful to my dissertation supervisors, Peter V. Rajsingh and Damien Forterre, for their invaluable guidance and steadfast support throughout the dissertation process. I also wish to extend my appreciation to all the distinguished professors from whom I had the privilege to learn at both institutions.

The dissertation also benefited from numerous contributions by various individuals, each playing an essential role in the project's success. I am thankful to all the experts who were interviewed for sharing their insights and dedicating their time to my research, and I equally appreciate everyone who participated in my survey.

Many others also deserve recognition for their support during this pivotal chapter of my life. I must especially acknowledge my parents' constant support and presence during these transformative years, even when I chose less conventional paths. This gratitude extends to all my family members, who were always there for me when I needed them.

I am equally thankful to my friends from Aerospace Engineering, particularly Álvaro, Cristele, Dar'ya, Eva, Francisco, Frederico, Inês, João, Miguel C., Miguel I., Miguel J., Pedro M., and my "Aero family" at Instituto Superior Técnico. Their support during those three intensive yet fulfilling years was crucial and continues to this day.

Here at Católica, I met extraordinary individuals such as Joana, João O., José, Inês C., Inês H., Leonor, and Mariana, who were great companions during this fantastic phase of this journey. Special thanks go to João and Vicente, who (literally) traveled with me throughout the entire Master's program, from Lisbon to Paris.

In the last year of my Master's, I am grateful for the friendships I formed in the Investment Banking specialization, as well as for my Double Degree colleagues at ESCP.

Lastly, I extend my thanks to all the incredible individuals I encountered through projects outside of the university over these years, namely friends from Grupos, EJNS, Missão País, and CCL.

To all of them, as we say in Beira Interior, "um bem-haja".

Pedro

Table of Contents

Abstract I

Resumo II

Acknowledgements III

List of Figures VIII

List of Tables IX

List of Abbreviations X

1 Introduction 1

2 Literature Review 4

2.1 Current Trends in the Automotive Sector 4

2.1.1 Autonomous Vehicles 4

2.2 Current Trends in the Cybersecurity Field 7

2.2.1 Key Challenges 9

2.3 Cybersecurity in the Automotive Sector 10

2.4 Cybersecurity in Autonomous Vehicles 11

2.4.1 Risks 11

2.4.2 Regulations 14

2.4.3 Mitigation and Possible Solutions 15

2.4.4 Public Perception 16

2.5 Key Concepts of Innovation 18

2.5.1 Creative Destruction 18

2.5.2 *The Innovator's Dilemma* and the DCF trap 18

2.5.3 Understanding Market Pull and Technology Push in Innovation 19

2.5.4 Exploring the Diffusion of Innovation and the Technology Acceptance Model 20

2.6 Exogenous Shocks and Dynamic Capabilities 21

2.6.1 Exogenous Shocks and the Concept of Fit 21

2.6.2 Dynamic Capabilities 22

2.6.3 Examples of Dynamic Capabilities in Action 23

3 Methodology **24**

3.1 Research Design 24

3.2 Data Collection 25

3.2.1 Primary Data Collection - Expert interviews 25

3.2.2 Primary Data Collection - Consumer insights survey 27

4 Analysis and Discussion **28**

4.1 Cybersecurity Risks and Mitigation Strategies 28

4.1.1 Cybersecurity Risks in the Automotive Sector 28

4.1.2 Automotive Sector Readiness for Cybersecurity Concerns 31

4.1.3 Materiality of Cybersecurity Concerns on Public Perception 34

4.1.4 Possible Mitigation Strategies for Cybersecurity Concerns 36

4.1.5 Is Cybersecurity a Potential Barrier? 40

4.2 Current levels of public concerns regarding self-driving cars 43

4.2.1 General Familiarity and Perception of AVs 43

4.2.2 Willingness to Adopt AVs of Different Levels 45

4.2.3 Cybersecurity Awareness and Concerns 46

4.2.4 Willingness to Adopt AVs of Different Levels After Cybersecurity Awareness and Concerns 49

4.2.5 Adoption and Acceptance of AVs 51

4.2.6 Demographics and Background 55

4.2.7 Differences in Adoption of AVs at Different Autonomy Levels Before vs. After Cybersecurity Awareness 61

4.2.8 Determinants of consumers' willingness to adopt AVs 63

5 Conclusions **75**

5.1 Main Findings - Triangulation 75

5.1.1 Theoretical Implications 77

5.1.2 Practical Implications 78

5.2 Limitations 79

5.2.1 Expert Interviews 79

5.2.2 Survey 79

5.3 Future research 80

Bibliography **A**

Appendices

Appendix A: Outline of survey questions L

Appendix B: Expert Interviews . . . . . N

.1 Interview scripts . . . . . N

.2 Summary of interview 1: AW . . . . . O

.3 Summary of interview 2: AR . . . . . Q

.4 Summary of interview 3: EC . . . . . S

.5 Summary of interview 4: PG . . . . . U

.6 Summary of interview 5: JF X

.7 Summary of interview 6: PR . . . . . Z

.8 Summary of interview 7: ES . . . . . AB

.9 Summary of interview 8: JB . . . . . AD

.10 Summary of interview 9: CR . . . . . AG

.11 Summary of interview 10: FM . . . . . AI

.12 Summary of interview 11: LS . . . . . AK

.13 Summary of interview 12: JS . . . . . AM

List of Figures

1 Self-driving Cars Market Size, By Region, 2018-2030 (Polaris Market Research, 2022) 1
2 Level of autonomy in autonomous vehicles from 0 to 5 (Goldman Sachs, 2022) 5
3 Research Design 24
4 Cybersecurity risks mentioned by experts per type of expert 29
5 Cybersecurity risks mentioned by experts per type of expert 37
6 Answers to the question “Based on our discussion, do you feel that cybersecurity concerns are currently a major barrier to the adoption of self-driving cars?” per type of expert 40
7 Answer distribution of question 1 44
8 Answer distribution of questions 2 and 3 44
9 Answer distribution of question 4 45
10 Answer distribution of question 5 46
11 Answer distribution of question 6 47
12 Answer distribution of question 7 48
13 Answer distribution of question 8 49
14 Answer distribution of question 9 50
15 Answer distribution of question 10 51
16 Answer distribution of question 12 52
17 Answer distribution of question 13 53
18 Answer distribution of question 14 54
19 Answer distribution of question 15 55
20 Answer distribution of question 16 56
21 Answer distribution of question 17 56
22 Answer distribution of question 18 57
23 Answer distribution of question 19 58
24 Answer distribution of question 20 58
25 Answer distribution of question 21 59
26 Answer distribution of question 22 60
27 Answer distribution of question 23 60
28 Regression Results for the First Attempt of Model for Level 0 and 1 67

29 Regression Results for the First Attempt of Model for Levels 2 and 3 67
30 Regression Results for the First Attempt of Model for Levels 4 and 5 68
31 Regression Results for the Final Model for Levels 0 and 1 69
32 Regression Results for the Final Model for Levels 2 and 3 69
33 Regression Results for the Final Model for Levels 4 and 5 70

List of Tables

1 Overview of interviewees 26
2 Categorized Cybersecurity Risks in Autonomous Vehicles 28
3 Categorized Mitigation Strategies for Cybersecurity Risks 36
4 Paired Sample t-Test Results for Willingness to Adopt AVs at Different Autonomy Levels 62
5 Frequency of Significant Independent Variables 64
6 Survey Questions Outline L

List of Abbreviations

ADS	Autonomous Driving Systems
AI	Artificial Intelligence
ASDL	Automotive Secure Development Lifecycle
AV	Autonomous Vehicle
CAM	Connected and Automated Mobility
CAN	Controller Area Network
DCF	Discounted Cash-Flow
DLE	Direct Lithium Extraction
EU	European Union
EV	Electric Vehicle
ICE	Internal Combustion Engine
IoT	Internet of Things
IT	Information Technology
ML	Machine Learning
OBD	On-board Diagnosis
OEM	Original Equipment Manufacturer
OT	Operational Technology
OTA	Over-the-Air
PEOU	Perceived Ease of Use
PU	Perceived Usefulness
RQ	Research Question
TAM	Technology Acceptance Model
UK	United Kingdom
US	United States
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2V PKI	Vehicle-to-Vehicle Public Key Infrastructure
V2X	Vehicle-to-Everything
WEIRD	Western, Educated, Industrialized, Rich and Democratic

1 Introduction

The emergence of autonomous vehicles, also known as self-driving cars, has sparked significant interest due to their potential to revolutionize the transportation sector. These cutting-edge vehicles promise enhanced safety, efficiency, and accessibility, announcing a paradigm shift in commuting. However, as self-driving cars become more entwined with advanced technologies, they face challenges, in particular escalating cybersecurity threats that could undermine their acceptance and use. This research, exploring cybersecurity threats in autonomous vehicles, aims to shed light on these emerging challenges (Nash et al., 2024).

The importance of this topic lies in the increasing prevalence of autonomous vehicles in contemporary transportation networks. The demand for such cars is forecast to expand consistently over the next ten years, indicating that this represents a growing market evolving from a mere concept to a tangible reality and penetrating key global markets (Polaris Market Research, 2022). As a result, understanding the implications and challenges associated with their widespread adoption becomes increasingly crucial for policymakers and industry stakeholders alike.

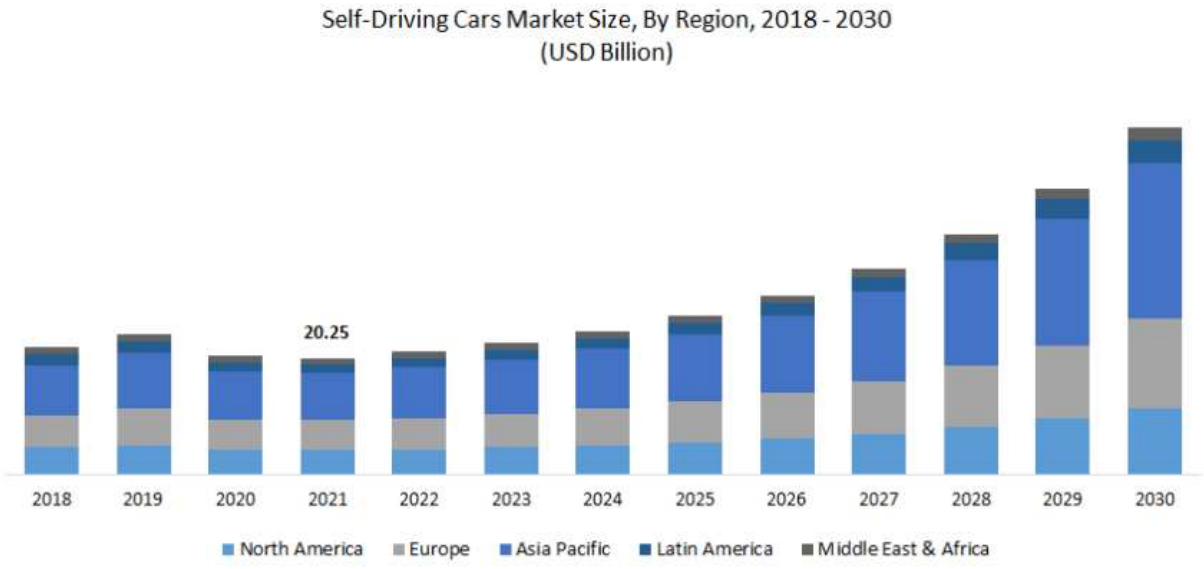

Figure 1: Self-driving Cars Market Size, By Region, 2018-2030 (Polaris Market Research, 2022)

In parallel with the potential market expansion, there is growing recognition of cybersecurity as a crucial concern for its advancement. Autonomous cars heavily rely on intricate sensor systems, onboard computers, and vehicle-to-infrastructure connectivity, which present new cybersecurity vulnerabilities (George et al., 2023). Essentially functioning as computers on wheels, these vehicles contain numerous processors and microprocessors, increasing the potential for exploitation

(Eliot, 2021). Because of this, concerns about the vulnerability of these vehicles to hacking and data misuse have raised considerable unease regarding cybersecurity and data privacy issues, potentially affecting their adoption (Prasetio & Nurliyana, 2023).

Autonomous cars are vulnerable to a range of cyber risks such as hacking, malicious software, and unauthorized access to sensitive data (Eliot, 2021; Nash et al., 2024). For instance, shared vehicles could store data from numerous users, making them susceptible to cyber theft. Likewise, connected and self-driving cars open up new possibilities for harmful ransomware attacks. As mobility managers gain a more comprehensive understanding of people's movements and activities, safeguarding against potential data exploitation becomes increasingly essential (Nash et al., 2024).

These vehicles' intricate design and interconnectedness make them susceptible to cyberattacks that could disrupt or even destroy them. As such, the prospect of hackers gaining control over a vehicle's operation, leading to malfunctions or crashes, is a primary concern. This poses a significant threat that could not only hinder consumer trust and adoption of this technology but also potentially endanger lives (Tomorrow Bio, 2023). Given these concerns, it is crucial to adopt a comprehensive strategy for cybersecurity to guarantee the secure and extensive implementation of autonomous vehicles.

The future of transportation, thus, is vulnerable to cybersecurity threats, particularly in the context of self-driving vehicles. The intricate relationship between ethics, threats, vulnerabilities, and market demands underscores the complexity of this issue (Nobles et al., 2023). Understanding and mitigating cybersecurity issues will be essential for successful integration as autonomous vehicles become more ingrained in society. This dissertation aims to examine whether cybersecurity concerns will impede the adoption of self-driving cars and how innovative measures can effectively address these challenges - ultimately ensuring a secure and robust future for autonomous transportation. Therefore, the primary research question driving the development of this study was the following:

RQ: How will cybersecurity concerns affect adoption of self-driving cars?

The investigation begins by examining current developments in both the automotive industry and the cybersecurity domain. Next, cybersecurity within the automotive sector as a whole will be assessed, and then focus specifically on autonomous vehicles; this section ends by exploring management theory related to innovation and to dynamic capabilities. Following that, the

methodology is outlined and includes details about research design and data collection methods for expert interviews and a consumer survey. The next chapter analyzes and discusses results from both sets of data collections before moving on to subsequent chapters. The concluding chapter presents key findings along with their theoretical and practical implications and the research limitations while also discussing paths for future research.

As mentioned, this question gains significance in light of increasing prevalence of autonomous vehicles and the growing complexity of their sensor systems, onboard computers, and connectivity, all of which introduce significant new cybersecurity risks (George et al., 2023). Introducing self-driving cars presents an opportunity to revolutionize transportation, but it also introduces new risks and obstacles, particularly in cybersecurity.

2 Literature Review

2.1 Current Trends in the Automotive Sector

The automotive market is currently undergoing significant transformations. Projections indicate that the sector will grow from US$315 billion in 2020 to approximately US$405 billion by 2030. This is mainly due to novel value propositions encompassing aspects such as fuel efficiency savings, enhanced safety features, and improved driving enjoyment (Goldman Sachs, 2022, 2023a). Nonetheless, this increase in profitability could exacerbate competitive pressures as entities outside the industry seek market entry.

Over the next decade, electrification of vehicles, moving away from internal combustion engines (ICEs), and the development of autonomous vehicle (AV) technology are expected to drive growth (Boston Consulting Group, 2023; Oliver Wyman, 2019). On another note, some analysts suggest a slowdown in electric vehicle momentum due to high costs and interest rates, alongside consumer concerns over electric vehicle (EV) range, recharge times, and charging infrastructure (Deloitte, 2024).

Consumer choices are heavily influenced by price in developed economies, while performance and quality are prioritized elsewhere (McKinsey & Company, 2024). Additionally, younger demographics (18 to 34-year-olds) are willing to try subscription models instead of traditional ownership, reflecting changing perceptions around ownership (Deloitte, 2024; EY, 2022).

Direct lithium extraction (DLE) is a technology that extracts lithium more efficiently, sustainably, and economically than conventional extraction techniques (Deloitte, 2023). DLE strives to procure lithium from brine solutions directly, eliminating extensive evaporation ponds and thereby diminishing environmental impact (Goldman Sachs, 2023b). Another trend in the automobile sector is lightweighting, which plays a crucial role in modern mobility by enhancing sustainability, cost-efficiency, and performance (Czerwiński, 2021).

2.1.1 Autonomous Vehicles

The current autonomous vehicle landscape is marked by continuous technological progress, experimentation, and limited commercial launches. In 2020, a vast majority of the vehicular presence on roads comprised level 0 (non-automated) or level 1 (driver assistance system-equipped) vehicles, with a lesser fraction appearing at automation levels such as level 2 (partial automation)

or beyond (MIT CSAIL, 2020).

Nonetheless, there have been notable strides within the sector; for instance, companies like Honda and Mercedes-Benz have successfully introduced level 3 autonomous vehicles to the market alongside numerous automotive manufacturers diligently pursuing advancements in their respective autonomous driving offerings (Goldman Sachs, 2022; Mercedes-Benz, 2023). A more detailed explanation for each level of autonomy is shown below in Figure 2.

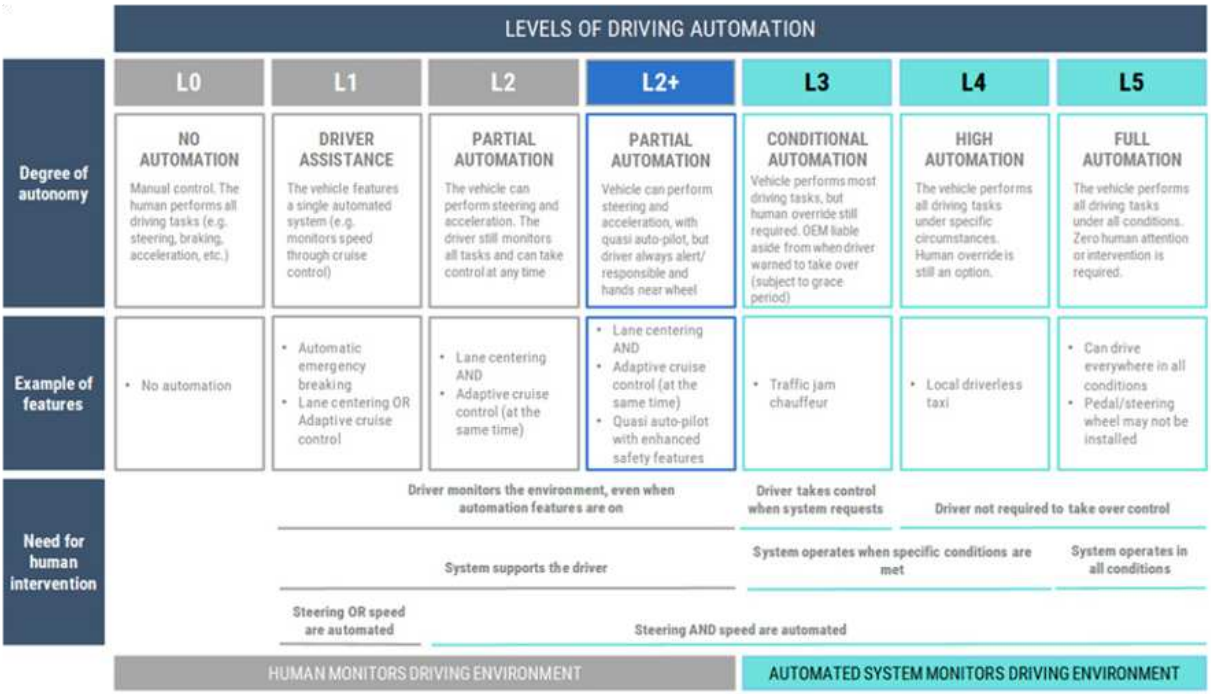

Figure 2: Level of autonomy in autonomous vehicles from 0 to 5 (Goldman Sachs, 2022)

Analysts predict that, by 2030, autonomous vehicle sales globally will reach approximately 20% at level zero, 36% at level one, and nearly 30% across levels two through two plus, culminating at around 15% at level three autonomy or greater (Goldman Sachs, 2022). This suggests significant advancements in self-driving technology (Deloitte, 2022). During this time, there is expected to be a marked shift towards the highest levels of autonomous capabilities.

Automotive sector innovators of this new technology include Original Equipment Manufacturers (OEM) such as Tesla, Mercedes-Benz, and Honda; auto-tech suppliers including Innoviz, Denso, and Aptiv; as well as information technology (IT) sector enterprises such as Alphabet and Baidu. These firms have competencies spanning scalable products, software innovations, and autonomous driving technologies alongside comprehensive business strategies (Goldman Sachs, 2022). They are essential in guiding the automotive industry's evolution towards enhanced electrification and autonomy (Markit, 2022).

The pace at which autonomous driving features are introduced reflects continuous improvement and deployment, leading to enhanced vehicle automation and operational efficiency (McKinsey & Company, 2023). As the costs of these systems are expected to decrease, autonomous driving technologies will become more accessible to both consumers and manufacturers (Deloitte, 2022).

At the same time, improvements in sensor technologies, such as LiDAR, radar, and cameras, are set to improve the perception and navigation abilities of these vehicles, which, along with increasing consumer acceptance due to economic benefits like lower costs per mile, also sets the stage for broader adoption (Ayala & Mohd, 2021; KPMG, 2020). Moreover, regulation is supporting this advancement, further propelling this technological evolution (Goldman Sachs, 2022).

Arguably, the most significant advantage of AVs would be their contribution towards significantly reducing accidents and, therefore, deaths on the road (Prasetio & Nurliyana, 2023). The reduction or elimination of human error reduces road incidents, thereby enhancing safety (Nobles et al., 2023; Prasetio & Nurliyana, 2023). Machine learning (ML) and artificial intelligence (AI) are developments that will make level 5 self-driving cars much safer (Nobles et al., 2023).

This growing field has attracted substantial funding and also holds the promise of creating numerous new job opportunities (KPMG, 2020). Consider the United Kingdom (UK), where the government has secured over £60m of new R&D funding to propel the AV sector from the lab to the commercial market (UK Department for Transport, 2022). This is a tangible testament to the sector's potential to stimulate economic growth and job creation.

Looking beyond the technology itself, AVs are set to address significant societal challenges, as they become positioned to revolutionize transportation accessibility, especially for groups traditionally limited in mobility, such as the elderly and disabled. This promise of enhanced accessibility is more than just a convenience — it is a step toward greater social inclusion and equality (Tomorrow Bio, 2023; UK Department for Transport, 2022).

AVs also play a vital but often overlooked role in promoting environmental sustainability (UK Department for Transport, 2022). Incorporating AVs into transportation systems reduces greenhouse gas emissions by optimizing driving patterns and alleviating traffic congestion, aligning with the broader international efforts to combat climate change (KPMG, 2020; UK Department for Transport, 2022).

However, concerns regarding vehicle failures have already surfaced. One notable example is the case of Kevin George Aziz Riad, where charges of vehicular manslaughter were brought following a crash caused by his Tesla operating on Autopilot (Krisher & Dazio, 2022). This incident underscores dangers associated with over-reliance on automated systems and resulted in calls for supervision of such technologies in consumer vehicles. The recent crash of a Tesla Model 3 car in Paris, which resulted in the death of the driver, also presents new legal and ethical challenges in the autonomous vehicle landscape, raising questions about the liability and safety of these vehicles (Mehta, 2022). Likewise, the cases of hit-and-run incidents involving autonomous cars in San Francisco expose the difficulties and complexities of integrating driverless technology into urban environments (Ingram, 2023).

Realizing AVs' full potential requires successfully integrating them with existing transportation infrastructures (KPMG, 2020). The target would be to develop an integrated vehicle ecosystem in which the vehicle collaborates with other automated vehicles to multiply the results, therefore increasing the effectiveness and efficiency of the overall transport network (UK Department for Transport, 2022).

2.2 Current Trends in the Cybersecurity Field

With the rapid adoption of new technologies, cybersecurity challenges are rising (Cisco, 2024). There is a widening digital gap between entities that can effectively incorporate cybersecurity measures and those that cannot (World Economic Forum (WEF), 2024). This division poses a significant risk, increasing vulnerabilities for less prepared entities, as in 2023, only 3% of global organizations had a 'mature' level of cybersecurity readiness, while 75% of companies believed that a cybersecurity incident would disrupt their business in the next 12-24 months (Cisco, 2024).

At the same time, there is a noticeable move towards collective accountability in cybersecurity. Stakeholders such as businesses, government bodies, and individuals are increasingly urged to collaborate to promote sustainable cybersecurity capabilities and address systemic weaknesses (Saeed et al., 2023). This collaborative approach is crucial for bridging the previously mentioned digital gap and improving the overall resilience of digital infrastructure (World Economic Forum (WEF), 2024).

In line with these patterns, the shift in focus within cybersecurity is from just defending against

cyberattacks to also emphasizing the development of cyber resilience – the ability to bounce back from and endure cyber incidents (World Economic Forum (WEF), 2024). This strategic change reflects the need for more resilient and flexible cybersecurity strategies in light of evolving threats.

Another crucial factor influencing today's cybersecurity landscape is the availability of skilled personnel, technology, and security resources. Access to these resources is considered essential for cyber-solid defenses, as it ensures that all organizations, regardless of size or industry, can maintain effective cybersecurity measures (Stedman, 2024).

An organizational culture prioritizing cybersecurity and adapting to changing threats is considered increasingly necessary for achieving effective cyber resilience (Chin, 2023). This entails aligning institutional values and practices with cybersecurity imperatives to ensure that it remains a top priority. To safeguard against cyber threats and quickly adapt to new challenges, it is essential to integrate cybersecurity into everyday business practices and prioritize it at all levels, from leadership to individual employees (Stackpole, 2022).

A significant proportion of enterprises also acknowledge the criticality of security in cloud technology (Ismayilov, 2022). This is integral to evolving cybersecurity strategies as public and hybrid cloud technologies become increasingly central to organizational security frameworks (Luxner, 2023).

Another advancement in cybersecurity strategies is implementation of the Zero Trust Security Model. This model operates on the principle of "never trust, always verify," requiring rigorous identity verification for every individual and device seeking to access network resources, regardless of their position concerning the network's perimeter (Dumitru, 2022; Jena, 2023). This approach represents a comprehensive network security shift beyond specific technologies. It is especially relevant in an era where traditional trust-based security models are proving insufficient against growing cyber threats and data breaches (Saeed et al., 2023).

Also, public-private partnerships are increasingly recognized as essential to improving cybersecurity standards (World Economic Forum (WEF), 2024). By promoting cooperation across different sectors, these collaborations enable the exchange of best practices and threat intelligence, enhancing overall cybersecurity capabilities.

However, these partnerships can also have the opposite purpose. For instance, recently leaked

documents have revealed details of Chinese firms supporting hacking operations, including government targeting requirements and involvement in cyber espionage. The content also affirms the organizations' collaboration with the Chinese authorities to address online gambling and carry out ransomware initiatives (Vicens, 2024).

2.2.1 Key Challenges

The literature emphasizes a landscape where conventional threats merge with new ones, requiring a multifaceted approach to cybersecurity (Gartner, 2023). Phishing continues to pose a significant threat, directly leading to financial fraud and indirectly acting as an avenue for ransomware attacks (Ghazi-Tehrani & Pontell, 2021). This situation presents a paradox: while basic attacks are easier, developing sophisticated and successful attacks demands more effort than previously needed.

The significance of cybersecurity within automation is also important (Mohsienuddin et al., 2020). By 2030, the automation industry is expected to profoundly transform work practices and potentially replace over 800 million workers. With the surge in cyber threats driven by new cloud network attacks and the Internet of Things (IoT), security automation has become a crucial response (Gartner, 2023).

Another challenge is the rapid adoption of new technologies by advanced organizations, creating a gap and leaving others struggling to maintain essential cybersecurity capabilities, as mentioned before in Chapter 2.2. This technology adoption race redefines the cybersecurity landscape (World Economic Forum (WEF), 2024).

As mentioned in the previous chapter, cyber-resilience is also related to zero-sum games. Maintaining high-quality cyber resilience is becoming increasingly difficult due to limited resources and capabilities. This situation highlights the need to strategically allocate resources and develop cybersecurity capabilities (World Economic Forum (WEF), 2024).

On another note, the digital economy's interconnectedness means that cybersecurity incidents can have widespread and accumulating effects (ENISA, 2021). The interconnected nature of digital systems underscores the importance of overall resilience in mitigating the escalating impact of cyber incidents.

Lastly, it is important to stress the increasing prevalence of software supply chain attacks, a trend forecast by the European Union Agency for Cybersecurity (Wang, 2021). These attacks pose a

substantial threat by exploiting vulnerabilities at various software development and distribution stages. The anticipated rise in such attacks highlights their stealth and sophisticated nature, aiming to compromise targets through multifaceted and evasive methods, drawing attention to the critical importance of implementing robust security measures throughout the software supply chain (Kshetri & Voas, 2019).

2.3 Cybersecurity in the Automotive Sector

Rapid advances in the automotive industry, especially cyber-physical systems, bring new cybersecurity challenges. Technologies like the Internet of Things and vehicle-to-everything (V2X) significantly contribute to the development of connected cars, integrating physical processes with computation and networking (Möller & Haas, 2019). IoT makes it possible for vehicles to talk to other devices and infrastructure, which makes this kind of ecosystem very sophisticated, where security holds the most significant importance (Elgazzar et al., 2022).

This pertains to unique functionalities that introduce new vulnerabilities, as evidenced in innovative applications such as car-sharing and connected parking. Thus, the automotive sector is increasingly aware of the need for robust industry standards (Schmittner & Macher, 2019). Among these are the automotive cybersecurity standards of Automotive iQ, the ISO 27000 series on IT security techniques, and the ISO 26262 on the functional safety of road vehicles, all essential components to consider when outlining cybersecurity measures.

Automotive system design and development must incorporate cybersecurity requirements. As discussed in Chapter 2.1.1, levels of autonomy linked with connectivity result in increasing needs for cybersecurity even in vehicle design, making it an integral part rather than an afterthought (Morris et al., 2020; Schmittner & Macher, 2019). As cars evolve into complex nodes within the IoT, addressing cybersecurity vulnerabilities from the beginning becomes increasingly essential.

However, enhancing vehicle performance often conflicts with cybersecurity requirements. As vehicles become more technologically sophisticated with advanced electronics, the industry's value chain is more vulnerable to cybersecurity failures (Morris et al., 2020). For instance, driverless and connected cars rely on sensor data that provides real-time decision-making, thereby expanding their potential attack surfaces and calling for a dynamic cybersecurity approach (Burkacky et al., 2020). To respond to these threats, UNECE WP.29 regulations will require

cybersecurity risk management practices, reflecting the critical need for automotive safety and functionality in cybersecurity (United Nations Economic Commission for Europe (UNECE), 2022).

Due to these risks, the cybersecurity market for the automotive industry is set to double in value by 2030 (Burkacky et al., 2020). It is important to remember that cybersecurity has implications across management practices and organizational strategies as a critical dimension that companies have to address (Morris et al., 2020). There are four primary clusters in automotive cybersecurity: automotive security, vehicle engineering, smart vehicle, and IT security. These areas underscore the need for diverse approaches in this field for future research and strategy (de Arroyabe et al., 2022).

This automotive cybersecurity also includes novelties like blockchain and artificial intelligence. For example, using blockchain can potentially improve operational efficiency and resilience in the specific case of securely sharing information between vehicles (Fraga-Lamas & Fernández-Caramés, 2019). Likewise, AI solutions for vehicular security include applications in anomaly detection, intrusion detection systems, and adaptive security frameworks (Pethő et al., 2021). All these technologies are involved in the increased security of operations while also contributing to increased efficiency and effectiveness in other cybersecurity measures.

2.4 Cybersecurity in Autonomous Vehicles

2.4.1 Risks

The advent of connected vehicle technologies has sparked a rise in remote cyber threats. For instance, it has been reported that 82% of the cyber-attacks taking place in the automotive industry are remote, which includes consumer vehicles, manufacturers, and dealerships, and half of the total number of vehicle theft cases have been blamed on keyless entry systems, showing that the system urgently needs to be secured with solid cybersecurity (Davies, 2023).

Such threats include weak Bluetooth capabilities in Tesla cars, and remote engine start and door unlock without permission in Honda models (Bradley, 2022). This year (2024), a Tesla Modem was hacked on-site at an event, with security researchers from Synacktiv showing off 24 different zero-day exploits and taking home a total of $722,500 (Gatlan, 2024). This case underscores the need for functional cybersecurity in the connected vehicle industry.

Also, in just three years, vehicular cyberattacks have exploded by a whopping 225%, with

the most common forms being data breaches and vehicle thefts, often through wireless critical fob systems (Bradley, 2022). These attackers target even traditional ICE vehicles, potentially cloning key signals and altering engine control units to cause accidents.

As discussed, self-driving cars represent a leap in this sector, from levels 2 or 2+, which require far more human intervention, towards fully autonomous levels 4 and 5 (Goldman Sachs, 2022). As they evolve and become increasingly computerized, AVs open up a range of vulnerabilities that cyber attackers could exploit (Eliot, 2021).

A significant vulnerability in vehicle cybersecurity lies in the OBD (on-board diagnostics) portal, which offers real-time data about a vehicle's status. Often overlooked, this portal grants hackers potential access to manipulate embedded systems, essentially turning the diagnostic tool into an open gateway for cyber threats (Klinedinst, 2016). While requiring physical access to the vehicle limits the scale of potential attacks, the risk remains substantial, especially for fleets of self-driving cars. Thus, robust cybersecurity measures are imperative to mitigate these risks (Ammar et al., 2019).

Also, over-the-air (OTA) technology has transformed how vehicle software updates and data are transmitted, enhancing efficiency and convenience. However, this technology also introduces significant cybersecurity risks, as a compromise in OTA communications could affect not just a single vehicle but an entire fleet (Eliot, 2021). Furthermore, traditional cybersecurity methods, largely reliant on post-release reviews, are increasingly inadequate in the dynamic environment of autonomous vehicles. These vulnerabilities highlight the potential for massive, nearly simultaneous cyber-attacks across fleets, underscoring the urgent need for enhanced protective measures in OTA systems (TechVertu Cyber Security, 2024).

On another note, the Controller Area Network (CAN) is the interior communication network of a vehicle, serving as its backbone. Breaches in this network expose it to manipulation and interference by hackers, posing significant threats to vehicle functionality and security (Khatri et al., 2021; Oladimeji et al., 2023). This vulnerability extends to the broader vehicle communication networks, encompassing both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) connections.

It is essential to point out that AV technology critically relies on these V2V and V2I communication systems, which, while crucial for the operation of autonomous vehicles, introduce new wireless attack vectors that expand the threat landscape significantly. Manipulation of these

technologies can lead to undesired decisions in the AI driving system, potentially endangering road users (K. Kim et al., 2021). Furthermore, cyberattacks can exploit these communication interfaces to alter information, intrude into safety-critical systems, and enable unauthorized vehicle tracking, making them critical targets (Bari et al., 2023).

Viewed through the lens of cybersecurity, this would constitute a significant failure for a self-driving car. The primary concern pertains to the safety of its occupants, representing a critical and alarming consequence since, in case of a breach, the hackers may succeed in hacking the car system, and, because of this, the car can easily experience an accident (Eliot, 2021). This risk may be more pronounced in a vehicle designed for full autonomy with no human intervention.

This is not just a hypothetical situation, since when simulating such attacks against vehicle sensors, they have shown their capability to cause malfunctions, which can compromise vehicle functionality and safety, potentially leading to a crash (Shah & Ali, 2023).

Related to this issue, adversarial machine learning introduces a new level of risk, where malicious actors might design attacks to deceive AI systems. These attacks can also change the decision-making of an autonomous vehicle, leading to unsafe behaviors on the road (Dede et al., 2021). The attacks could involve deceiving vehicles or causing their systems to fail in recognizing critical signals or objects, such as traffic signs, which could significantly affect safety.

These sensor-based threats underline a crucial cybersecurity feature for self-driving cars: how enabling technology may inadvertently introduce new safety risks. An outstanding incident that brought the element of cybersecurity to autonomous vehicles was when Tesla had to recall some 570,000 cars since software updates on them were misdiagnosing stationary objects (TechVertu Cyber Security, 2024).

Conversely, cybercriminals can also appropriate personal details and financial information, such as a credit card number, identity theft, and fraud (Eliot, 2021). In a more direct financial context, cars could start being held for ransom, locking out functionalities until a payment is made.

As can be observed, the automotive industry faces high stakes as advancements in autonomous technologies not only introduce new technical challenges for the companies but also amplify potential cybersecurity risks, which can lead to financial losses from direct costs associated with breaches and, perhaps even more damaging, a loss of customer confidence, which can significantly decrease demand due to safety concerns (Eliot, 2021). The industry, therefore,

must balance innovation with robust cybersecurity measures to protect customers and maintain trust.

There is an increasing need for proactive measures, including regular security checking and on-time patch updating for new vulnerabilities (George et al., 2023). However, a modern autonomous vehicle comprises millions of lines of software code, and many electronic control units, which subsequently lead to extensive data flows (George et al., 2023). These complexities and interdependence, associated with frequent software updates, underlined the significant cybersecurity challenges.

On a separate note, cybersecurity issues in the automotive sector also have geopolitical implications. Specifically, for the Biden administration, there is a growing apprehension surrounding Chinese-manufactured smart cars as potential threats to national security (Daly, 2024).

2.4.2 Regulations

Regarding AV regulation, the central challenges are information asymmetries between developers and independent evaluators, the adaptability of bad actors, and the risks of error within increasingly complex software systems (Blumenthal & Csernatoni, 2022). Therefore, the continued need to develop and adapt technological and regulatory frameworks is essential.

For this reason, the rapidly evolving technology in the self-driving car industry requires the development of innovative and flexible regulatory approaches. There is a strong need to balance innovation with safety and security, particularly as it touches upon harmonizing international cybersecurity standards to accommodate the global scope of autonomous vehicle development and deployment, as well as a recognized need for a regulatory framework that can quickly adapt to technological advancements while ensuring robust safety and cybersecurity through agile and preemptive regulations (Sirisup & Petchmark, 2022; TechVertu Cyber Security, 2024). Furthermore, there is a widespread belief that government intervention is always necessary to protect against cyber risks (Eliot, 2021; Parliamentary Assembly of the Council of Europe, 2020; Prasetio & Nurliyana, 2023).

Because manufacturers of autonomous vehicles play a critical role in ensuring product safety, they face the essential task of complying with policy regulations to manage consumer trust and liability. Cybersecurity in autonomous vehicles is not merely a luxury but a requirement, especially as cars become increasingly autonomous (Stagnaro, 2023).

All of these concerns arise from the novelty of the situation and the resulting absence of established rules. The transition to a stage where vehicles are responsible for their own actions could potentially create a "responsibility gap", which existing legal frameworks may struggle to address adequately (Parliamentary Assembly of the Council of Europe, 2020; Stagnaro, 2023).

2.4.3 Mitigation and Possible Solutions

A comprehensive approach includes strategies that protect communication channels, harden components, and focus on a resilient vehicle design (George et al., 2023; K. Kim et al., 2021; Sandler, 2023) — adopting IT processes, such as data protection, encryption, and secure software development, within enterprises operating in the AV sector. These strategies, along with pre-release cybersecurity tests, are instrumental in preserving system integrity and ensuring secure system development for vehicles (Nash et al., 2024; TechVertu Cyber Security, 2024).

In particular, encryption and source-code software signing are game-changers, prompting the automotive industry to treat cybersecurity with the same seriousness as scrutinizing their tech products (Nash et al., 2024). All of these processes led to the development of intrusion detection systems and anomaly detection algorithms, which are crucial in identifying and mitigating cyberattacks.

Therefore, it is crucial to implement cybersecurity measures throughout the entire product lifecycle, integrating defense mechanisms from the concept phase and designing security into products at an early stage to minimize vulnerabilities and effectively adapt to evolving threats, a concept known as 'security by design' (George et al., 2023; Sandler, 2023). This integration begins with threat analysis and risk assessment, establishing a cybersecurity concept that focuses on both functional safety and security to protect against technical system failures and cyber threats.

This measure could also allow for integrating new inputs such as private 5G networks, edge computing, and high-performance processors, which are thought to contribute toward advancements in AV capabilities (Itemis, 2023). This happens because 'security by design' ensures resilient cyber protection, mitigating the potential expansion of the possible attack surface of the new inputs.

On a different note, compartmentalization involves structuring the vehicle's software and hardware systems into separate, isolated modules. If an attacker compromises one component, the isolation prevents the attack from spreading to other critical systems, thereby limiting the po-

tential damage (National Highway Traffic Safety Administration, 2021). Redundancy refers to duplicating essential components or functions, which ensures that if one part fails due to a cyber-attack, another can take over without affecting the vehicle's functionality. Together, these two strategies enhance the resilience of autonomous cars against cyber threats, ensuring continuous safe operation (Kukkala et al., 2022).

Integrating artificial intelligence in autonomous vehicle cybersecurity also presents a promising avenue, as it will be instrumental in fortifying AVs from advanced cyber threats (Dede et al., 2021). The development of such highly sophisticated AI and machine learning algorithms for anomaly detection is also associated with the utilization of big data and communications technologies (K. Kim et al., 2021).

Other recommendations for mitigating cybersecurity risks include using smaller network segments, enforcing periodic software updates, and adopting the Vehicle-to-Vehicle Public Key Infrastructure (V2V PKI) (Itemis, 2023). Regular software updates ensure prompt patching of security vulnerabilities, while smaller network segments help contain potential breaches by limiting the attacker's ability to move laterally across the vehicle's network.

Specifically designed for autonomous and connected vehicles, the V2V PKI is a critical security framework. It uses cryptographic techniques to securely authenticate and exchange information between vehicles in real-time (Cybrary, 2022). This helps prevent unauthorized data interception and ensures trustworthy and secure vehicle communications.

2.4.4 Public Perception

Public acceptance of AVs is a complex topic. The media significantly influences public perceptions of new technologies like autonomous vehicles. More specifically, media coverage, whether positive or negative, impacts public attitudes towards AVs with sensational and negative news, particularly regarding cybersecurity breaches, intensifying public fear and skepticism (Eliot, 2021).

For instance, acceptance of automated driving has generally been increasing but is subject to caveats, especially after dramatic accidents, indicating that high-profile incidents significantly affect public trust and acceptance (DGITM/SAGS/EP, 2019).

On the other hand, it has been found that currently only about 16% of Americans are "very likely" to ride in an AV, with 28% being "not likely at all", indicating a high level of reluctance

and skepticism (Stagnaro, 2023). Also, a third of respondents consider AVs less safe than conventional vehicles, underscoring existing safety concerns, with fears of digital security breaches further fueling skepticism, and 73% of potential users express concerns regarding hacker attacks on the vehicle or system security (Stagnaro, 2023).

The willingness to adopt these vehicles depends on their level of autonomy as well, since 31.1% of consumers prefer using a level 2 AV, while 8.8% favor a level 5 AV (Prasetio & Nurliyana, 2023). This reflects a growing interest in AVs, as well as a variance in comfort levels with different degrees of vehicle autonomy. Interestingly, the observed higher public acceptance of long-term adoption suggests that gradual familiarization may lead to more positive long-term attitudes (DGITM/SAGS/EP, 2019).

Demographic trends also indicate a higher tendency among younger, higher-income men to purchase AVs, with more reluctance often associated with safety concerns among women and other demographic groups, with informed individuals being more likely to support AV adoption (DGITM/SAGS/EP, 2019).

In line with this last idea, transparency is crucial for building trust. Disclosing safety records, performance data, and cybersecurity measures of AVs to the public can significantly influence perceptions (Tomorrow Bio, 2023).

On another note, the differences associated with demographic and socioeconomic factors highlight the need for comprehensive public information campaigns, encompassing targeted communication and marketing strategies (DGITM/SAGS/EP, 2019). One suggestion in this field is promoting AVs to influential individuals and celebrities to significantly affect public perception and adoption rates (Prasetio & Nurliyana, 2023).

Effectively addressing consumer expectations is also critical for AV acceptance and adoption. There is often a gap between consumer expectations and the actual capabilities of AVs, and it may result in underestimating AVs, leading to inefficiencies or safety risks, or overestimating them, leading to unrealistic expectations of near-perfect operation (Seetharaman et al., 2021). Balancing these perceptions is essential for the smooth integration of AVs into daily life.

Working in partnership with government institutions and collaborating with regulators and safety experts are crucial in developing AVs under a uniform and clearly defined regulatory framework. Such collaborations not only enhance safety and reliability but also guide manufacturers in meet-

ing current safety expectations and preparing for future challenges and innovations (Sirisup & Petchmark, 2022). This regulatory framework provides consumers with tangible confidence in the AVs' reliability while setting benchmarks for public trust (Tomorrow Bio, 2023).

Lastly, discussing vehicle construction *per se*, the design, regulation, and ongoing testing of AVs are crucial for their safety and reliability, which in turn builds public trust. Prioritizing these aspects in both design and continuous research phases is essential to anticipate potential issues and show the vehicles' reliability (Sirisup & Petchmark, 2022). Furthermore, a strong focus on safety helps adapt to the changing technological landscape and keeps consumer confidence high over time.

In addition to safety, strong cybersecurity measures are critical for advancing AV technology. Proactive cyber protection prevents cyber incidents and is vital to maintaining consumer confidence and public trust (George et al., 2023). Addressing cybersecurity challenges involves not just technical countermeasures but also a strategic approach to prevent a crisis in social acceptance of AVs, pointing out the need for continuous investment in securing AV systems and adding comprehensive security measures (Stagnaro, 2023).

2.5 Key Concepts of Innovation

2.5.1 Creative Destruction

The concept of creative destruction has played a crucial role in the study of innovation management (Robra et al., 2023). Joseph Schumpeter introduced this idea (Schumpeter, 1994), where he pointed out that continuous innovation drives economies forward by replacing old ideas with new ones (p. 83).

Almost seven decades after Schumpeter, around 60 definitions are found in different scientific papers, which can be merged into a simple multidisciplinary definition: Innovation involves a series of steps through which organizations convert ideas into enhanced or new products, services, or processes (Baregheh et al., 2009). This transformation is crucial for firms to progress, remain competitive, and establish distinct positions in their market.

2.5.2 *The Innovator's Dilemma* and the DCF trap

Christensen (1997) influential work *The Innovator's Dilemma* articulates a framework to understand innovation through three distinct lenses: disruptive, sustaining, and efficiency-oriented

innovations. The notion of the innovator's dilemma introduces a paradox consistently observed across the historical landscape of business.

It highlights how large, seemingly invulnerable corporations often face sudden and dramatic declines. This phenomenon occurs despite these companies engaging in practices traditionally seen as correct — primarily, listening to their existing customers' needs and desires. However, their focus on sustaining technologies and incremental improvements can prevent them from recognizing and adapting to disruptive innovations that have the potential to change the market fundamentally (Christensen et al., 2018).

Thus, responding to current customer demands can lead to short-term success and satisfaction, but it may also pave the way for long-term failure (Christensen et al., 2015). Companies become so focused on refining their offerings based on immediate feedback that they overlook innovative approaches emerging at the margins of their market. These novel innovations eventually mature, gaining traction and usurping established businesses from their dominant positions (Christensen et al., 2015).

From this issue arises the discounted cash flow (DCF) trap, also explored by Christensen et al. (2013). This refers to using discounted cash flow analysis to evaluate potential investments in disruptive technologies. Most executives compare the financial outcomes of innovation to a baseline scenario in which no action is taken. The presumption is that the current state of the business will continue indefinitely without new investments.

2.5.3 Understanding Market Pull and Technology Push in Innovation

Innovation can be propelled by two primary forces (Ameka & Dhewanto, 2013). The first is the 'market pull', a demand-driven approach, which ignites innovation by addressing unmet consumer needs in the market. This process, often called 'invent-to-order', involves individuals or groups that recognize those needs and seek to transform them into tangible products or services that benefit a broad audience (Boyer & Kokosy, 2022). For example, the rise of smartphones was driven mainly by consumer demand for more extensive connectivity and convenience.

On the other hand, the 'technology push' drives innovation from a different angle, where researchers or companies, motivated by the desire to innovate beyond the current market offerings, initiate new advancements. This approach is less about responding to the current market and more about breaking new ground with novel technologies. It often leads to 'creative destruc-

tion', where new technologies disrupt existing markets and pave the way for new industries (Boyer & Kokosy, 2022). An example of a technology push is renewable energy technologies, pursued due to their potential rather than existing demand.

Both 'market pull' and 'technology push' are essential for fostering innovation (W. J. Kim & Lee, 2009). Market pull typically leads to replacing or enhancing existing products, while technology push can create entirely new markets or disrupt existing ones (Walsh et al., 2002). Understanding and balancing these forces is crucial for businesses aiming to stay competitive and drive economic growth.

2.5.4 Exploring the Diffusion of Innovation and the Technology Acceptance Model

Lastly, it is essential to analyze the adoption, diffusion, and acceptance of new technologies using the innovation diffusion framework and the technology acceptance model (TAM).

The "Diffusion of Innovation Theory", articulated by Rogers (1962), explains the mechanism by which new ideas or products gain momentum and spread. Adoption unfolds progressively, whereby individuals adopt new ideas at different stages, with 'early adopters' often displaying distinct characteristics compared to later adopters. Understanding these traits and the dynamics of how innovations spread can significantly enhance the effectiveness of introducing new concepts or products. Effective diffusion strategies depend on comprehending the target audience's inclinations and motivations, which is crucial for facilitating the adoption process (Rogers, 1962).

The Technology Acceptance Model, initially developed by Davis (1993), introduces a framework that focuses on the internal factors affecting an individual's decision to accept and use new technology. The model emphasizes two criteria: perceived usefulness (PU) and perceived ease of use (PEOU). Perceived usefulness relates to the extent to which an individual perceives that utilizing a specific system would improve their job productivity or overall efficiency. This criterion acknowledges that if individuals perceive technology as beneficial for accomplishing their tasks more efficiently, they are more likely to adopt it (Davis, 1993; Davis et al., 1989).

On the other hand, perceived ease of use refers to how effortless one finds the operation of new technology; if potential users believe they can adopt this new tool without much difficulty or effort, their willingness to embrace this change increases significantly. These two dimensions

interplay harmoniously within TAM by suggesting that utility and user-friendliness govern acceptance behavior toward technological innovations (Davis, 1993; Davis et al., 1989).

TAM advances Rogers' Diffusion of Innovation Theory by emphasizing user perceptions instead of just innovation traits like advantage or compatibility (Venkatesh & Davis, 2000). While Rogers highlighted how innovation qualities influence diffusion across societies, he overlooked the individual psychological aspects within organizations. Davis's additional layer links beliefs about software (usefulness and ease of use) to adoption actions, filling gaps in Rogers' theory (Davis, 1993). This approach connects subjective judgments with usability assessments, promoting more effective interventions and aligning closely with user-centered design principles — thus improving understanding and strategies around technology acceptance among users (Blut et al., 2017).

2.6 Exogenous Shocks and Dynamic Capabilities

Understanding the drivers of organizational success and performance requires a multifaceted approach to understanding how a firm can adapt to rapidly changing environments.

2.6.1 Exogenous Shocks and the Concept of Fit

Exogenous shocks are sudden, unexpected events that significantly alter the external environment in which organizations operate. These shocks can arise from various sources, including technological advancements, political upheavals, economic crises, demographic shifts, health-related events, and environmental changes (Teece, 2007). Examples include disruptive technological innovations, economic recessions, shifts in consumer demographics, pandemics, and climate change. Such events can profoundly impact organizations, often leading to dramatic changes in performance distribution among firms (Aldrich, 1979; Hannan & Freeman, 1977).

Exogenous shocks, by disrupting the status quo, not only create new opportunities but also pose new threats. The ability of organizations to swiftly adapt to these changes determines their survival and success. This process of selection, where external shocks favor certain firms over others, underscores the crucial role of alignment between a firm's internal characteristics and the external environment (Levinthal, 1991).

The concept of fit in organizational performance is of paramount importance, as it signifies the alignment of a firm's resources, capabilities, and strategies with the external environment

(Venkatraman & Camillus, 1984). A good fit can lead to superior performance, enabling firms to capitalize on new opportunities and mitigate threats, while a poor fit can result in adverse outcomes. Firms well-aligned with the external environment can effectively respond to changes, thereby enhancing their performance (Miles & Snow, 1984).

Exogenous shocks can significantly alter the competitive landscape. For instance, during the internet revolution, firms like Compaq, Dell, and IBM experienced varying impacts on their performance. Some benefited from the external shock, while others were negatively affected, illustrating how exogenous factors can lead to shifts in the competitive landscape (Porter, 1980).

2.6.2 Dynamic Capabilities

A company's dynamic capabilities involve its capacity to combine, develop, and adapt internal and external skills to meet the needs of quickly evolving circumstances. This concept, designed namely by David Teece, emphasizes the benefits of a firm's ability to adapt to exogenous shocks through sensing opportunities and threats, making timely decisions, and reconfiguring resources (Teece et al., 1997). Dynamic capabilities are not just a survival strategy but a means to improve performance in today's fast-paced business environment.

Barreto (2010) refines the scholarship on dynamic capabilities by seeking a more concrete definition. He frames dynamic capabilities as "the firm's potential to systematically solve problems, formed by its propensity to sense opportunities and threats, to make timely and market-oriented decisions, and to change its resource base" (Barreto, 2010). In retooling the definition, Barreto seeks to operationalize the concept in a way that can show how a firm deploying dynamic capabilities can achieve superior performance.

Dynamic capabilities are critical for firms in hypercompetitive and high-velocity environments, where adaptability is vital to long-term survival and success. Four fundamental dimensions explain a firm's adaptive capabilities (Eisenhardt & Martin, 2000).

The first dimension is sensing opportunities and threats, which involves accurately interpreting changes in the external environment. Firms must effectively gather and process information despite challenges such as bounded rationality, limited information-gathering, attention, and processing abilities (Simon, 1997).

The second dimension is making timely decisions, where firms need to act at the optimal time to capitalize on opportunities and mitigate threats. This involves assessing the urgency and timing

of market entry or product launches (Helfat & Peteraf, 2003).

The third dimension focuses on market-oriented decisions, requiring firms to align their strategies with market demands and customer preferences. This necessitates a business culture that not only responds to but also anticipates and shapes market trends, prioritizing creating superior customer value (Day, 1994).

Finally, the fourth dimension is changing the resource base. Firms must be willing to gain, release, or reconfigure resources to adapt to new challenges. This can involve internal development, external acquisitions, or restructuring existing resources (Simon, 1997).

2.6.3 Examples of Dynamic Capabilities in Action

Nokia and Fujifilm Cases

The contrasting fates of Nokia and Fujifilm underscore the importance of dynamic capabilities. Once a leader in mobile phones, Nokia failed to adapt to the smartphone revolution, leading to a significant decline in performance (Doz & Kosonen, 2010). In contrast, Fujifilm successfully navigated the transition from analog to digital technology by diversifying its product offerings and reconfiguring its resource base, thereby maintaining its competitive edge (Tripsas & Gavetti, 2000).

Microsoft and Amazon

Satya Nadella, who later became CEO, reflected on Microsoft's acquisition of Nokia's mobile division as a misstep, highlighting the challenges of making timely and market-oriented decisions (Nadella, 2017). In contrast, under Jeff Bezos's leadership, Amazon has exemplified strong dynamic capabilities by continuously sensing new opportunities, such as cloud computing, and effectively reconfiguring its resources to exploit them (Krause, 2024).

3 Methodology

3.1 Research Design

This research design aimed to analyze how public perceptions of cybersecurity risks could impact the adoption of autonomous vehicles. The methodology is described in Figure 3 below.

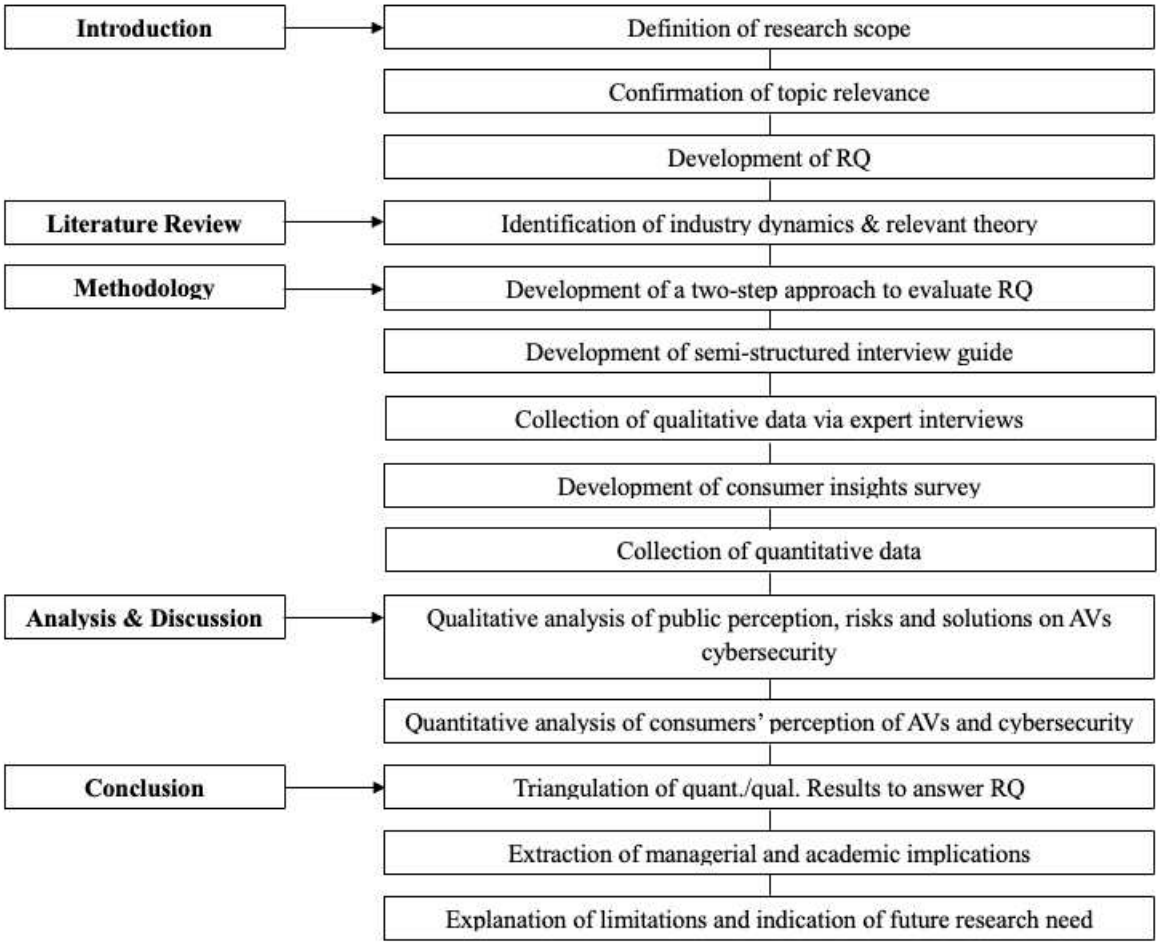

Figure 3: Research Design

A mixed-methods approach using triangulation was selected, combining quantitative and qualitative data with both inductive and deductive thinking (Sekaran & Bougie, 2016). First, semi-structured expert interviews were held with cybersecurity experts, academics specializing in cybersecurity, automotive engineers, and analysts from the automotive industry. Expert interviews were considered an ideal method for exploring in-depth insights (Qu & Dumay, 1995; Weiss, 1995) (see Chapter 3.2.1). Then, quantitative data was collected through a survey, with the aim of analyzing potential customer perceptions and acceptance of self-driving cars as well as potential cybersecurity concerns (see Chapter 3.2.2). Finally, the qualitative research and

literature review outcomes were triangulated with those from the quantitative research.

3.2 Data Collection

The paragraphs below discuss the data collection methods used in Chapter 4.

3.2.1 Primary Data Collection - Expert interviews

Semi-structured interviews are a standard method in business research for conducting qualitative research (Bansal et al., 2018). Researchers utilize this approach to gather 'facts' or acquire an understanding of viewpoints, attitudes, experiences, procedures, behaviors, or forecasts (Rowley, 2012). Semi-structured interviews offer the significant benefit of examining motivations, beliefs, and attitudes. (Barriball & While, 1994). Furthermore, they are best suited for situations where speaking with the expert only once is necessary and can allow the researcher to notice non-verbal indicators during the interview (Barriball & While, 1994; Cohen & Crabtree, 2006).

A set of interview questions guides the interaction between the interviewer and respondent in semi-structured interviews. This guideline offers a clear framework and is instrumental in generating reliable, comparable qualitative data (Cohen & Crabtree, 2006). The development of the guide was based on inductive reasoning, drawing upon existing knowledge of the subject (Rowley, 2012). Although the guidelines provide a structured approach, they allow the exploration of new topics as the dialogue moves forward (Magaldi & Berler, 2020). It is important to note that asking follow-up questions enhances flexibility and tailors the gathered data to the specific circumstances (TurnerIII, 2010).

The interview guideline included around ten questions, as detailed in the Appendix, with each interview lasting about 30 minutes on average. In order to try to collect ordinal data and measure experts' perceptions of the subjects addressed, a few Likert scale-like questions were integrated (Joshi et al., 2015). It is important to note that adjustments were made to utilize the specialized expertise of the interviewees better while ensuring that specific core questions were posed to the majority of the experts.

The twelve experts who were interviewed came from diverse backgrounds, including academia, OEMs, national authorities, and other relevant fields, and they contributed a wide range of viewpoints. Invitations for interviews were sent to more than forty potential participants through various channels such as email, LinkedIn, sector events, personal networks, and direct referrals.

The experts are described anonymously in Table 1, detailing their current roles, areas of expertise, and experience, with the study falling within the ideal range, which suggests data saturation occurs within twelve interviews (Guest et al., 2006). The interviews were carried out using the platform Teams.

Code	Current position and expertise
AW	Cybersecurity specialist at a national cybersecurity center, expertise in national security, focusing on espionage and cyberattacks on critical infrastructure, automotive privacy, and safety issues.
AR	Solutions architect in operational technology and cybersecurity, with expertise in addressing cybersecurity threats in transportation, focusing on digitalization and automation in trains, cars, and infrastructure.
EC	Information Security Manager, expertise in Cyber Threat Intelligence, Security Operations Center, Digital Forensics, and SIEM & Log Management services with 20 years of experience in the cybersecurity and IT sector.
PG	Coordinator of an information technology and communications support center of the thematic program for climate action and sustainability, expertise in cybersecurity and data protection with 25+ years of experience in the field.
JF	Coordinating Professor and researcher at a Portuguese university, with expertise in security, wireless vehicular communications, cooperative connected, and automated mobility, and author/co-author of over 120 publications.
PR	Investigator and PhD candidate at a leading Portuguese university specializing in sensor-fusion and V2X. Over 20 years of experience in IT management, systems, and networks, including seven years as Technology Unit Coordinator.
ES	Former director at a European OEM, current director at a prominent national institution dedicated to automotive support and services, expertise in driver support services, new technologies, electric vehicles, and leading initiatives in service creation and garage audits with 25+ years of experience.
JB	Chief Information Security Officer at a prominent national institution dedicated to automotive support and services, with expertise in information technology and over 20 years of experience.
CR	Site director at a prominent French automotive OEM, with expertise in the automotive repair market and supervision of the Autoeuropa factory launch, with 25+ years of experience in the sector.
FM	Senior consultant on strategy & digitization at a European luxury automotive OEM, expertise in the autonomous driving sector with one year of experience.
LS	Product Owner for Autonomous Driving for a major German electronics manufacturer in partnership with a prominent German OEM, with expertise in test systems and firmware and former experience in home automation research with strong industry ties.
JS	Business Development Manager for Automotive & Off-Road at a leading global provider of mission-critical software solutions. Over 15 years of experience in safety-critical software and systems development across different sectors, including the automotive.

Table 1: Overview of interviewees

3.2.2 Primary Data Collection - Consumer insights survey

The review of existing literature (detailed in Chapter 2) demonstrated the importance of consumer acceptance in the diffusion of disruptive innovations. Therefore, taking cybersecurity concerns into account as a crucial factor impacts consumers' likelihood to adopt autonomous vehicles. A survey was conducted to understand customers' perspectives better.

Various platforms disseminated the survey online, enabling cost-effective data collection and potentially rapid response rates (Fowler Jr, 2013). The survey (see Appendix A) comprised 26 questions covering demographic, multiple choice, 5-point Likert scale, matrix, and rating scale questions. It was categorized into six sections: general familiarity and perception of autonomous vehicles; willingness to adopt AVs with different autonomy levels; awareness and concerns regarding cybersecurity; willingness to adopt AVs with different autonomy levels after considering cybersecurity aspects; adoption and acceptance assessment using the TAM model; and demographics and background questions. The survey was conducted in English and Portuguese, online, free from researcher interference, with an international population, utilizing the Qualtrics platform for its design and administration. The limitations of the survey are discussed in Chapter 5.2.2.

It was initiated by n = 249 participants in April 2024, with 98.4% completing the entire questionnaire. Those who did not finish were excluded from the data, resulting in a reduced sample size of n = 245 observations. A qualifying question was used to evaluate respondents' ability to identify invalid responses, leading to 6 responses being discarded and resulting in a sample size of n = 239.

It is generally recommended that a representative sample should be large enough to offer a margin of error between 5% and 10% at a confidence level of 95% (Bartlett et al., 2001). For populations larger than 10,000, a sample size ranging from 200-400 is typically considered representative (Krejcie & Morgan, 1970). Considering the wide array of companies and stakeholders within the automotive industry, utilizing a sample size as indicated would likely provide insights with some degree of reliability into cybersecurity concerns.

4 Analysis and Discussion

In Chapter 4.1, insights from expert interviews are analyzed, while in Chapter 4.2, consumer survey outcomes are examined. By triangulating data from both primary and secondary data (from Chapter 2), it is then evaluated whether cybersecurity concerns affect the adoption of self-driving cars in Chapter 5.1.

4.1 Cybersecurity Risks and Mitigation Strategies

A keyword analysis was conducted for some questions to cluster the most frequent reasons thematically. Word-based coding was used to analyze the qualitative data, enabling the indexing and categorizing text to establish a framework of thematic ideas (Gibbs, 2007). For others, a direct analysis was performed based on the respondents' opinions on specific topics.

4.1.1 Cybersecurity Risks in the Automotive Sector

The semi-structured interviews with cybersecurity and automotive experts highlighted various cybersecurity risks associated with connected and autonomous vehicles (AVs). Table 2 shows the keywords and phrases from the interviews allocated to the respective categories concerning cybersecurity risks associated with this type of vehicle.

Risk Category	**Trigger Keywords/Phrases**
Unauthorized Vehicle Access	unauthorized access, remote access, remote control
Hacker Attacks	hacker attacks, malware, ransomware, cyberattacks
Data Privacy and Theft	data privacy, personal data, GDPR, data protection, data theft, information collection, biometric data
Physical Safety and Integrity	physical safety, passenger safety, accidents, security risks
Endpoint Security Solutions	endpoint security, encryption, secure communication
Regulatory and Legal Matters	regulatory standards, legal implications, liability
Consumer Awareness and Transparency	consumer awareness, transparency, incident response, monitoring
IP Theft	IP theft, OEM, protecting the IP
Connectivity and Standardization Issues	connectivity, universal language, standardization, communication
Supply Chain Vulnerabilities	component shortage, supply chain, market shortages

Table 2: Categorized Cybersecurity Risks in Autonomous Vehicles

Although both groups acknowledged the importance of robust cybersecurity measures, their perspectives and emphasis on specific risks differed, as can be observed in the following image.

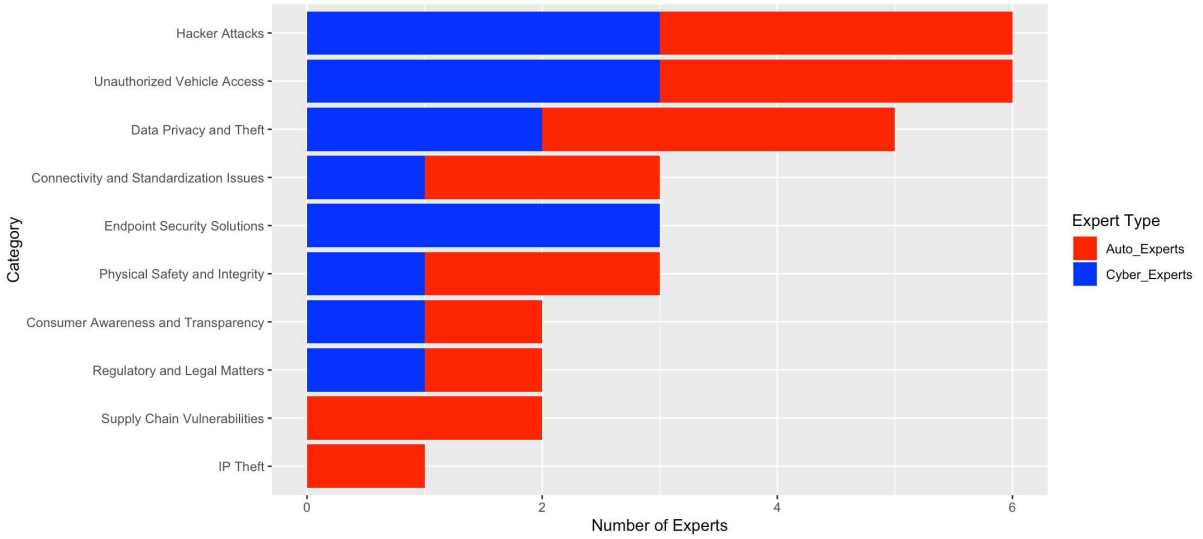

Figure 4: Cybersecurity risks mentioned by experts per type of expert

A risk that was mentioned by half of the experts of both groups was remote or unauthorized vehicle access. PG, a cybersecurity expert, emphasized this as the highest concern if an unauthorized entity gains control of a vehicle. Automotive experts like JB echoed this concern, stating that unauthorized remote control of vehicles influences consumer decisions and undermines trust in AV technology.

Hacker attacks were another critical concern for both groups, and half of both groups mentioned them. Cybersecurity experts focused on the complexity and sophistication of these attacks. AR pointed out that each attack needs to be engineered for a specific scenario, making the current systems relatively safe due to their complexity. However, AR also warned that as systems become more standardized, the cost of attacks could decrease significantly, causing the ease of cyber infractions to rise. Similarly, PR highlighted the increased attack surface and potential consequences of remote control of vehicles, stressing the risk of vehicles being used for terrorist attacks or other malicious purposes by rogue actors. On the other hand, automotive experts like CR pointed out how hacking has the potential to disrupt manufacturing processes or halt factory operations.

Despite being discussed by five experts and being one of the most mentioned concerns, data theft was viewed differently by the two groups. PG ranked it third in terms of concern, noting that while worrying, data theft did not compromise the physical integrity of people or vehicles. In contrast, automotive experts called attention to the breach of personal data privacy, mainly as connected vehicles collect increasing amounts of personal information. JB mentioned that

violations of individual data privacy could severely impact consumer confidence in AV technologies.

One notable difference between different experts concerned with safety and physical integrity. Cybersecurity experts mostly prioritized ensuring that the systems operate as intended without unauthorized interference. AW stressed the importance of maintaining the integrity of vehicle systems to ensure that no one can alter or control the car's configuration. Similarly, JS raised urgent concerns about the massive exploitation of vulnerabilities, particularly in systems like remote parking, which could allow control of an entire fleet. In contrast, automotive experts were more concerned with the direct physical safety of passengers and the potential for cyberattacks to cause accidents. ES called attention to vulnerabilities in convenience features such as keyless entry, which, while popular with consumers, pose significant security risks.

Two experts also mentioned regulatory and legal matters. JF pointed to the need for stringent cybersecurity standards set by regulators. Automotive experts were more concerned with the legal implications of cybersecurity incidents, particularly regarding liability in cases where autonomous vehicles cause harm. ES raised questions about who would be responsible if an autonomous vehicle acted in a way that resulted in an accident.

Lastly, it is essential to examine the risks identified uniquely by each group of experts. Three cyber experts emphasized the need for comprehensive endpoint security solutions and encryption for autonomous vehicles, a concern not shared by the auto experts. For instance, expert EC pointed out the importance of implementing thorough endpoint security solutions for autonomous vehicles and noted the critical need for encrypted communication with central systems and robust security measures across the entire ecosystem. This emphasis on comprehensive endpoint security reflects the need for a technology push approach in innovation, where pioneering new security measures can protect against evolving cyber threats (Boyer & Kokosy, 2022).

In contrast, two auto experts focused on supply chain vulnerabilities, particularly component shortages and potential security risks from dubious suppliers. One of them also mentioned the importance of protecting intellectual property at the OEM level. This divergence in concerns among the experts is understandable, as these risks are specific to each field and may not be immediately apparent to those outside of their respective areas of expertise.

In general, the interview findings concurred with trends identified in the literature. The latter indicated that the automotive sector is increasingly aware of cybersecurity threats, especially

with the advent of connected and autonomous vehicles, which are vulnerable to remote cyber threats and data breaches (Bradley, 2022; Davies, 2023). Experts' concerns about unauthorized access and data theft mirrored the literature on these vulnerabilities.

Furthermore, these risks illustrate the importance of maintaining a good fit between a firm's internal cybersecurity capabilities and the external threat landscape, as outlined in the dynamic capabilities framework (Venkatraman & Camillus, 1984).

4.1.2 Automotive Sector Readiness for Cybersecurity Concerns

The complexity of the automotive sector's cybersecurity landscape was a prominent theme among experts. Eight out of twelve experts identified the integration and security of numerous components from different manufacturers as particularly challenging. JF described this as a "worst-case scenario" for cybersecurity, especially considering the added complexity of connectivity and over-the-air updates. AR echoed this sentiment, noting that while cybersecurity issues in vehicles are similar to those in other industrial applications, the automotive sector has unique constraints related to computing power and power consumption.

Six experts, including PG and AW, discussed the life-and-death implications of cybersecurity in the automotive sector. AW compared the automotive sector to healthcare, noting that both involve risks to human life, making cybersecurity especially critical. This comparison again highlights the importance of maintaining a good fit between a firm's internal capabilities and the external environment to ensure robust cybersecurity measures safeguarding human lives (Venkatraman & Camillus, 1984).

Vehicles need to communicate with various systems, including GPS and the Internet, adding layers of complexity. AW argued that the stakes are higher in the automotive industry because of the direct impact on people's lives compared to sectors such as banking.

Adding to this complexity, EC emphasized the necessity of treating autonomous vehicles as endpoints similar to other IT and OT devices. He pointed out the challenges of monitoring and securing these endpoints, noting that the principles applied to current industrial and IT environments could be extended to autonomous vehicles. This includes ensuring comprehensive logging, real-time data retrieval, and robust monitoring systems to effectively detect and respond to threats.

The standards and regulations governing automotive cybersecurity are still evolving, as noted by

seven experts. JF mentioned that some brands, like Porsche, have stopped selling specific models that do not meet the latest cybersecurity standards. This aligns with JB's detailed overview of various standards, like ISO/SAE 21434 for cybersecurity in road vehicles and ISO 26262 for functional safety, which are crucial for ensuring compliance and protecting against cyber threats. The emphasis on adhering to stringent standards reflects the industry's recognition of the high stakes involved.

Expert perceptions varied significantly regarding the automotive sector's readiness to handle large-scale cyber-attacks. Only five out of twelve experts provided concrete numerical ratings. The majority of the experts felt uncomfortable giving a rating due to a lack of knowledge or familiarity with the subject. JF expressed confidence in the European Union's stricter regulations, which help ensure high preparedness, rating the readiness as 9 or 10. However, he noted that the industry is still in a complicated phase, particularly with software integration. FM rated the current protections at 7, indicating that while adequate for the limited number of equipped vehicles, there is potential for improvement, as the industry must invest significantly more in cybersecurity as the technology rolls out to a more extensive fleet. FM asserted that the feeling of safety could diminish as more vehicles become connected and attractive targets for cyber attackers.

On another note, LS highlighted that many vehicle components might not have faced extensive cybersecurity testing, making them vulnerable to advanced attacks. He emphasized that the automotive sector is currently behind in terms of frequent updates and cybersecurity readiness compared to other sectors, rating it a 5. This aligns with JS's observation that, while the automotive sector is advanced in terms of compliance, it lags in effectiveness, mainly due to the stringent safety-critical requirements that slow down the implementation of security measures.

CR rated the current level of preparedness among companies and individuals as very low, between 2 and 4. It noted that many people still fall for phishing attempts, which could lead to significant factory costs, demonstrating the need for better education and training.

Three experts compared the automotive sector to other industries, underscoring its unique difficulties and higher stakes due to potential physical harm. While AW noted previously that both the automotive and healthcare sectors involve risks to human life, making cybersecurity especially critical, AR pointed out that vehicles have unique constraints related to computing power and power consumption, which are less of an issue in industries such as railways and aviation.

PR emphasized the critical nature of cybersecurity in the automotive sector due to the potential for physical harm, stressing that the sheer number of vehicles and their operation in urban environments make this situation more relevant than most other cybersecurity issues. He pointed out that the consequences of cyberattacks on vehicles are direct and potentially catastrophic, such as using vehicles for terrorist attacks, which shows the heightened stakes in automotive cybersecurity compared to other sectors. This means that the unstructured nature of the automotive environment, with vehicles interacting freely in urban settings, adds a layer of complexity not present in more controlled environments.

The automotive sector faces challenges due to its complexity and integration of advanced technologies. JF described the difficulty of maintaining security across numerous software components and the potential for malicious behavior from sensors, which can be subtle but severely impact safety. PG emphasized the sector's specificities, such as the need for communication with various systems and the potential for large-scale damage in the event of cyber incidents.

The evidence from the interviews was consistent with the literature, which underscored the severe complexity and high stakes of cybersecurity in the automotive sector. Eight experts pointed to the multifaceted nature of automotive cybersecurity, noting that integrating components from various manufacturers exacerbates the challenge, aligning with the literature's considerations on the complexity of securing diverse systems (Burkacky et al., 2020).

The concerns about unauthorized access, data theft, and stringent standards and regulations raised by both cybersecurity and automotive experts align with the literature's emphasis on these vulnerabilities. For instance, PG and JB stressed the importance of robust standards like ISO 26262 and ISO/SAE 21434 to mitigate risks (Morris et al., 2020). The literature also demonstrated these standards as essential for maintaining comprehensive security frameworks (Schmittner & Macher, 2019).

Moreover, experts focused on the potential for physical harm and the critical nature of cybersecurity in the automotive sector echoed the literature about the direct impact on human life, as well as the potential for large-scale damage. PG's comparison of automotive cybersecurity to industries like healthcare further highlights this critical nature, as the consequences of security breaches can be fatal (Elgazzar et al., 2022). The literature similarly explored the high stakes involved, particularly in preventing life-threatening scenarios.

These comparisons also revealed the distinct challenges faced by the automotive sector in main-

taining cybersecurity, which is in line with the idea of dynamic capabilities, as firms in different industries must adapt their internal processes and resource configurations to address specific external challenges effectively (Eisenhardt & Martin, 2000; Teece et al., 1997).

As discussed by the experts, the automotive sector's readiness for large-scale cyberattacks reflected ongoing concerns in the literature about the industry's preparedness. JF and FM noted the current limitations and the need for substantial improvements as more connected vehicles hit the roads. This aligned with the literature, stressing the need for continuous adaptation and investment in cybersecurity measures to stay ahead of potential threats (Morris et al., 2020; United Nations Economic Commission for Europe (UNECE), 2022).

4.1.3 Materiality of Cybersecurity Concerns on Public Perception

When it comes to public perceptions of AVs, experts focused on the intrinsic link between safety and cybersecurity. Six out of twelve experts, including AW and JF, noted that the most critical concern in cybersecurity was safety, which involves ensuring that a car operates as intended without unauthorized interference. For instance, JF further explained that in languages like Portuguese, the terms safety and security are often used interchangeably, highlighting the interconnected nature of these concepts. This matched the current literature, which indicates that safety is a primary concern for consumers considering AVs, with many wary of the potential for cyberattacks that could compromise vehicle control and safety (George et al., 2023; Tomorrow Bio, 2023).

Only one expert, FM, highlighted significant demographic differences in the perception of AV cybersecurity. He shared that Chinese consumers are more willing to adapt to new technologies and have less fear of cybersecurity risks compared to consumers in Europe or the US. This observation supported findings in the literature that demographic factors, including cultural differences, play a significant role in shaping attitudes towards AVs (Stagnaro, 2023).

Four experts, including EC, noted that the average consumer does not concern themselves with cybersecurity issues daily, as most people are unaware of the extensive cybersecurity strategies and regulations in place, such as the new Cybersecurity Law and specific guidelines from agencies like the CISA in the US. This lack of awareness is widespread, with many consumers prioritizing aspects like the brand and color of a vehicle over its cybersecurity features. EC emphasized that much of the responsibility for cybersecurity lies with state regulation and man-

ufacturers, who must ensure compliance with stringent standards without burdening consumers with technical details.

Furthermore, PR and PG noted that while technological advancements in AVs are crucial, consumers often prioritize more immediate concerns like aesthetics and brand reputation. This reflects the importance of effective diffusion strategies as articulated in the Diffusion of Innovation Theory, where understanding the target audience's inclinations and motivations is crucial for facilitating the adoption process (Rogers, 1962).

The media significantly influences public attitudes towards AVs. Sensational and negative news, particularly regarding cybersecurity breaches, can intensify public fear and skepticism (Eliot, 2021). Four experts, including CR, highlighted this by pointing out the potential negative impact of drawing too much attention to cybersecurity issues, suggesting it might deter people from adopting AVs.

Trust in the current cybersecurity measures of AVs is another critical factor influencing public perception. Six experts, including AW and JB, pointed out that while some people might be overly concerned about cybersecurity, others might be too lax. However, the general trend shows increasing investment in cybersecurity as it becomes a more significant public concern. This reflects the literature's evidence that effective cybersecurity measures are crucial for fostering adoption by alleviating perceived risks (George et al., 2023). AR added that a significant cyberattack causing loss of life could rapidly shift public awareness and adoption of cybersecurity measures.

Three experts noted that skepticism regarding new technologies, such as electric cars, often overlaps with attitudes toward AVs. For instance, PR suggested that comprehensive information about AVs' cybersecurity, akin to energy consumption labels on household appliances, has yet to be available to consumers.

LS likened the public's adaptation to AVs to the transition from traditional phones to smartphones. The real impact on consumer decisions will come from tangible events, such as accidents, that make the implications of cybersecurity failures concrete and understandable. He suggested that only when these issues become real and noticeable to users will they significantly influence purchasing decisions.

JS also shared this view, stating that cybersecurity issues might not significantly deter most

consumers, as people already trust smartphones with sensitive information. However, incidents that risk human lives could potentially cause hesitation.

The concept of relinquishing control to AI is another significant concern. Autonomous driving involves ceding control to AI, which can be intimidating for many people. AW noted that this could be a substantial hurdle for public acceptance of AVs despite the potential benefits of AI in improving safety and efficiency. This concern is consistent with the literature, which suggests that balancing consumer expectations with the actual capabilities of AVs is essential for their smooth integration into daily life (Seetharaman et al., 2021), as well as aligns with the Technology Acceptance Model, where perceived usefulness and ease of use are critical factors influencing user acceptance of new technologies (Davis, 1993).

4.1.4 Possible Mitigation Strategies for Cybersecurity Concerns

Similarly to the first subchapter, related to cybersecurity risks, table 3 shows the keywords and phrases from the interviews allocated to the respective categories concerning mitigation strategies that could be placed to counter cyber threats.

Risk Category	**Trigger Keywords/Phrases**
Information Sharing and Collaboration	sharing experiences, database of attacks, sharing attack signatures, transparency, reward ethical hacking, collaboration
Trust and Public Perception	trust, public perception, transparency, consumer trust
Regulatory and Standardization	regulatory body, standards, ISO 27001, specific regulations, compliance, legislation, certification
Secure Development Practices	secure development, Security by Design, vulnerability assessments, risk analysis, audits, quality control
Encryption and Communication Security	encryption, secure communications, end-to-end encryption, data encryption, firewalls, intrusion detection systems
Continuous Monitoring and Updates	continuous security checks, alarms, regular updates, security patches, intrusion detection
Component Security and Resilience	supply chain security, malicious components, redundant systems, component control, resilience, fail-safes, anomaly detection
Marketing and Consumer Education	marketing, public communication, safety demonstrations, consumer education
Artificial Intelligence and Machine Learning	artificial intelligence, machine learning, human-like behavior, AI-driven driving

Table 3: Categorized Mitigation Strategies for Cybersecurity Risks

The evaluation of mitigation strategies for cybersecurity in AVs revealed a range of expert opinions, highlighting both contrasts and similarities between approaches proposed by cybersecurity and automotive experts (see figure 5)

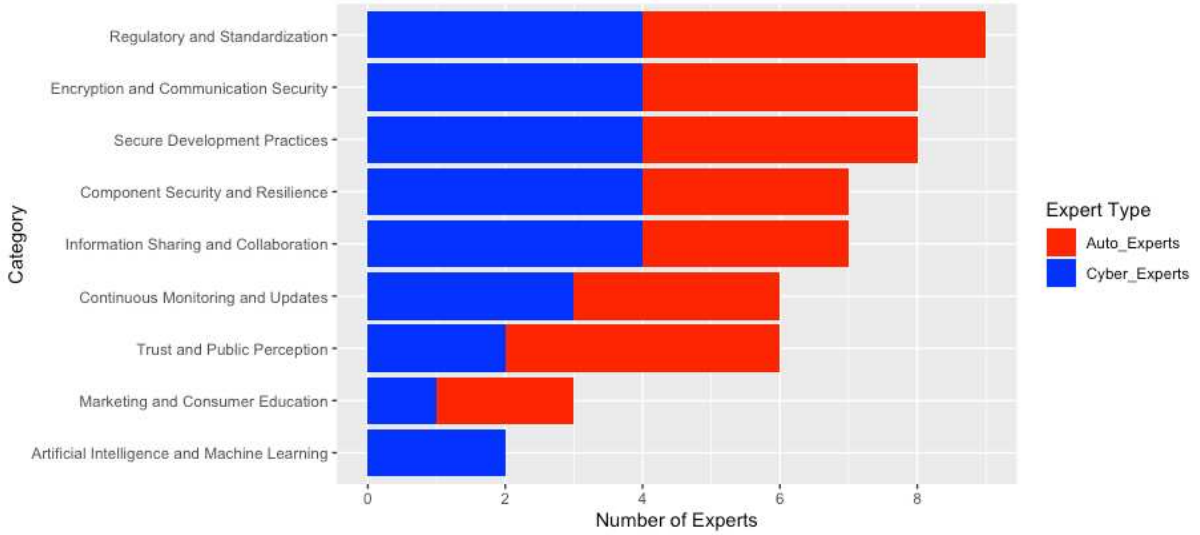

Figure 5: Cybersecurity risks mentioned by experts per type of expert

The chart, which displays the distribution of responses from automotive experts and cybersecurity experts, shows no significant differences between the two groups. This indicates that, regarding addressing potential cyber threats, the proposed measures by both groups are mostly aligned.

The most frequently mentioned mitigation strategy by both automotive and cybersecurity experts is regulatory and standardization efforts, noted by nine out of twelve experts. Automotive experts like CR and JB emphasized the importance of developing clear regulatory frameworks and establishing security standards, with CR even mentioning a solid trend towards standardization of technologies, especially with regulations, which opposes the idea of specialization. ES pointed out the need for an institutional regulatory body to guarantee security, similar to the Euro NCAP safety tests affecting car insurance costs in Germany. This strategy aligns with the literature's focus on regulatory compliance and the role of independent assessments in building public trust (Sirisup & Petchmark, 2022). PG from the cybersecurity sector stressed the need for specific regulations for the automotive sector, like those in banking and healthcare, to ensure compliance and facilitate experience sharing among car manufacturers.

The second most critical category is encryption and communication security. Eight out of twelve experts stated that secure communication is essential for safeguarding autonomous vehicles against cyber threats. For instance, JB elaborated on using end-to-end encryption to protect communications between the vehicle and external infrastructure, such as vehicle-to-everything (V2X) systems. EC reinforced this by underlining the necessity of encrypting all communi-

cation between the vehicle and central systems, both in transit and at rest, to protect sensitive information from unauthorized access. This approach reflects the technology push aspect of innovation, where integrating advanced encryption technologies can protect against evolving cyber threats and drive the safe deployment of autonomous vehicles (Boyer & Kokosy, 2022).

Eight experts also mentioned secure development practices, equally from both sectors. PG highlighted the necessity of integrating security into all project phases, the already presented principle of "Security by Design". AR pointed out the importance of validation at each stage of the value chain to thwart potential exploits. JB and LS, from the automotive perspective, emphasized the importance of adhering to secure software development techniques and incorporating test-driven development principles to ensure continuous and flexible testing, as this approach ensures the vehicle's code is safe and reliable. The literature concludes similarly that incorporating security measures from the outset is crucial for creating resilient systems (George et al., 2023).

Information sharing and collaboration were highlighted by seven experts. JF and PG, both cybersecurity experts, stressed the need for sharing attack signatures and experiences among companies to prevent isolated incidents. From the automotive side, JB suggested collaboration between manufacturers, governments, and other stakeholders to establish security standards and share information on threats and best practices. This collaborative approach aligns with the concept of market pull in innovation, where addressing industry-wide challenges through shared knowledge and standards can drive the effective adoption of secure technologies (Boyer & Kokosy, 2022).

The concepts of component security and resilience were another area of alignment for seven out of the twelve experts. For instance, AR pointed out the use of established standards like ISO/IEC 62443, which provide a framework for designing systems based on risk analysis. This approach plays a crucial role in isolating different system components and ensuring their continued functioning even in the event of a compromise. This focus on robust standards and resilience aligns with the dynamic capabilities framework, where firms must continuously reconfigure their resources to manage risks and maintain operational integrity (Teece et al., 1997).

JF drew parallels with the redundancy found in aviation and rail, although he acknowledged the challenge of applying such extensive measures in the automotive sector due to cost and practical constraints. PR expanded on this by discussing the importance of sensor redundancy

to mitigate physical attacks on sensors and ensure resilience in the face of cybersecurity threats. The literature also supported these strategies, underscoring the importance of redundancy and compartmentalization in designing resilient systems (Nash et al., 2024).

Six of the experts discussed the importance of regular software updates and intrusion detection systems, which they deemed essential for maintaining the security of AVs. JB outlined various measures, including implementing firewalls and intrusion detection systems and ensuring vehicle systems are updated with the latest security patches. AR pointed out the necessity of ongoing validation at every phase of the value chain to thwart potential exploits. EC also noted the importance of continuous monitoring and implementing robust endpoint security measures, viewing autonomous vehicles as endpoints similar to mobile devices and personal computers. The literature reinforces this approach, stressing the importance of maintaining up-to-date systems to address vulnerabilities promptly (Sandler, 2023).

Building public trust and shaping positive perceptions are critical for adopting autonomous vehicles, also perceived by half of the experts interviewed. Transparency in handling cybersecurity incidents and disclosing protective measures can reassure consumers, which was emphasized by JF and is supported by relevant literature (Tomorrow Bio, 2023). Despite ES's skepticism about the public's genuine desire for transparency, robust safety records, and consistent performance, as stressed by FM, are fundamental in gaining trust. As mentioned before, this is closely tied to the Diffusion of Innovation Theory, as effective communication and transparency are vital in facilitating the adoption process and building trust among early adopters and the broader public (Rogers, 1962).

Lastly, two less frequently mentioned mitigation strategies were marketing and consumer education (cited by one cybersecurity expert and two automotive experts) and the integration of AI and machine learning in the systems (cited by two cybersecurity experts). Despite their lower mention frequency, these measures are also noted in the literature. Effective marketing strategies, akin to those used by Tesla, are crucial for showcasing safety and reliability (DGITM/SAGS/EP, 2019), while AI has significant potential in enhancing cybersecurity (K. Kim et al., 2021).

The literature underscored the importance of developing comprehensive cybersecurity measures incorporating encryption, secure software development, and robust industry standards (George et al., 2023; Nash et al., 2024). It also supported the interviewees' calls for transparency and consumer awareness, highlighting the need for public-private partnerships and collective ac-

countability in cybersecurity (World Economic Forum (WEF), 2024).

4.1.5 Is Cybersecurity a Potential Barrier?

The opinions of experts from the automotive and cybersecurity sectors diverged on the significance of cybersecurity for the adoption of self-driving cars.

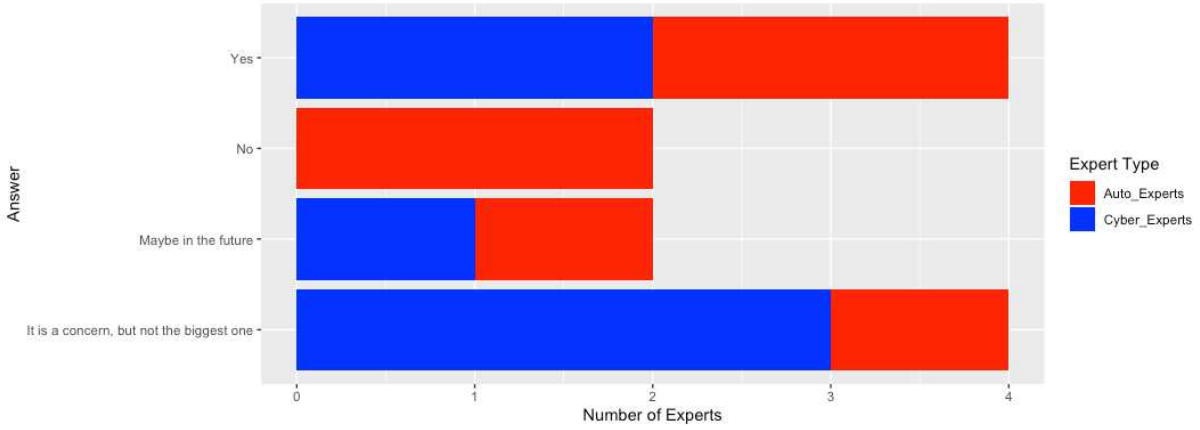

Figure 6: Answers to the question "Based on our discussion, do you feel that cybersecurity concerns are currently a major barrier to the adoption of self-driving cars?" per type of expert

As can be observed, most cybersecurity experts interviewed recognized the significance of security concerns, with five out of six regarding it as a concern. This widespread acknowledgment highlighted a prevalent awareness of security risks associated with emerging technologies. Notably, while half of the cyber experts did not view cybersecurity as the top priority, none entirely disregarded its relevance, and another expert thought that cybersecurity might become increasingly pertinent in the future.

In contrast, auto experts presented a divided front. Two experts expressed cybersecurity concerns, echoing the caution of their cybersecurity counterparts. However, another two did not see cybersecurity as an issue, highlighting a significant divergence in opinions within the group. Adding to the division, one expert considered cybersecurity a potential future concern, while the remaining expert acknowledged it but did not view it as the primary concern.

Considering experts' opinions, JF noted that cybersecurity could be a considerable barrier, much like it has been for autonomous drones, where, despite technological readiness, fear of breaches has halted progress. Similarly, PG pointed out the growing public awareness of cyber threats, which could create significant barriers. As public consciousness about cybersecurity risks grows, the demand for robust security measures becomes imperative, potentially stalling

AV adoption if not addressed convincingly. CR and JB aligned with this viewpoint, stressing the necessity of transparent communication and robust security measures to build consumer trust and facilitate AV adoption. These perspectives are consistent with the Diffusion of Innovation Theory, which suggests that perceived risks and uncertainties can significantly slow down the adoption of new technologies (Rogers, 1962), as well as the Technology Acceptance Model, where building trust through perceived ease of use and usefulness is critical for user acceptance and widespread adoption of new technologies (Davis, 1993).

Conversely, AR and AW contended that while cybersecurity is crucial, it is not the primary barrier to AV adoption. They pointed out that modern vehicles already have technologies susceptible to cyber threats, indicating that the public's lack of awareness means cybersecurity might not be the foremost concern. AW added that the success of AVs hinges more on the quality of AI and system reliability than on cybersecurity alone. With appropriate measures, cybersecurity risks can be effectively managed.

FM and JS downplayed cybersecurity as a significant obstacle, considering it one of many issues to resolve. While FM advised prioritizing technological development and operationalizing AVs, with cybersecurity addressed later, JS believed early adopters would embrace the technology despite potential cybersecurity concerns, suggesting that brand reliability would influence consumer decisions more than cybersecurity concerns alone, sharing a similar view presented by Rogers (1962).

ES highlighted the industry's responsibility to mitigate cybersecurity risks to protect brand reputation and market position. She stressed that maintaining consumer trust and preventing incidents that could damage reputations are vital, arguing that ensuring cybersecurity is about competitive performance and long-term success, not just compliance, aligning with the concept of dynamic capabilities (Teece et al., 1997).

EC and PR offered a nuanced view of cybersecurity's evolving importance. EC agreed with JS and ES, noting that while cybersecurity concerns are significant, they are not seen as major barriers by the average consumer, who prioritizes brand reputation, cost, and convenience. However, he insisted on the necessity for stringent cybersecurity regulations and standards to protect consumers and build trust in AV technology. PR echoed this sentiment, predicting that cybersecurity will become crucial in consumer decision-making as AVs become more prevalent. He pointed out the vulnerability of interconnected vehicles to cybersecurity threats, drawing parallels to the

IoT industry and urging the implementation of robust security measures.

In line with PR's comments, LS also viewed cybersecurity as a future concern that needs addressing. He emphasized the potential impact of cybersecurity failures, such as traffic disruptions or accidents, which are easily understood by the public and could significantly affect AV adoption. He also advocated for gradually introducing autonomous functionalities to manage cybersecurity issues effectively over time.

Despite their different backgrounds, the experts shared several standard views. Across both sectors, there was an extensive acknowledgment that cybersecurity risks are real and must be addressed. Most experts agreed that AVs could be vulnerable to attacks that compromise safety and functionality without robust cybersecurity measures. There was also a shared understanding that effective cybersecurity strategies are essential. This included continuous monitoring, secure communication protocols, and comprehensive security frameworks to protect AVs from potential threats.

However, the experts' perspectives also diverged significantly, as cybersecurity experts tended to view cybersecurity as a more significant barrier compared to automotive experts. Cybersecurity professionals emphasized the growing public awareness and potential scrutiny that could stall AV adoption. In contrast, automotive experts saw cybersecurity as one of many technical challenges that needed to be managed, not a fundamental roadblock. Automotive experts typically view cybersecurity as a post-launch issue that requires attention after the technology becomes operational, whereas cybersecurity experts argue that these risks need early and continuous attention throughout the development process.

The literature review provided a broader context that supported and enriched the expert opinions. It underscored the critical need for comprehensive cybersecurity measures, such as encryption, secure communication protocols, and continuous monitoring and updating. This was in line with the experts' views on the importance of robust security frameworks to protect AVs from cyber threats (George et al., 2023; TechVertu Cyber Security, 2024).

The literature also accentuated the significant impact of public perception on adopting AVs. High-profile cybersecurity incidents and media coverage can amplify fears and skepticism, influencing consumers' willingness to embrace the technology. This aligned with the cybersecurity experts' focus on growing public awareness and the potential for scrutiny (Eliot, 2021; Stagnaro, 2023) as well as reflecting the Diffusion of Innovation Theory, especially the impor-

tance of the early adopters' role on technology adoption (Rogers, 1962).

Furthermore, both the literature and expert opinions stressed the need for effective regulatory frameworks to address cybersecurity concerns. Such regulations can provide a safety net, build consumer confidence, and ensure that AVs meet stringent security standards (Sirisup & Petchmark, 2022). This is consistent with the dynamic capabilities framework, where firms must adapt to regulatory changes and ensure that their internal processes align with external requirements to remain competitive and secure (Teece et al., 1997).

Lastly, the literature also pointed out the challenges of integrating new cybersecurity measures into existing vehicle designs. The complexity of AV systems and their interdependencies create potential vulnerabilities that need to be addressed from the outset. This resonated with the experts' views on the necessity of secure design and continuous security assessments (Morris et al., 2020).

4.2 Current levels of public concerns regarding self-driving cars

The survey results (n = 239) were used to make generalizations about consumer acceptance, and conclusions were drawn between the findings and the literature discussed in Chapter 2. The final conclusions regarding consumer acceptance are detailed in Chapter 5.1.

4.2.1 General Familiarity and Perception of AVs

The first set of questions assessed the baseline understanding and initial perceptions of autonomous vehicles. The literature (see Chapter 2.4.4) showed that prior usage, interaction, or even knowledge of the technology behind would be essential factors concerning the adoption of self-driving cars (DGITM/SAGS/EP, 2019).

The first question asked respondents whether they had ever used or interacted with an autonomous vehicle. 78.7% affirmed that they have used/interacted with them, while 21.3% have neither used nor interacted with them.

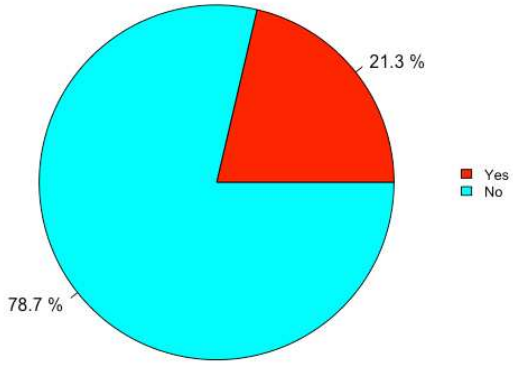

Figure 7: Answer distribution of question 1

Then, respondents were asked to rate their familiarity with the concept of self-driving cars and the technology behind them on a scale from 1 (not familiar at all) to 5 (extremely familiar).

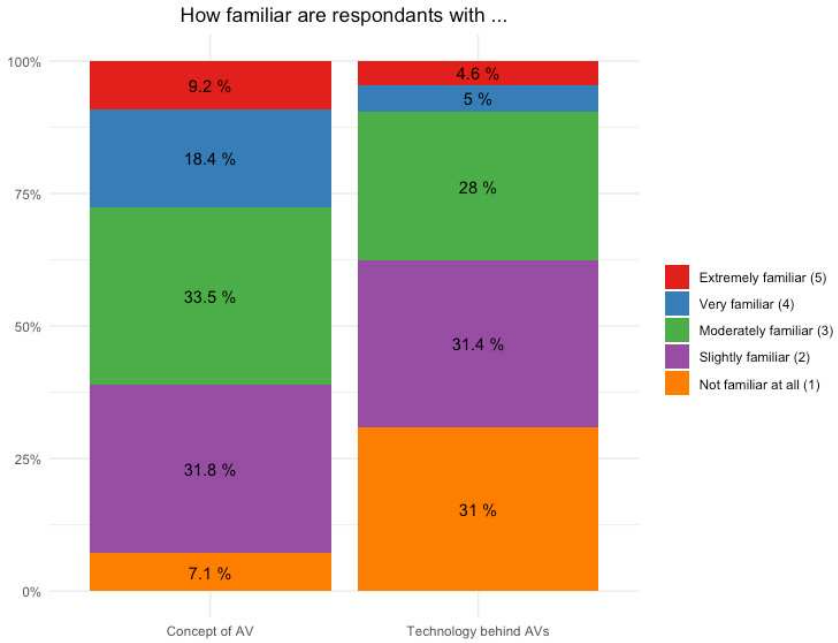

Figure 8: Answer distribution of questions 2 and 3

According to the research, 31.8% of respondents had a slight familiarity with the idea of AVs, while 33.5% had a moderate familiarity. On the other hand, only 37.6% of respondents were at least moderately familiarized with the technology underlying AVs. Notably, 62.4% of respondents knew very little to nothing about the technology underlying AVs, with 31% knowing nothing and 31.4% knowing just a little. On the other hand, only 7.1% of respondents did not know what AVs are, which suggests that while most people are aware of the idea, there is still a substantial knowledge gap on the underlying technology.

Lastly, respondents were presented with three statements regarding their agreement with the correlation between AVs and safety, comfort, and disruption capacity. Using a scale of one (strongly disagree) to five (strongly agree), respondents expressed different levels of agreement with each statement.

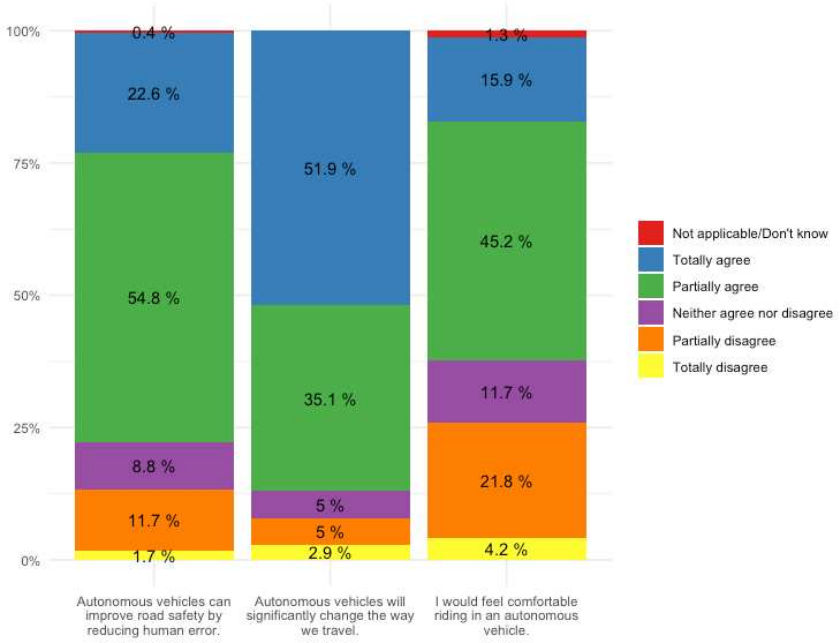

Figure 9: Answer distribution of question 4

In terms of safety improvement, a significant majority, 54.8%, partially agreed that AVs can improve road safety by reducing human error. Additionally, 22.6% totally agreed, and only 1.7% totally disagreed; in terms of impact on travel, over half of the respondents, 51.9%, totally agreed that AVs would significantly change the way we travel. Another 35.1% partially agreed, while only 2.9% totally disagreed. Lastly, opinions were more varied regarding comfort with riding in an AV. While 45.2% partially agreed and 15.9% totally agreed, a higher 21.8% partially disagreed and 4.2% totally disagreed.

These results indicate that while respondents were generally optimistic about AVs' safety and transformative potential, there were mixed feelings about personal comfort when riding in one.

4.2.2 Willingness to Adopt AVs of Different Levels

The literature (see Chapter 2.4.4) has also shown that different levels of autonomy would mean different acceptance rates (Prasetio & Nurliyana, 2023).

For this reason, this question asked the respondents on a scale of 1 to 5 their willingness to

adopt vehicles with each type of autonomy level, from level 0 (no autonomy at all) to level 5 (full autonomy, no human intervention).

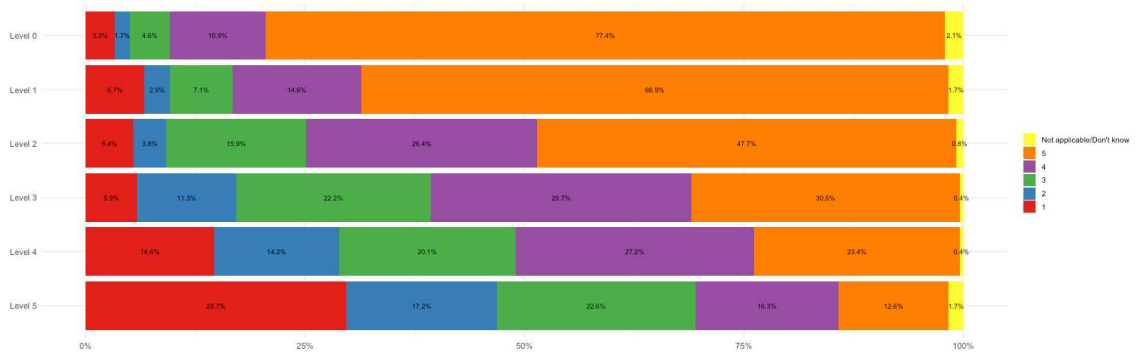

Figure 10: Answer distribution of question 5

As expected, different levels of autonomy corresponded to various levels of acceptance, and despite the numbers varying, the overall trend remained quite similar (Prasetio & Nurliyana, 2023). For Levels 0 to 2, the maximum willingness to adopt decreased slightly, but the combined percentages of the higher acceptance ratings (3 to 5) remained virtually the same. However, starting from Level 3, the willingness to adopt AVs began to decrease rapidly. At Level 5, almost half of the respondents (47.9%) showed little to no desire to adopt vehicles with total autonomy.

Christensen's insights in *The Innovator's Dilemma* shed light on varying consumer attitudes toward autonomous vehicles. As companies develop increasingly autonomous technologies, they may confront a challenge: balancing the needs of current customers with the disruptive potential of these innovations, which could profoundly reshape consumer behavior. This dynamic is reflected in the survey findings, where willingness to adopt declines as autonomy levels rise, possibly due to concerns about the disruptive impact of highly autonomous vehicles (Christensen et al., 2015).

4.2.3 Cybersecurity Awareness and Concerns

This set of questions explicitly addressed participants' concerns about cybersecurity threats like unauthorized access to personal data, remote hijacking, and software attacks. These concerns reflected the literature's findings on the potential impact of cybersecurity on consumer trust and willingness to adopt this new technology (DGITM/SAGS/EP, 2019; Eliot, 2021; Stagnaro, 2023).

Firstly, respondents were presented with three cybersecurity risks (unauthorized access to personal data, remote hijacking, and software attacks), which should be evaluated on a scale from 1 to 5 on their level of concern, with 1 being not concerned at all and 5 being very concerned.

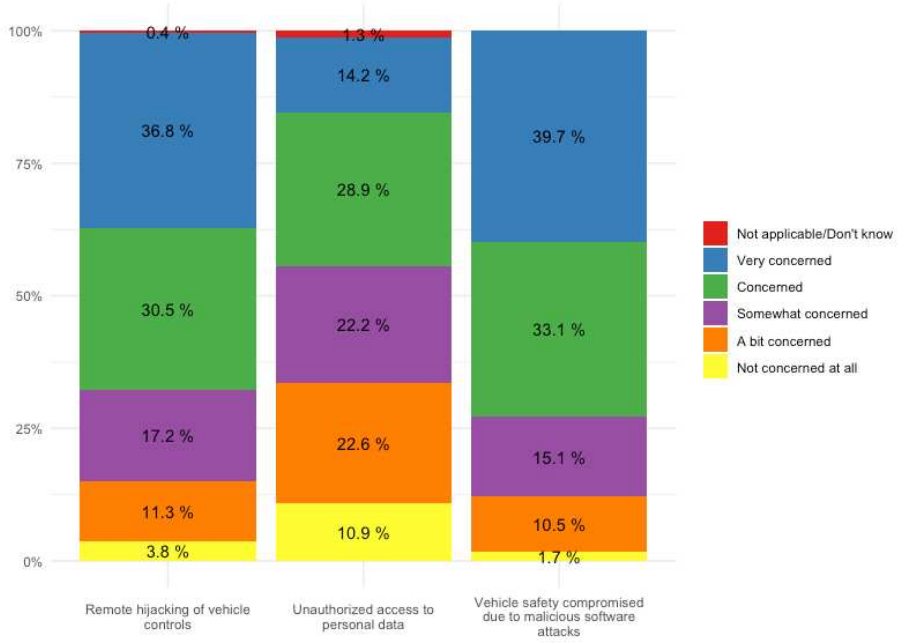

Figure 11: Answer distribution of question 6

As observed above, respondents recorded different levels of concern for each threat. A majority of respondents, 36.8%, were very concerned, and 30.5% were concerned with remote hijacking of vehicle controls, while only 3.8% were not concerned at all.

Only 14.2% were very concerned about unauthorized access to personal data, and 28.9% were concerned about this threat, while a third of the respondents had little to no concerns. This threat was the least important for the survey's respondents.

Finally, high levels of concern were observed, with 39.7% very concerned, 33.1% concerned, and only 1.7% not concerned at all, regarding the compromise of vehicle safety due to malicious software attacks.

These results showed that respondents are significantly concerned about cybersecurity threats, with the highest concerns about vehicle safety being compromised due to malicious software attacks and the possibility of remote hijacking of AV controls. These numbers were similar to the ones presented in the literature, where 73% of potential users were also concerned about hacker attacks on the vehicle or system security (Stagnaro, 2023).

Also, this high level of concern among respondents corroborates the expert opinions, particularly those of PR and PG, who highlighted remote hijacking and software attacks as primary cybersecurity threats. For instance, PR stressed the catastrophic potential of remote control takeovers, which mirrors the survey respondents' significant concern about these threats.

Respondents were then asked if they were aware of any cybersecurity incident involving AVs, to which one-sixth answered yes, more than 70% said no, and about 12% said that they were not sure.

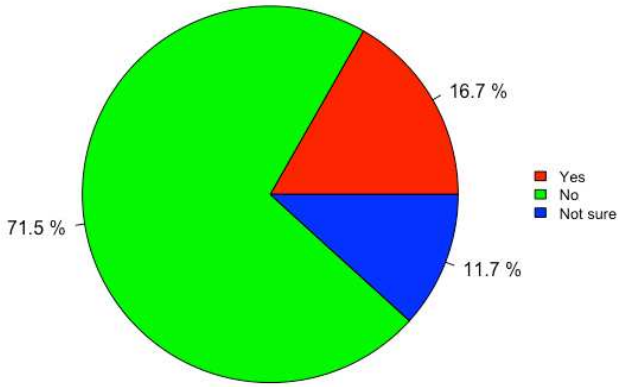

Figure 12: Answer distribution of question 7

Lastly, three statements were presented to the respondents, asking them to indicate whether cybersecurity is a significant concern for them, whether they trust cybersecurity measures, and whether the possibility of cybersecurity breaches deters them from adopting AVs. Respondents indicated varying degrees of agreement with each statement on a scale ranging from one (strongly disagree) to five (strongly agree).

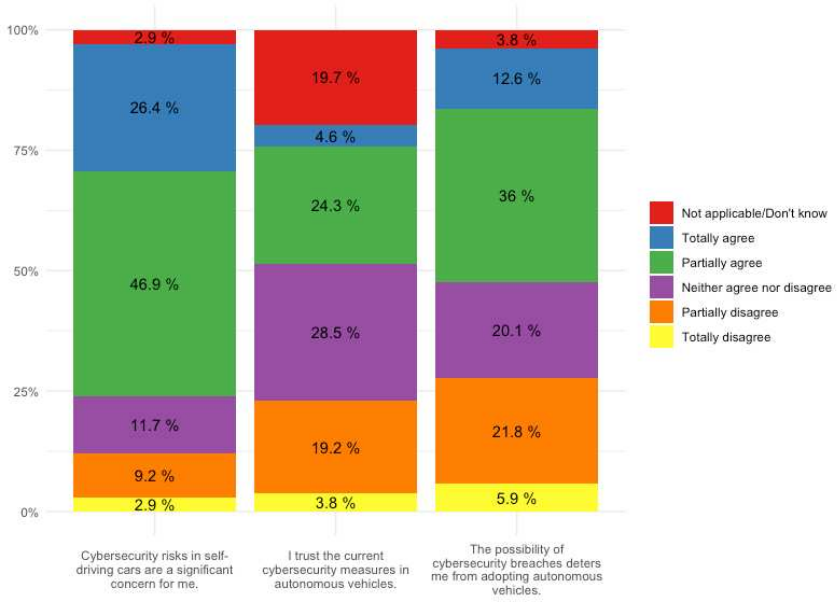

Figure 13: Answer distribution of question 8

Regarding the first statement, 46.9% of respondents partially agreed that cybersecurity risks in self-driving cars were a significant concern, while 26.4% totally agreed. Only a small percentage, 2.9%, totally disagreed, indicating widespread concern about cybersecurity risks among respondents.

For the second statement, 24.3% of respondents partially agreed that they trust the current cybersecurity measures in autonomous vehicles. However, a significant portion, 28.5%, neither agreed nor disagreed, and 19.7% did not know how to answer this statement, indicating uncertainty about the effectiveness of these measures. Furthermore, 23% disagreed with the statement, either partially or totally, reflecting some lack of trust in current cybersecurity measures.

In response to the third statement, 36% of respondents partially agreed that the possibility of cybersecurity breaches deters them from adopting AVs. On the other hand, 21.8% partially disagreed, and 5.9% totally disagreed, showing that while concerns about cybersecurity breaches impact adoption willingness, there were different levels of apprehension.

4.2.4 Willingness to Adopt AVs of Different Levels After Cybersecurity Awareness and Concerns

The same questions from Chapter 4.2.2 were posed once again, following cybersecurity awareness and potential concerns, to determine if there were statistically significant differences between the initial questions and these ones.

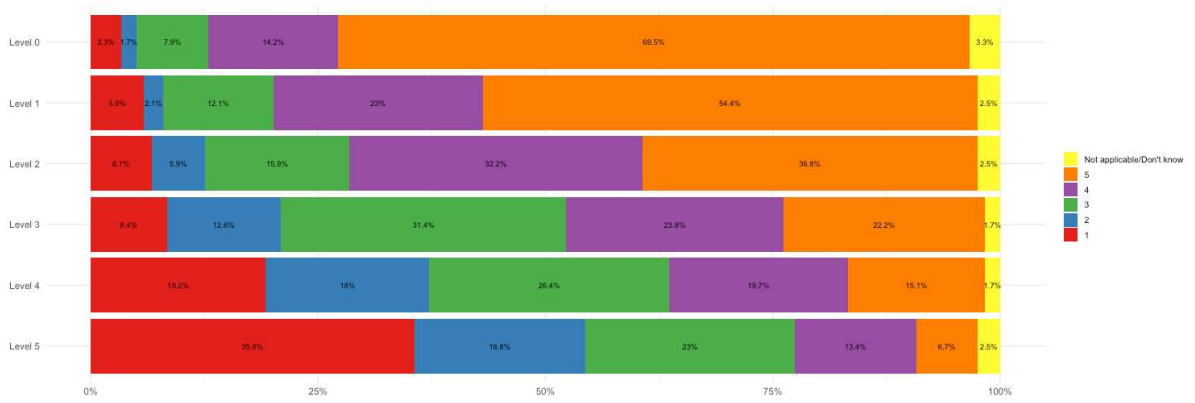

Figure 14: Answer distribution of question 9

As can be observed, the numbers were partially similar to those shown in Chapter 4.2.2, but there were some notable differences.

While the lowest levels of willingness to adopt AVs at levels 0, 1, and 2 remain similar, the percentages of respondents indicating maximum willingness (5) decreased across all levels compared to the initial responses. For Level 0, the maximum willingness decreased from 77.4% to 69.5%; for Level 1, it decreased from 66.9% to 54.4%; and for Level 2, from 47.7% to 36.8%. Instead, there was an increase in responses indicating more moderate willingness (3 or 4) to accept these lower levels of autonomy.

When analyzing the higher levels of autonomy (levels 3, 4, and 5), the willingness to adopt AVs was visibly lower. The higher levels of willingness decreased significantly. For instance, for level 3, the maximum willingness decreased from 30.5% to 22.2%. For Level 4, it decreased from 23.4% to 15.1%. Primarily at Level 5, the maximum willingness decreased from 12.6% to 6.7%, while the percentage of respondents showing little to no willingness to adopt increased significantly, with Level 4 autonomy showing an increase from 14.6% to 19.2% for the lowest willingness, and more than a third of respondents (35.6%) indicating low willingness for Level 5 autonomy.

This confirms what was seen in the literature, stating the potential impact of cybersecurity on consumer trust and willingness to adopt AVs (DGITM/SAGS/EP, 2019; Eliot, 2021; Stagnaro, 2023). However, the statistical significance of the differences between the two questions will be tested later in Chapter 4.2.7.

4.2.5 Adoption and Acceptance of AVs

The literature (see Chapter 2.5.4) noted that social, psychological, and cognitive factors, where consumer emotions and risk perceptions play pivotal roles, influence the acceptance and adoption of new technologies.

The questions in this set incorporated the Technology Acceptance Model, assessing the trade-offs between perceived benefits and cybersecurity risks, suggesting that effective cybersecurity measures can foster adoption by alleviating perceived risks (George et al., 2023).

The first question asked respondents to rate their level of agreement with two statements, one concerning whether the benefits of self-driving cars outweighed their cybersecurity risks and the other regarding whether, if cybersecurity concerns were adequately addressed, respondents would prefer a self-driving car.

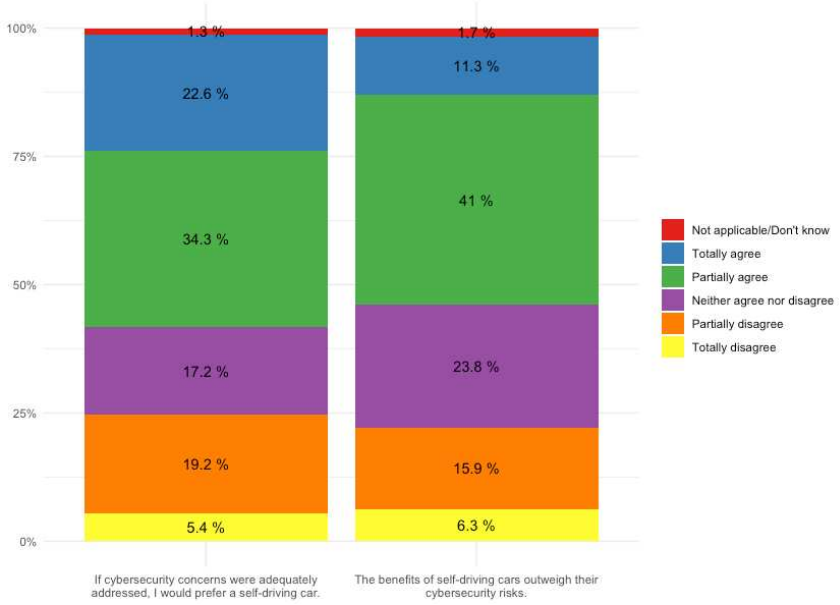

Figure 15: Answer distribution of question 10

The results indicated that a significant portion of respondents (56.9%) would prefer self-driving cars if cybersecurity concerns were adequately addressed. This points to a strong potential market for autonomous vehicles, contingent on resolving cybersecurity issues. However, when evaluating whether the benefits of self-driving cars outweigh their cybersecurity risks, a slightly smaller, yet still majority percentage (52.3%) agreed. This demonstrates that there is general openness to self-driving vehicles despite a significant degree of concern about cybersecurity risks.

This discrepancy between these figures points to a potential conditional acceptance among certain respondents. Many were willing to adopt self-driving cars, but their willingness hinged on effective cybersecurity measures. The percentages of partial and total disagreement (24.6% for preference if concerns addressed and 22.2% for benefits outweighing risks) still underscore the necessity for robust cybersecurity solutions to foster consumer trust for an important fraction of the consumers. This trend converged with the literature, implying that addressing cybersecurity concerns is crucial for accepting and adopting autonomous vehicles (Tomorrow Bio, 2023).

These results align with the expert opinions, particularly those of PG, who stressed that addressing cybersecurity risks is essential for fostering trust and acceptance. The survey respondents' conditional acceptance based on effective cybersecurity measures reflects this expert insight.

On another important note, it is possible to associate these results with the diffusion of innovation theory, as perceptions of safety and cybersecurity can significantly impact the adoption of autonomous vehicles, as well as the TAM, since robust cybersecurity measures can enhance adoption by mitigating perceived risks, indicating the importance of perceived usefulness and ease of use (Davis, 1993; Rogers, 1962).

Then, respondents were asked to rank the importance of safety, cybersecurity, convenience, cost, and environmental impact on a scale of 0 to 100 when considering the adoption of AVs. The results can be observed in Figure 16.

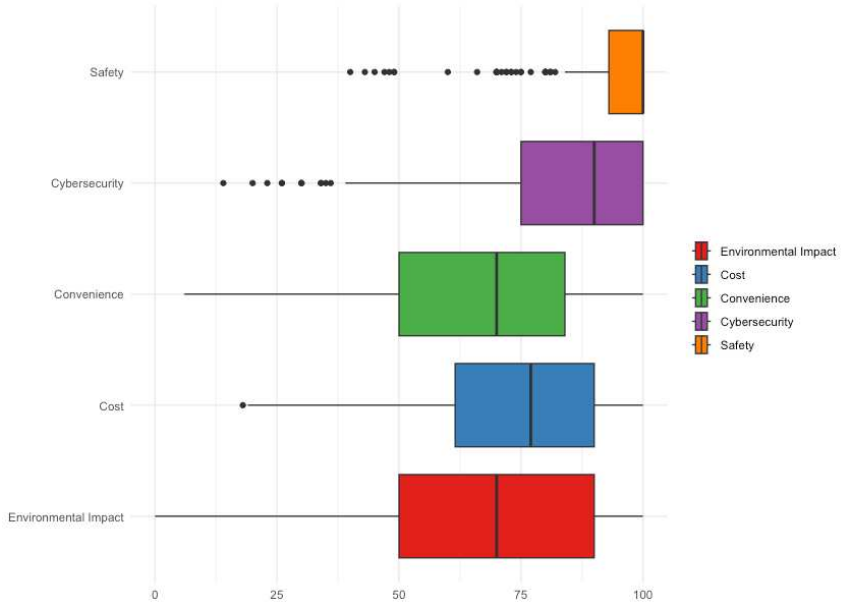

Figure 16: Answer distribution of question 12

The most important factor for respondents was safety, as evidenced by the narrow distribution and high median value near 100. Cybersecurity was the second most critical factor, with a slightly wider distribution but still a high median. Convenience and cost had moderate importance, with broader distributions indicating varying levels of concern among respondents. Environmental impact showed the most comprehensive distribution, indicating diverse opinions but maintaining a relatively high median value. These results showed that while all factors were considered essential, safety and cybersecurity stood out as the primary concerns for potential adopters of AVs.

In this context, it is essential to remember that expert JF's comparison of the importance of cybersecurity in AVs to other critical sectors underscores the necessity of solid security frameworks to gain consumer trust. The survey results, showing safety and cybersecurity as top concerns, align with these expert insights.

To test the hypothesis presented in the literature, respondents were asked how likely they would be to use an autonomous vehicle (AV) for daily commuting if AVs had a proven strong record of cybersecurity, rated on a scale from 1 (extremely unlikely) to 5 (extremely likely).

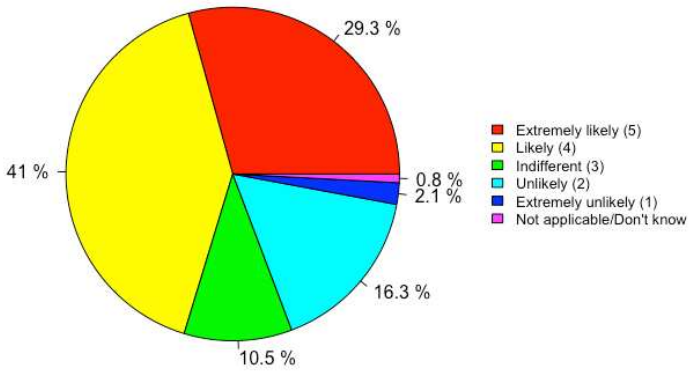

Figure 17: Answer distribution of question 13

The distribution showed that a significant portion of respondents, 41%, were likely to use AVs for daily commuting if cybersecurity concerns were addressed. This was followed by 29.3% who showed the highest likelihood of using AVs under these conditions. Additionally, 16.3% of respondents were unlikely, while 10.5% were indifferent, and a small percentage, 2.1%, were extremely unlikely to use AVs for commuting.

This distribution indicated that a majority of respondents (70.3%) would consider using AVs for

daily commuting if they had a strong record of cybersecurity, coinciding with literature that suggests guarantees of safety positively impact consumer perceptions (Tomorrow Bio, 2023). This strong inclination towards adoption underlines the critical role of cybersecurity in influencing consumer acceptance of autonomous vehicles.

Subsequently, respondents were asked about factors that would make them more willing to use self-driving cars. They could choose one or more of the following options: enhanced cybersecurity, a proven safety record, lower costs, or personal enjoyment.

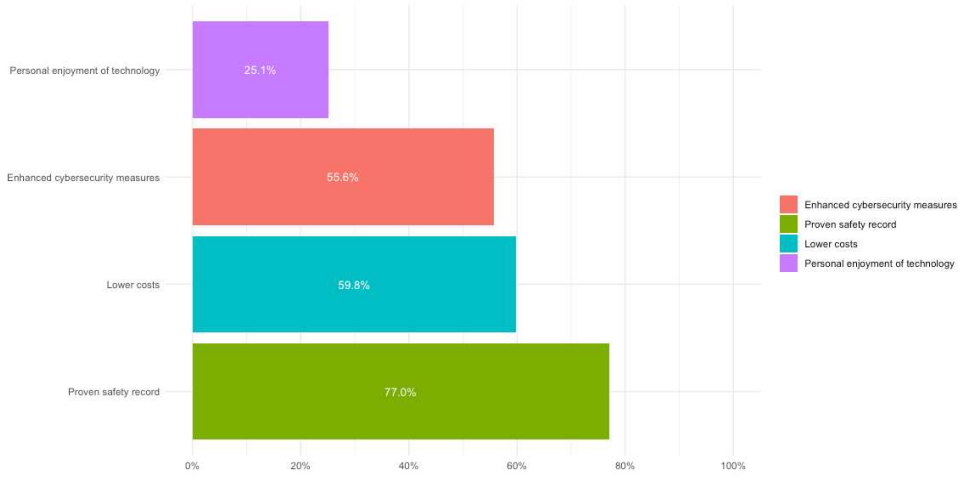

Figure 18: Answer distribution of question 14

The graph above reveals that 77.0% of respondents chose a proven safety record as the most significant factor that would increase their willingness to use self-driving cars. This was followed by 59.8% of respondents selecting lower costs, while 55.6% chose enhanced cybersecurity measures. Personal enjoyment of technology was the least influential factor, selected by only 25.1% of respondents.

These results confirmed that safety is the paramount concern for the majority of respondents when it comes to adopting self-driving cars. The significant emphasis on cost and cybersecurity further stressed the importance of addressing practical and security-related concerns to increase consumer willingness to adopt this technology.

Finally, financial factors were analyzed. Respondents were asked how much more they would pay for enhanced cybersecurity features in an AV, assuming the cost would be the same as a traditional vehicle.

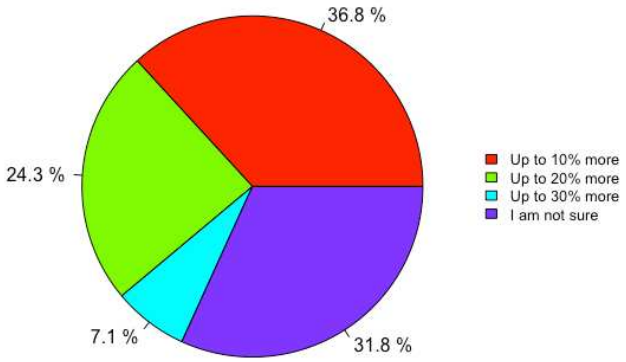

Figure 19: Answer distribution of question 15

As can be observed, the majority of respondents, 61.1%, were not willing to pay more than 20% extra for enhanced cybersecurity features in an AV. These results highlighted that, while there was a willingness to pay extra for improved cybersecurity, most respondents were only comfortable with a modest increase in cost. A significant percentage of respondents who were unsure (31.8%) indicated uncertainty or a need for more information regarding the value and benefits of enhanced cybersecurity features in autonomous vehicles.

4.2.6 Demographics and Background

Analyzing the demographic characteristics of respondents through the lens of Dynamic Capabilities can yield valuable insights into how firms can respond to how diverse age groups and educational backgrounds perceive and adapt to emerging technologies like autonomous vehicles. This knowledge can empower firms to tailor strategies and marketing approaches, ensuring alignment with the evolving external environment and thereby enhancing their overall performance (Barreto, 2010; Teece et al., 1997).

Figure 20 illustrates that the age distribution was predominantly skewed towards the younger segments.

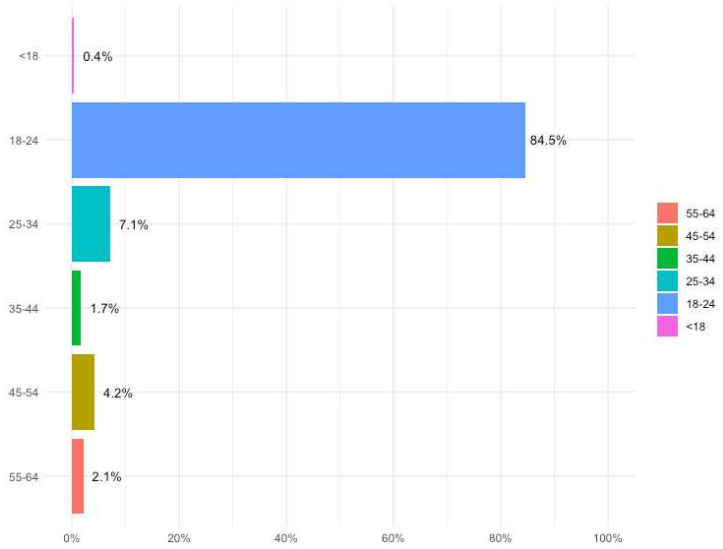

Figure 20: Answer distribution of question 16

More than three-quarters of the participants, 84.5%, fell within the 18-24 age bracket. A smaller percentage, 7.1%, belonged to the 25-34 age range, while only a minority were aged 35 and above. Specifically, 1.7% were in the 35 to 44 age range, 4.2% in the 45 to 54 age range, and 2.1% in the 55 to 64 age range. Additionally, a very small percentage, 0.4%, were under 18 years old.

This age distribution was predominantly younger individuals, particularly those between 18 and 24.

Regarding gender, a slight majority of the population was male (n = 120), with a close percentage of female population (n = 119).

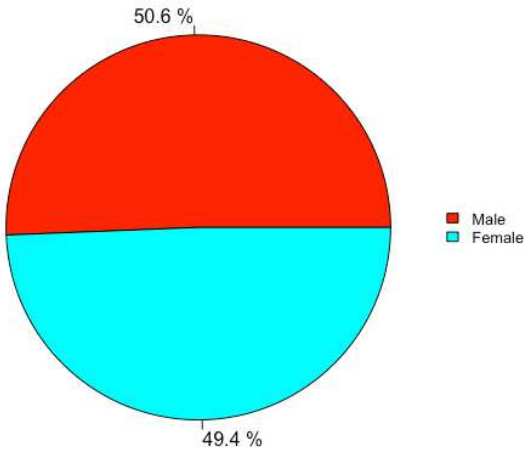

Figure 21: Answer distribution of question 17

Analyzing nationalities, most respondents of this survey were Portuguese, who made up 81.6% of total respondents. The remaining respondents came from a variety of countries. Specifically, 2.9% of respondents were from Italy, the same percentage from Spain, 2.1% from France, and 1.7% each from Argentina, the US, and Germany. Additionally, 0.8% of respondents were from Brazil, with the same percentage also from Mexico, and 0.4% each from Norway and the Netherlands. Lastly, 2.9% of respondents were from other countries.

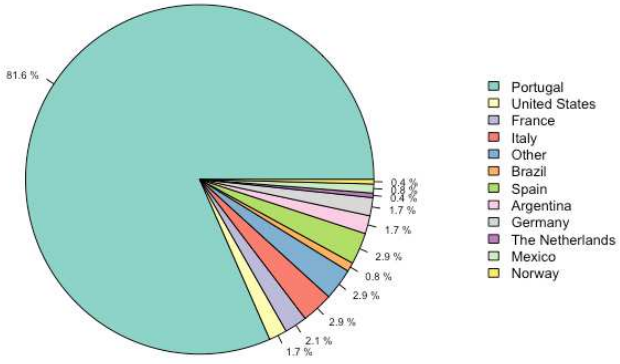

Figure 22: Answer distribution of question 18

This distribution shows a strong dominance of Portuguese respondents, which may have influenced the survey's overall findings. The diversity among the smaller portions of other nationalities added a broader perspective but was significantly outweighed by the Portuguese majority.

Education-wise, most respondents had either a high school or a bachelor's degree. Specifically, 35.1% of respondents were high school graduates, and 46.4% had a bachelor's degree. A smaller proportion, 15.9%, had a master's degree, and 0.4% had a professional degree. Only a few respondents, 0.8%, had a doctorate, and 1.3% had less than a high school education.

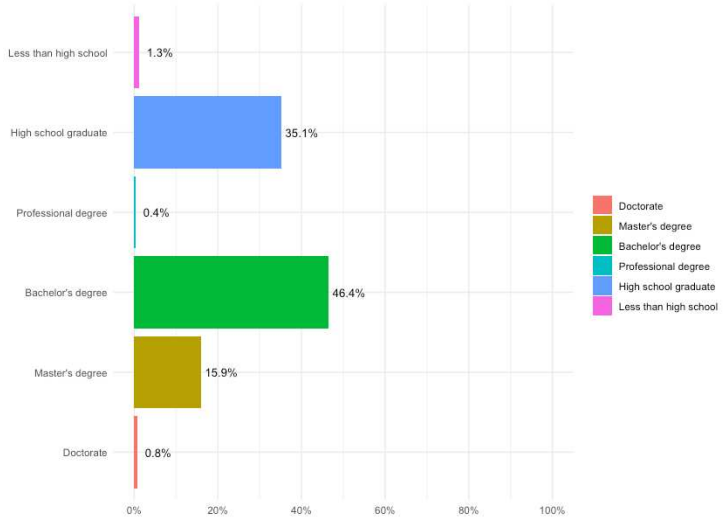

Figure 23: Answer distribution of question 19

This educational distribution revealed that the survey sample was well-educated, with a significant portion having completed higher education. This may have influenced the results, as individuals with higher education levels might have different perspectives on technology and autonomous vehicles than those with less formal education.

Regarding income, most respondents reported incomes before taxes between €40,000 and €59,999 (15.1%) and €20,000 and €39,999 (15.1%). This was followed by those earning less than €20,000 (12.1%), €60,000 to €79,999 (10.0%), and €80,000 to €99,999 (7.5%). A smaller proportion reported incomes of more than €150,000 (6.7%), while 2.9% reported incomes between €100,000 and €149,999. However, a significant portion of respondents, 30.5%, preferred not to disclose their income.

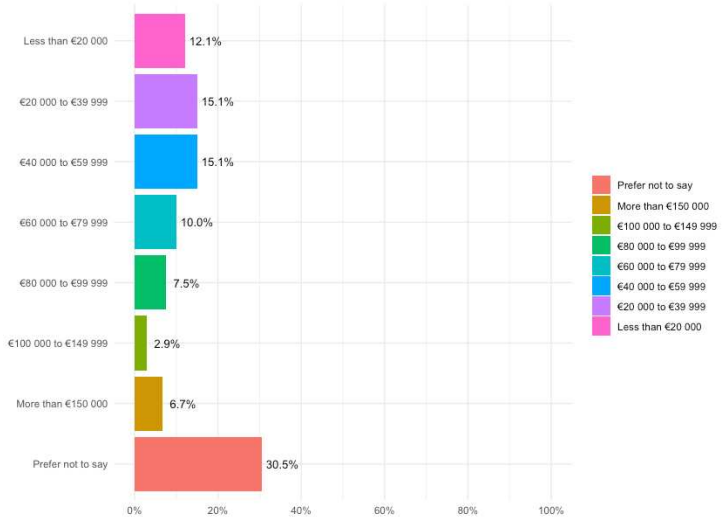

Figure 24: Answer distribution of question 20

The high percentage of respondents who preferred not to disclose their income may have affected income analysis regarding the adoption of autonomous vehicles. This nondisclosure suggests caution in interpreting the income data, as it may not fully represent the financial backgrounds of survey participants.

The respondents also showed a diverse distribution in terms of political affiliation — specifically, 11.7% identified as conservative, 30.1% as liberal, and 25.1% as moderate. A smaller portion, 12.1%, was non-affiliated. Additionally, 3.3% selected "Other", and a non-negligible portion, 17.6%, opted not to disclose their political affiliation.

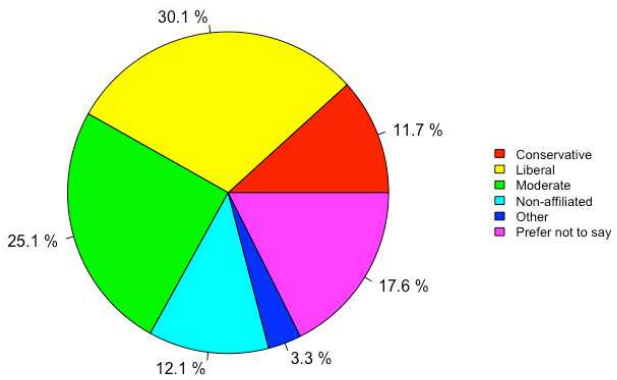

Figure 25: Answer distribution of question 21

As with the income variable, the high percentage of respondents in the non-affiliated, other, and prefer not to say categories made it challenging to assess correlations between political affiliation and adopting autonomous vehicles. This lack of precise distribution across different political orientations means that caution is needed when concluding that political beliefs influence AV adoption.

Another important subject for the analysis was the respondents' primary mode of transportation.

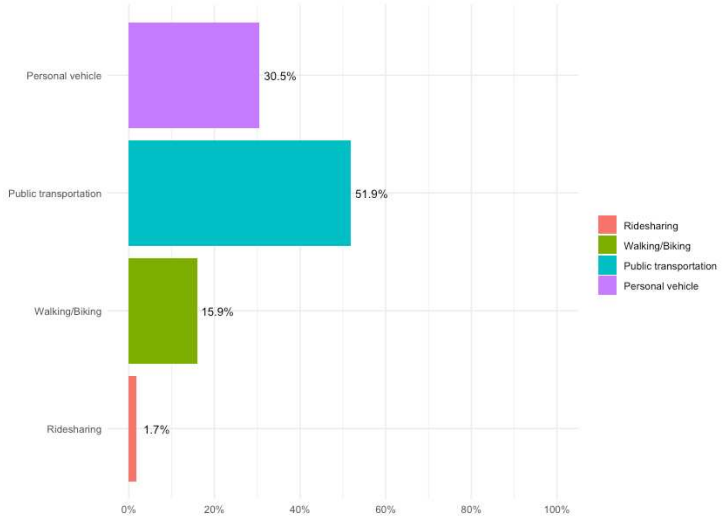

Figure 26: Answer distribution of question 22

The distribution of responses was as follows: 51.9% of respondents primarily used public transportation, making it the most common mode of transport among the survey participants. This was followed by 30.5% who primarily used a personal vehicle. Walking or biking was the primary mode of transport for 15.9% of respondents, while only 1.7% primarily used ridesharing services. This distribution highlights respondents' reliance on public transportation and personal vehicles.

Lastly, since this study involved cars, it is essential to know what percentage of the population held a valid driver's license.

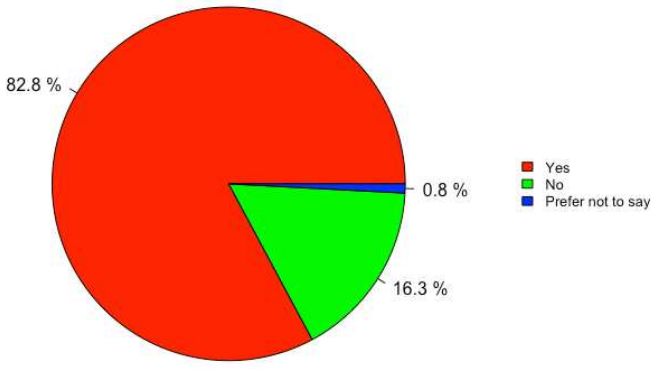

Figure 27: Answer distribution of question 23

The majority of respondents, 82.8%, reported that they had a valid driver's license. Meanwhile, 16.3% of respondents did not hold a valid driver's license, and a small fraction, 0.8%, preferred not to say. This distribution indicated that the vast majority of respondents were licensed drivers,

which is relevant for understanding their familiarity and comfort with vehicles in general.

In Chapter 5.2.2, limitations are explained related to the sample population.

4.2.7 Differences in Adoption of AVs at Different Autonomy Levels Before vs. After Cybersecurity Awareness

This section examines whether respondents' willingness to adopt autonomous vehicles (AVs) at various levels of autonomy changed significantly after being exposed to cybersecurity concerns. The analysis employed a paired sample t-test to compare the responses to Question 5 (before cybersecurity information) and Question 9 (after cybersecurity information).

A t-test is appropriate for this analysis because it assesses whether there are notable distinctions between two related groups (Liang et al., 2019). Here, each participant's willingness to adopt AVs at different autonomy levels served as both pre-test and post-test observations, with the introduction of cybersecurity threats being the intervening factor.

The null hypothesis (H_0) for this analysis was:

> H_0: There is no significant difference in the willingness to adopt autonomous vehicles at different levels of autonomy before and after exposure to cybersecurity information.

This hypothesis implies that cybersecurity concerns did not influence or alter the decision-making process regarding the adoption of AV technology.

The alternative hypothesis (H_1) posits:

> H_1: There is a significant difference in the willingness to adopt autonomous vehicles at different levels of autonomy before and after exposure to cybersecurity information.

This hypothesis implies that cybersecurity information influenced respondents' perceptions and, potentially, their willingness to adopt AV technology.

The t-test pairs pre-information exposure scores (responses to Question 5) with the corresponding post-information exposure scores (responses to Question 9). The analysis calculated the mean difference, the standard deviation of the difference, and the p-value.

An analysis of the results will be presented where:

- A p-value less than 0.05 calls for rejecting the null hypothesis, suggesting that cybersecurity concerns significantly affect willingness to adopt AVs.

- A p-value higher than 0.05 provides evidence in favor of the null hypothesis, suggesting that cybersecurity concerns did not have a significant effect on willingness to adopt.

Comparison	Mean Diff	SD of Diff	P-Value	Result
Level0_before vs. Level0_after	0.130	0.641	2.28e-03	Very significant
Level1_before vs. Level1_after	0.134	0.693	3.64e-03	Very significant
Level2_before vs. Level2_after	0.210	0.672	3.13e-06	Extremely significant
Level3_before vs. Level3_after	0.285	0.739	1.19e-08	Extremely significant
Level4_before vs. Level4_after	0.370	0.724	1.64e-13	Extremely significant
Level5_before vs. Level5_after	0.280	0.797	2.08e-07	Extremely significant

Table 4: Paired Sample t-Test Results for Willingness to Adopt AVs at Different Autonomy Levels

As can be observed, the p-values for the differences observed were below 0.01 at levels 0 and 1 (very significant) and below 0.001 for the remaining levels (extremely significant).

These findings demonstrate that consumers generally decreased their willingness to accept AVs across all levels of autonomy after respondents were informed about cybersecurity concerns. Notably, the p-values decreased as the level of automation increased, with the exception of level 5, suggesting that the differences were more significant at higher levels of automation.

This implied that generally, higher autonomy levels corresponded to more statistically significant differences in responses before and after exposure to cyber threat information, as evidenced by Table 4 and the responses shown in Chapter 4.2.4.

This finding is consistent with insights from expert interviews, where cybersecurity professionals, including PG, emphasized the crucial role of cybersecurity awareness in the acceptance of AV technologies. They observed that greater awareness of potential threats typically increases consumer caution. Additionally, experts like PR and AR pointed out that as vehicle automation levels rise, the complexity and potential risks of cybersecurity threats also escalate, which may account for the more pronounced differences observed at higher levels of autonomy.

The findings of this analysis also align with the Technology Acceptance Model, as cybersecurity concerns directly impact perceived usefulness and perceived ease of use, thereby influencing willingness to adopt AVs. The decrease in willingness to adopt across all levels of autonomy after cybersecurity information exposure reflects how perceived threats can lower these perceptions, thereby affecting adoption decisions (Davis, 1993).

The concept of dynamic capabilities is also relevant here. Firms that develop strong dynamic capabilities in cybersecurity can better adapt to these concerns, ensuring their AV technologies are perceived as safe and reliable. This adaptability can mitigate the negative impact of cybersecurity concerns on consumer willingness to adopt AVs, emphasizing the strategic importance of dynamic capabilities in maintaining high performance in the evolving AV market (Teece et al., 1997).

Interestingly, even for level 0 and level 1 vehicles, which constitute the majority of current cars on the roads and have no or minimal automation, there was still a statistically significant difference between responses before and after exposure to cybersecurity concerns. This suggests that despite having little to no exposure to such threats, respondents generally became more averse to adopting a "normal car", which could indicate an "irrational" or emotional aspect pertaining to fears associated with cybersecurity.

This insight aligns with some expert views, particularly those of PR, who noted that even minimal automation levels could trigger significant concerns due to general apprehensions about cybersecurity, indicating an emotional response to perceived threats.

4.2.8 Determinants of consumers' willingness to adopt AVs

The analyses and the literature (see Chapter 2) were used to develop linear regression models that identified factors affecting willingness. The outcomes were examined in Chapter 5.1, leading to conclusions about acceptance levels and the implications of cybersecurity concerns.

This subchapter presents the regression analysis conducted to understand the relationships between various independent variables and a set of dependent variables, which represent different levels of willingness to adopt autonomous vehicles with varying levels of autonomy (from 0 to 5) before and after the "exposure" to cybersecurity concerns and threats.

The independent variables are derived from the responses to the survey questions, with each variable corresponding to a specific question in the survey. The questions cover the various aspects presented in the previous subsections, such as familiarity with the concept and technology of AVs, agreement with statements on AVs, willingness to adopt AVs, and concerns about cybersecurity.

All Likert scale responses were converted to corresponding numeric codes, each mapping to a number. For the purposes of regression analysis, responses such as "Not sure" and "Prefer not

to say" were treated as missing values (NAs). By eliminating non-ordered categorical responses that do not contribute to the linear relationship under modeling, this approach has the purpose of enhancing the curve fitting of the regression model.

A linear regression was chosen for this analysis due to its simplicity in implementation and interpretation and because of the nature of the variables. The straightforward examination of the relationships between independent and dependent variables, along with the reasonable approximation of the intervals between Likert scale points as equal, made linear regression an appropriate method.

As a first step, each independent variable was individually regressed against each dependent variable to eliminate variables that would not be significant enough to justify the consumers' willingness to adopt AVs at each different level. The significant predictors (p-value <0.05) were then filtered and counted to identify the most influential independent variables. It is important to stress that variables with a p-value precisely equal to 0 were not counted, as it is virtually impossible to achieve this in practical scenarios.

UsedVA (Q1)	**FamiliarConcept (Q2)**	**FamiliarTech (Q3)**
3	11	10
Q4_1	**Q4_2**	**Q4_3**
12	8	8
Q6_1	**Q6_2**	**Q6_3**
7	5	5
Q8_1	**Q8_2**	**Q8_3**
5	9	7
Q10_1	**Q10_2**	**ImportanceSafety (Q12_1)**
10	9	4
ImportanceConvenience (Q12_3)	**ProvenSecurityDailyCommuting (Q13)**	**Age (Q16)**
5	8	2
Gender (Q17)		
5		

Table 5: Frequency of Significant Independent Variables

As can be observed, the majority of the background and demographic variables did not have a low p-value, and this can be attributed to a few reasons. Firstly, the distribution of responses for variables like education and country exhibited a high skew towards one or two categories. This skewness made regression analysis impractical because it did not exhibit the distribution of variability necessary for robust statistical modeling.

Additionally, variables like income and political affiliation were frequently marked with non-responses such as "Other" or "Prefer not to say," which significantly reduced the sample size

for these categories and further compromised a regression analysis. These issues collectively led to the exclusion of many background and demographic control variables from the final models, which cannot be compared with what the literature has previously said (DGITM/SAGS/EP, 2019).

Then, to assess potential multicollinearity issues when producing the final model, the Variance Inflation Factor (VIF) was calculated for various levels both before and after exposure. The VIF is a crucial metric for detecting multicollinearity in regression models. The majority of VIF values ranged from 1.2 to 2.8, with no variable reaching a value higher than 3.1, which indicates an acceptable level of multicollinearity for most variables.

This range suggests that while some collinearity exists, it is not severe enough to compromise the model's validity. Generally, VIF values above 5 are considered problematic, whereas values between 1 and 5, especially around 3, indicate a moderate correlation that should be monitored but is still acceptable.

Also, to avoid multicollinearity issues, a correlation matrix with the remaining numerical independent variables (i.e., all of the remaining independent variables except for UsedVA and Gender, which are categorical) was built. The results of this matrix were fascinating, revealing several high correlations that align logically with the survey questions.

For instance, a high correlation between FamiliarConcept and FamiliarTech (0.76) was not unexpected as both pertain to respondents' familiarity with the concept and technology of autonomous vehicles, respectively. This could show that those familiar with the idea of autonomous vehicles were likely to be familiar with the technology behind them as well, so intuitively, these factors are not orthogonal.

Similarly, the correlation between Q10_1 and Q10_2 (0.49) made sense as both questions related to the perceived benefits and preferences for self-driving cars. Respondents who believed in the benefits of self-driving vehicles (Q10_1) were also likely to express a preference for self-driving cars if cybersecurity concerns were addressed (Q10_2).

The correlations involving the variables related to perceptions on AVs, such as Q4_1, Q4_2, and Q4_3, also reflected logical connections. For example, Q4_1 (believing in the reduction of human error) showed a correlation with Q4_2 (feeling comfortable in an AV), which is not surprising since if a respondent believes that AVs can reduce human errors, improving safety,

then that person naturally does not feel uncomfortable riding this type of vehicle.

These high correlations were not surprising, given the related nature of the survey questions. They highlighted how perceptions and familiarity with various aspects of autonomous vehicles tended to cluster together, reflecting coherent patterns in respondents' attitudes and beliefs about this emerging technology.

Based on the correlation analysis and the logical connections between the survey questions, the following variables were initially chosen for the final model: FamiliarConcept, Q4_1, Q6_1, Q8_2, Q8_3, Q10_1, ProvenSecurityDailyCommuting, Age and Gender. These variables were selected due to their significant individual relationships with the dependent variables and their relevance to the key factors influencing the adoption of autonomous vehicles (AVs).

The variables also balanced the need for a comprehensive model that captured various dimensions of familiarity, perceived benefits, security concerns, and demographic factors while also addressing multicollinearity issues. This selection ensured that the final model was robust, interpretable, and capable of providing meaningful insights into the factors influencing the willingness to adopt different levels of AV autonomy.

Expert interviews further supported the significance of certain independent variables, such as familiarity with AV technology and trust in cybersecurity measures, which align with the survey findings.

The following images (Figures 28, 29, and 30) show the first attempt at the final model.

	Dependent variable:			
	Level0_before	Level0_after	Level1_before	Level1_after
	(1)	(2)	(3)	(4)
Constant	4.037*** (0.672)	3.582*** (0.738)	3.650*** (0.899)	3.029*** (0.873)
FamiliarConcept	0.214*** (0.081)	0.179** (0.090)	0.208* (0.109)	0.178* (0.106)
Q4_1	-0.108 (0.104)	-0.023 (0.112)	-0.023 (0.139)	0.003 (0.133)
Q10_1	0.075 (0.087)	0.029 (0.095)	0.165 (0.117)	0.163 (0.112)
ProvenSecurityDailyCommuting	-0.141* (0.077)	-0.068 (0.084)	-0.120 (0.103)	-0.004 (0.099)
Age	0.028 (0.082)	0.064 (0.089)	0.035 (0.110)	-0.080 (0.105)
GenderMale	0.082 (0.154)	0.126 (0.168)	-0.233 (0.206)	-0.126 (0.199)
Q8_2	0.109 (0.086)	0.207** (0.093)	0.168 (0.116)	0.343*** (0.111)
Q8_3	0.129* (0.071)	0.093 (0.078)	0.092 (0.095)	0.085 (0.093)
Q6_1	-0.043 (0.061)	-0.145** (0.067)	-0.197** (0.082)	-0.297*** (0.079)
Observations	121	120	120	119
R2	0.155	0.160	0.136	0.241
Adjusted R2	0.086	0.091	0.065	0.178
Note:				*p<0.1; **p<0.05; ***p<0.01

Figure 28: Regression Results for the First Attempt of Model for Level 0 and 1

	Dependent variable:			
	Level2_before	Level2_after	Level3_before	Level3_after
	(1)	(2)	(3)	(4)
Constant	2.244*** (0.811)	1.403 (0.857)	1.509* (0.892)	1.320 (0.926)
FamiliarConcept	0.248** (0.098)	0.288*** (0.104)	0.196* (0.108)	0.172 (0.113)
Q4_1	-0.011 (0.125)	0.042 (0.131)	0.139 (0.138)	0.189 (0.141)
Q10_1	0.247** (0.105)	0.183 (0.111)	0.219* (0.116)	0.074 (0.119)
ProvenSecurityDailyCommuting	0.105 (0.093)	0.196** (0.098)	0.295*** (0.102)	0.310*** (0.105)
Age	-0.180* (0.099)	-0.130 (0.103)	-0.118 (0.109)	-0.080 (0.112)
GenderMale	-0.331* (0.185)	-0.246 (0.196)	-0.266 (0.204)	-0.092 (0.211)
Q8_2	0.192* (0.104)	0.254** (0.109)	0.136 (0.114)	0.231* (0.117)
Q8_3	0.166* (0.086)	0.147 (0.091)	-0.075 (0.095)	-0.188* (0.098)
Q6_1	-0.169** (0.074)	-0.205** (0.078)	-0.172** (0.082)	-0.129 (0.084)
Observations	121	119	121	120
R2	0.234	0.269	0.321	0.339
Adjusted R2	0.171	0.209	0.265	0.284
Note:				*p<0.1; **p<0.05; ***p<0.01

Figure 29: Regression Results for the First Attempt of Model for Levels 2 and 3

	Dependent variable:			
	Level4_before	Level4_after	Level5_before	Level5_after
	(1)	(2)	(3)	(4)
Constant	0.512 (0.871)	1.164 (0.910)	-1.306 (0.928)	-0.770 (0.980)
FamiliarConcept	0.117 (0.105)	0.103 (0.111)	0.115 (0.112)	0.146 (0.119)
Q4_1	0.161 (0.134)	0.218 (0.139)	0.204 (0.143)	0.216 (0.149)
Q10_1	0.217* (0.113)	0.105 (0.117)	0.343*** (0.121)	0.299** (0.126)
ProvenSecurityDailyCommuting	0.527*** (0.100)	0.397*** (0.103)	0.455*** (0.106)	0.195* (0.111)
Age	-0.005 (0.106)	0.029 (0.110)	0.117 (0.113)	0.177 (0.118)
GenderMale	-0.116 (0.199)	-0.175 (0.207)	0.104 (0.212)	0.008 (0.223)
Q8_2	0.084 (0.112)	0.109 (0.115)	-0.189 (0.119)	-0.138 (0.124)
Q8_3	-0.218** (0.093)	-0.377*** (0.097)	-0.110 (0.099)	-0.187* (0.104)
Q6_1	-0.112 (0.080)	-0.078 (0.082)	0.177** (0.085)	0.229** (0.088)
Observations	121	120	121	120
R2	0.477	0.441	0.480	0.379
Adjusted R2	0.434	0.395	0.438	0.328
Note:				*p<0.1; **p<0.05; ***p<0.01

Figure 30: Regression Results for the First Attempt of Model for Levels 4 and 5

In the process of refining our model, it was crucial to understand why certain variables that appeared significant in individual regressions might lose significance when included in a more comprehensive model.

The variables ‘Q4_1’, ‘Age’, and ‘Gender’ showed significance in individual regressions due to their capturing some aspects of the variance in the dependent variable. However, it seemed that, compared to other more directly relevant and significant predictors, their individual contributions became less significant when part of a more complex model. This implies that we cannot analyze and compare demographic variables with the findings of the literature (DG-ITM/SAGS/EP, 2019).

The chosen variables for the final model (‘FamiliarConcept’, ‘Q6_1’, ‘Q8_2’, ‘Q8_3’, ‘Q10_1’ and ‘ProvenSecurityDailyCommuting’) were retained because they provide a more robust and focused explanation of the willingness to adopt AVs. This approach ensured a more concise and interpretable model.

The following images (Figures 31, 32 and 33) show the final model.

	Dependent variable:			
	Level0_before	Level0_after	Level1_before	Level1_after
	(1)	(2)	(3)	(4)
Constant	3.979*** (0.618)	3.715*** (0.678)	3.713*** (0.828)	2.829*** (0.801)
FamiliarConcept	0.193*** (0.071)	0.179** (0.078)	0.153 (0.096)	0.178* (0.092)
Q6_1	-0.047 (0.060)	-0.153** (0.065)	-0.198** (0.081)	-0.288*** (0.077)
Q8_2	0.112 (0.085)	0.203** (0.092)	0.182 (0.114)	0.348*** (0.109)
Q8_3	0.128* (0.071)	0.093 (0.078)	0.098 (0.095)	0.084 (0.092)
Q10_1	0.044 (0.076)	0.039 (0.082)	0.130 (0.102)	0.145 (0.097)
ProvenSecurityDailyCommuting	-0.163** (0.072)	-0.070 (0.078)	-0.111 (0.097)	-0.009 (0.092)
Observations	121	120	120	119
R2	0.144	0.152	0.124	0.234
Adjusted R2	0.099	0.107	0.077	0.193
Note:				*p<0.1; **p<0.05; ***p<0.01

Figure 31: Regression Results for the Final Model for Levels 0 and 1

	Dependent variable:			
	Level2_before	Level2_after	Level3_before	Level3_after
	(1)	(2)	(3)	(4)
Constant	1.766** (0.762)	1.137 (0.795)	1.370 (0.828)	1.328 (0.856)
FamiliarConcept	0.236*** (0.088)	0.289*** (0.091)	0.216** (0.095)	0.225** (0.098)
Q6_1	-0.146* (0.074)	-0.186** (0.077)	-0.156* (0.081)	-0.118 (0.082)
Q8_2	0.206* (0.105)	0.262** (0.108)	0.138 (0.114)	0.223* (0.116)
Q8_3	0.166* (0.087)	0.146 (0.091)	-0.073 (0.095)	-0.188* (0.098)
Q10_1	0.194** (0.094)	0.163* (0.097)	0.236** (0.102)	0.133 (0.104)
ProvenSecurityDailyCommuting	0.093 (0.089)	0.196** (0.093)	0.319*** (0.097)	0.342*** (0.099)
Observations	121	119	121	120
R2	0.190	0.249	0.299	0.324
Adjusted R2	0.148	0.209	0.263	0.288
Note:				*p<0.1; **p<0.05; ***p<0.01

Figure 32: Regression Results for the Final Model for Levels 2 and 3

	Dependent variable:			
	Level4_before	Level4_after	Level5_before	Level5_after
	(1)	(2)	(3)	(4)
Constant	0.694 (0.802)	1.509* (0.843)	-0.757 (0.862)	-0.052 (0.913)
FamiliarConcept	0.138 (0.092)	0.119 (0.097)	0.153 (0.099)	0.155 (0.105)
Q6_1	-0.110 (0.078)	-0.079 (0.081)	0.163* (0.084)	0.210** (0.088)
Q8_2	0.079 (0.110)	0.104 (0.115)	-0.204* (0.119)	-0.149 (0.124)
Q8_3	-0.216** (0.092)	-0.372*** (0.097)	-0.108 (0.099)	-0.180* (0.104)
Q10_1	0.266*** (0.099)	0.171* (0.103)	0.442*** (0.106)	0.394*** (0.111)
ProvenSecurityDailyCommuting	0.564*** (0.094)	0.452*** (0.097)	0.508*** (0.101)	0.261** (0.105)
Observations	121	120	121	120
R2	0.469	0.426	0.464	0.355
Adjusted R2	0.441	0.396	0.436	0.321
Note:				*p<0.1; **p<0.05; ***p<0.01

Figure 33: Regression Results for the Final Model for Levels 4 and 5

A notable observation from the regression results was that both R^2 and adjusted R^2 values generally increased with the level of autonomy. This indicated that as the level of autonomy increased, the model explained more of the variance in the dependent variable. This makes sense because independent variables related to familiarity with the notions of autonomous vehicles and cybersecurity can explain more variations at higher autonomy levels. As the level of autonomy increased, the significance of these factors grew, making them more influential in the decision-making process.

However, it is important to note that the R^2 and adjusted R^2 values, especially for levels 0, 1, and 2, were not exceptionally high, which suggested a relatively modest proportion of variance in the dependent variable explained by the independent variables at these levels. Therefore, evaluations and analyses involving these independent variables should be made with caution, considering their limited explanatory power. This caveat is important when considering the significance of independent variables within the model, especially when making predictions or generalizations.

Analyzing the independent variables individually, the variable FamiliarConcept ("On a scale of 1 (not at all familiar) to 5 (very familiar), how familiar are you with the concept of self-driving cars?") significantly influenced willingness to adopt for lower levels of autonomy (Levels 0 to 2). Thus, the higher the level of familiarity with the concept, the willingness to adopt on average rose, *ceteris paribus*.

This might indicate how familiarity with the concept of autonomous vehicles is crucial for initial acceptance. Its higher significance in lower levels compared to higher levels could further suggest that individuals who are less informed about AVs might have heightened concerns about cybersecurity, leading to a decreased willingness to adopt vehicles with little to no autonomy. This is also partially explained by the literature, as more informed individuals are more likely to adopt AVs (DGITM/SAGS/EP, 2019). Another plausible explanation is that other variables may become more significant for explaining the variance at higher levels of autonomy, reducing the relative importance of FamiliarConcept.

Furthermore, the variable ProvenSecurityDailyCommuting ("If autonomous vehicles had a proven strong record of cybersecurity, how likely would you use one for daily commuting?") consistently showed significance across different levels of autonomy, notably at higher levels (Levels 3 to 5), with a positive impact on willingness to adopt. This illustrates that the perceived security and safety record of autonomous vehicles is a critical factor influencing the adoption at higher levels of autonomy. Given the increasing complexity and potential risks associated with higher levels of autonomy, it was logical that security concerns played a more significant role, consistent with what the literature presents (Sirisup & Petchmark, 2022).

The experts also consistently mentioned the critical way cybersecurity influences consumer trust and adoption of AVs. For example, cybersecurity experts underscored the importance of a proven security track record, which aligns with the significant impact of the variable ProvenSecurityDailyCommuting in our regression analysis.

Despite expected behavior for the majority of variables, it should be noted that for level 0 vehicles before cyber threat exposure, the effect was negative. This means that if an average respondent had an increased likelihood of adopting an AV for daily commuting, their willingness to adopt a vehicle decreased, which seems not plausible. However, the R^2 and adjusted R^2 for this regression were not particularly high, so the reliability of this negative correlation could be limited.

The variable Q6_1 ("How concerned are you about cybersecurity risks in autonomous vehicles?") was also significant at multiple levels, particularly after the cybersecurity information exposure for levels 0 to 2, with a non-surprising negative effect. One example was the regression for level 2 after cyber threat exposure, where, on average if the level of concern increased by one unit, the willingness to adopt decreased by 0.186, *ceteris paribus*.

Once again, this was expected as cybersecurity concerns directly impact trust and willingness to adopt, especially at higher levels where technology reliance is greater. The increased significance after exposure suggested that awareness and information about cybersecurity risks heightened concern, influencing adoption decisions.

It is essential to go back to qualitative data from expert interviews, where experts noted that increasing public awareness of cybersecurity risks could significantly impact consumer decisions, which is reflected in the significant negative effect of cybersecurity concerns (Q6_1) on willingness to adopt AVs at multiple levels.

However, what was not expected was the significant positive effect of this variable at level 5 AV. Here, both before and after cyber threat exposure, there was an unexpected increase in willingness to adopt level 5 AVs, coupled with an increase in respondents' level of concern.

Additionally, the variables Q8_2 ("I trust the current cybersecurity measures in autonomous vehicles") and Q8_3 ("The possibility of cybersecurity breaches deters me from adopting autonomous vehicles") showed varied significance before and after cybersecurity information exposure. Specifically, Q8_2 became more significant after exposure for most levels of autonomy, and the value increased. This highlighted the role of trust in cybersecurity measures in post-exposure scenarios and its positive impact on willingness to adopt for levels between 0 and 3.

Thus, educating users about cybersecurity can influence trust and, consequently, adoption decisions, a conclusion that accords with the literature (DGITM/SAGS/EP, 2019) and with expert interviews, which stressed the necessity of educating consumers about existing cybersecurity measures to build trust and facilitate adoption.

Nonetheless, similarly to the variable Q6_1, there was an exception at level 5, where the significance was higher before exposure. Here, the effect was significant but negative for level 5 AVs before exposure. This would mean, counter-intuitively, that more trust in cybersecurity measures would decrease willingness to adopt. Still, the significance was not so relevant (p-value lower than 0.1 but higher than 0.05), so this exception was not a significant concern.

Conversely, Q10_1 ("The benefits of self-driving cars outweigh their cybersecurity risks") seemed generally to decrease in significance and value after exposure to cybersecurity concerns across levels 2 to 5. However, it remained with a positive effect on willingness to adopt

different AVs (with the exception of level 5). For example, with level 4, before exposure to cybersecurity concerns, on average, if the perception of AV benefits outweighing cyber risks increased one unit, this increased willingness to adopt by 0.266, *ceteris paribus*. Then, after exposure, the value decreased to 0.171, and the significance decreased as well, from less than 0.01 to less than 0.1.

This observation is not surprising, given how cybersecurity threats may have caused a part of the sample population to doubt the potential positive impact of AVs, shifting their focus to the downside. This effect was similar to the reaction to high-profile incidents, where exposure to negative news significantly impacted acceptance by drawing greater attention to the associated risks and downsides (Eliot, 2021).

In a more general analysis, the significance of several variables changed after respondents were exposed to cybersecurity information. For example, Q8_2 showed increased significance post-exposure. This indicated that cybersecurity information could alter perceptions and priorities, making security measures and trust in these measures more crucial in the decision-making process.

Finally, ProvenSecurityDailyCommuting stood out as a consistently significant variable across different levels of autonomy, both before and after cybersecurity exposure. This underscores the overarching importance of a proven security track record for the adoption of autonomous vehicles.

Once again, the findings align with the Technology Acceptance Model as proposed by Davis (1993), which emphasizes perceived usefulness and perceived ease of use as critical factors influencing the adoption of new technologies. In this context, variables such as ProvenSecurityDailyCommuting can be seen as proxies for perceived usefulness, reflecting the respondents' belief that autonomous vehicles will improve their daily commutes and overall efficiency. This connection is particularly evident in the increased willingness to adopt higher levels of autonomy when familiarity and perceived security are high.

Moreover, the diffusion of innovation theory by Rogers (1962) illustrates the importance of understanding how new technologies spread among different adopter categories. The varying significance of factors like cybersecurity concerns and trust in security measures before and after exposure indicates a shift in adopter categories, from early adopters to more cautious ones, underscoring the necessity of targeted communication strategies to facilitate broader acceptance.

The concept of dynamic capabilities is integral to understanding how organizations can effectively navigate the challenges and opportunities presented by AV technologies. Firms' ability to sense, seize, and transform opportunities related to AV adoption is reflected in the varied significance of regression variables before and after cybersecurity exposure (Teece et al., 1997). The ability to rapidly adapt to changing consumer perceptions and concerns about cybersecurity (Q6_1, Q8_2, Q10_1) demonstrates the need for dynamic capabilities.

Companies that can efficiently gather and process information about consumer attitudes towards AVs, make timely decisions, and reconfigure their resources to address cybersecurity concerns will likely be more successful in promoting AV adoption (Helfat & Peteraf, 2003). This strategic adaptability is crucial for firms operating in the high-velocity environment of AV technology, where maintaining a competitive edge requires continuous innovation and responsiveness to external shocks, such as cybersecurity threats (Eisenhardt & Martin, 2000).

5 Conclusions

5.1 Main Findings - Triangulation

Based on the triangulation of literature, expert interviews, and survey data, it is evident that while cybersecurity concerns are significant, they are unlikely to impede the adoption of autonomous vehicles (AVs). Instead, the results underline the crucial need to implement robust cybersecurity measures. These measures, along with transparent communication and regulatory frameworks, are key to building public trust and supporting the adoption of AVs, thereby reassuring the audience about the safety of AVs.

A consistent theme across the literature, survey responses, and expert interviews is the impact of cybersecurity concerns on consumer acceptance of AVs. The literature emphasizes that perceived safety and security are crucial factors in adopting new technologies, especially AVs, where the threat of cyber-attacks can significantly deter potential users (Davis, 1993; Rogers, 1962). This concern was reflected in the survey findings, with the majority of respondents expressing significant concerns about cybersecurity risks, such as remote hijacking and malicious software attacks.

Experts further illuminated these concerns, noting the unique risks posed by AVs due to their complexity and the integration of components from various manufacturers. Unlike other sectors, the life-and-death stakes involved in AV technology, where a cyber-attack could potentially lead to accidents and loss of life, make its cybersecurity issues particularly pressing.

The survey provided insights into specific consumer behaviors and concerns, which enhanced our understanding of AV adoption. For instance, literature indicates that concerns are higher for fully autonomous vehicles (Level 5) compared to partially autonomous ones, suggesting that as the level of autonomy and perceived risk increases, so do cybersecurity concerns (Prasetio & Nurliyana, 2023). This trend was confirmed through regression analyses and t-tests.

The t-test results revealed that when respondents considered cyber threats, their willingness to adopt AV technology generally decreased, with a more pronounced decline at higher levels of autonomy. However, the regressions also identified other significant factors influencing AV adoption beyond cybersecurity, such as trust in the technology, knowledge of how the technology works, and overall safety of the vehicle.

Safety and cybersecurity concerns related to safety were prominent in both regression models

and survey analysis, particularly in questions 6, 12, and 14. These questions showed that system attacks and failures had a more significant impact on AV adoption than data breaches or risks to personal information. This finding aligns with expert insights, pointing to the essential requirement for consumers to feel safe and secure inside an AV for smoother adoption.

Experts had differing views on whether public awareness of cybersecurity risks is increasing, yet survey results supported the notion that this factor could influence AV adoption. High-profile incidents tend to heighten fears and skepticism, making transparent communication and robust security measures vital for building public trust. This stresses the importance of raising public awareness, aiming to empower the audience about their role in adopting AV technology.

Despite cybersecurity concerns, both expert interviews and survey findings suggested that AV adoption is likely to continue. Survey data indicated that while respondents were concerned about cybersecurity threats, 70.3% were willing to use AVs for daily commuting if these concerns were adequately addressed. This demonstrates a potential path to overcoming these barriers and should instill optimism about the future of AVs.

Experts echoed this sentiment, asserting that although cybersecurity is a critical issue, it can be managed through comprehensive regulatory frameworks, continuous monitoring, and public awareness efforts, as also highlighted in the literature (George et al., 2023; Sirisup & Petchmark, 2022; Tomorrow Bio, 2023). They argue that these steps can bolster consumer confidence and facilitate the integration of AVs into mainstream use, which reflects Christensen's account of how a disruptive innovation moves from initial niche adoption into being more widely used (Christensen, 1997).

Additionally, experts provided practical insights into the challenges of implementing cybersecurity, such as technical complexities and the necessity for industry-wide standards. Regulatory standards addressing cybersecurity concerns are evolving, with standards like ISO/SAE 21434 for road vehicle cybersecurity playing a crucial role in ensuring compliance and protection against cyber threats. Both literature and experts also emphasized the significance of industry collaboration and adherence to these standards as a strategy to mitigate the negative impact of cybersecurity risks on AV adoption.

The complexity and interdependencies of AV systems create potential vulnerabilities that must be addressed from the outset. This requires continuous security assessments and a proactive approach to cybersecurity. Moreover, many experts pointed out that the automotive industry

is actively improving cybersecurity, which reassures consumers and mitigates potential barriers to adoption. These practical considerations are essential for developing effective strategies to enhance AV security and support adoption, a view shared by literature and partially corroborated by survey results (Stagnaro, 2023).

In summary, while cybersecurity concerns have the potential to affect the adoption of AVs, they are manageable with adequate strategies. With robust cybersecurity measures, transparent communication, and regulatory frameworks, these concerns will not pose a significant barrier to adopting autonomous vehicles.

5.1.1 Theoretical Implications

The conclusions of this study on cybersecurity concerns affecting the adoption of autonomous vehicles (AVs) have profound implications for several critical management theories discussed in the literature review, underscoring the significance of this research.

Firstly, findings support and expand upon the Technology Acceptance Model (TAM), as this study highlights that perceived cybersecurity risks directly impact both PU and PEOU, thereby influencing willingness to adopt AVs (Davis, 1993). For instance, survey results consistently showed a decline in willingness to adopt AVs after respondents were informed about cybersecurity threats, underscoring the importance of addressing these concerns to improve AV technologies' perceived usefulness and ease of use (Davis et al., 1989; Venkatesh & Davis, 2000).

This research also aligns with Rogers's *Diffusion of Innovation Theory*, particularly in the concept of early adopters. These early adopters, despite significant cybersecurity concerns, represent a notable 6.7% of respondents showing the highest level of willingness to adopt Level 5 AVs. Their foundational interest and trust in technology suggest that, if managed correctly, the adoption of AVs can follow a typical diffusion path (Rogers, 1962). The presence of these early adopters, even in the face of substantial risks, signals that the adoption of AVs is likely to continue and expand, provided that the industry can effectively address and mitigate cybersecurity concerns.

Furthermore, automation, particularly the rise of AVs, can be considered an exogenous shock in the industry, representing a significant technological disruption. This aligns with the framework of exogenous shocks and the concept of fit, where firms must adapt to sudden changes in the external environment to survive and thrive (Aldrich, 1979; Levinthal, 1991; Teece, 2007).

The rapid advancement of AV technology introduces new challenges and opportunities, necessitating that firms respond effectively. Dynamic Capabilities informs how firms can effectively navigate the challenges and opportunities presented by AV technologies (Barreto, 2010; Teece et al., 1997). In this context, robust cybersecurity measures play a pivotal role for promoting AV adoption and helping a firm attain superior performance over peers.

Companies that can efficiently gather and process information about consumer attitudes towards AVs, make timely decisions, and reconfigure their resources to address cybersecurity concerns will likely be more successful. This strategic adaptability, with robust cybersecurity measures at its core, is critical in the high-velocity environment of AV technology, where maintaining a competitive edge requires continuous innovation and responsiveness to external shocks, such as evolving cybersecurity threats that occur in real time (Eisenhardt & Martin, 2000; Helfat & Peteraf, 2003; Simon, 1997).

5.1.2 Practical Implications

A coalition between policymakers, manufacturers, and cybersecurity professionals is needed for successful adoption of autonomous vehicles (AVs) to occur.

Firstly, it is important to invest in advanced security technologies and establish industry-wide standards. These robust cybersecurity protocols are essential for protecting AVs from potential threats. Manufacturers must prioritize integrating these security measures right from the design phase to prevent vulnerabilities and ensure users' safety.

Moreover, transparent communication plays a pivotal role in building public trust. It is not enough to have strong cybersecurity measures in place; consumers need to be informed about them. Clear and transparent information about implemented security protocols and measures can significantly alleviate consumer concerns. Regular updates, public demonstrations of cybersecurity measures, and open channels for addressing consumer questions and fears are necessary. This transparency can bridge the gap between technological advancements and consumer confidence, ultimately fostering a more positive public perception of AVs. This open communication also ensures that policymakers, manufacturers, and cybersecurity professionals are fully informed and involved in the process.

In addition to technological and communication strategies, comprehensive regulatory oversight is essential. Policymakers must establish stringent regulatory frameworks that mandate high

cybersecurity standards, as well as continuous monitoring. These regulations should be adaptable to the evolving nature of cyber threats, as well as include provisions for regular updates and audits of AV systems. By ensuring these frameworks are in place, regulatory bodies can help create a safer environment for AV adoption, boost consumer confidence, and support the industry's growth.

5.2 Limitations

This dissertation is subject to limitations that may impact applicability of its findings. One constraint was the relatively brief four-month timeframe of this study, which suggests need for a longer duration.

5.2.1 Expert Interviews

Semi-structured interviews were limited in scope and depended on the researcher's judgment. The interview guide, developed through an inductive process and based on an overview of relevant literature, may have introduced biases. Constraints regarding time and resources when selecting experts, as well as favoring those who were readily available to participate, may have limited collection of more diverse perspectives. Nonetheless, the overall quality of experts was high.

Acknowledging biases present in expert opinions is vital, particularly when these opinions may not accurately represent the broader population due to limitations imposed by small sample sizes (Houghton et al., 2013). Studies have shown that smaller sample sizes can lead to significant biases, which may render findings less reliable and representative (Lin, 2018). Additionally, choice and method of sample selection can also introduce biases, such as selection bias and sampling error, that can further distort the outcomes of a study (Bhandari, 2020).

5.2.2 Survey

Data obtained from a self-reported online survey inevitably contain inaccuracies (Bryman, 2016). Despite conducting the survey on an international scale, Portugal accounted for approximately 81.6% of participants, with significant representation from countries sharing similar cultural backgrounds, such as Spain, Italy, and France. This geographical concentration may skew findings and limit their generalizability to a broader international context.

Furthermore, the population sampled exhibited homogeneity across various other demographic factors, particularly age and education levels. The majority of respondents were young adults (84.5% aged 18-24) and highly educated, with 46.4% holding a bachelor's degree. This homogeneity potentially limits our ability to properly evaluate how these demographics influence consumer acceptance of autonomous vehicles. This issue is common in research involving human subjects, particularly those from WEIRD populations (Western, educated, industrialized, rich, and democratic), who are considered to be among the most psychologically distinct people globally (Henrich et al., 2010).

Additionally, the inherent issue of acquiescence bias affects Likert scales used to measure qualitative data, as individuals tend to exhibit positive inclinations in survey responses (Krosnick, 1999). This could lead to overestimating positive attitudes toward autonomous vehicles and related technologies. Researchers use quantitative techniques like t-tests, correlation matrices, and linear regressions, but they rely on qualitative insights, which could lead to a biased outcome due to a lack of objectivity and subjective interpretation.

Furthermore, a significant percentage of respondents who preferred not to disclose certain information, such as income (30.5%) and political affiliation (30.1%), adds another layer of limitation. This nondisclosure hinders a comprehensive analysis of how these variables might influence the adoption of autonomous vehicles.

5.3 Future research

Given this study's emphasis on potential ownership of autonomous vehicles, future research could examine whether cybersecurity concerns differ across various forms of mobility, including car-sharing and ride-hailing services like Uber, Bolt, and Lyft.

This research predominantly addressed light vehicles, given their advanced development relative to heavy vehicles. Future studies could explore categories of autonomous vehicles, distinguishing between passenger and cargo transport, to assess whether cybersecurity concerns vary by vehicle type.

Furthermore, this study opens the door to investigating the influence of geopolitical factors on the AV industry. Future research could explore how geopolitical disputes impact AV development and shape public perceptions, particularly regarding cybersecurity.

Future researchers are encouraged to engage with larger, more demographically diverse con-

sumer populations to better understand the determinants of AV acceptance. Longitudinal studies tracking shifts in consumer attitudes, alongside technological, regulatory, and industry developments, could provide deeper insights into cybersecurity concerns and their effect on AV adoption.

Lastly, it is crucial to include a broader range of stakeholders in future studies. Involving government officials, policymakers, NGOs, consumer behavior researchers, and geopolitical analysts will help gather a comprehensive understanding of complex cybersecurity challenges in AV adoption.

Bibliography

Aldrich, H. E. (1979). *Organizations and environments*. Prentice-Hall.

Ameka, I., & Dhewanto, W. (2013). Technology push vs. market pull in technology university innovation commercialization: Case study of itb. *Information Management and Business Review*, *5*(7), 337–341. https://doi.org/10.22610/imbr.v5i7.1060

Ammar, M., Janjua, H., Thangarajan, A. S., Crispo, B., & Hughes, D. (2019). Securing the on-board diagnostics port (obd-ii) in vehicles. *SAE International Journal of Transportation Cybersecurity and Privacy*, *2*(2), 83–106. https://doi.org/10.4271/11-02-02-0009

Ayala, R., & Mohd, T. K. (2021). Sensors in Autonomous Vehicles: A Survey. *Journal of Autonomous Vehicles and Systems*, *1*(3), 031003. https://doi.org/10.1115/1.4052991

Bansal, P., Smith, W. K., & Vaara, E. (2018). New ways of seeing through qualitative research. *Academy of Management Journal*, *61*(4), 1189–1195.

Baregheh, A., Rowley, J., & Sambrook, S. (2009). Towards a multidisciplinary definition of innovation. *Management Decision*, *47*(8), 1323–1339. https://doi.org/10.1108/00251740910984578

Bari, B. S., Yelamarthi, K., & Ghafoor, S. (2023). Intrusion detection in vehicle controller area network (can) bus using machine learning: A comparative performance study. *Sensors*, *23*(7). https://doi.org/10.3390/s23073610

Barreto, I. (2010). Dynamic capabilities: A review of past research and an agenda for the future. *Journal of Management*, *36*(1), 256–280.

Barriball, K. L., & While, A. (1994). Collecting data using a semi-structured interview: A discussion paper. *Journal of Advanced Nursing-Institutional Subscription*, *19*(2), 328–335. https://doi.org/10.1111/j.1365-2648.1994.tb01088.x

Bartlett, J. E., Kotrlik, J. W., & Higgins, C. C. (2001). Organizational research: Determining appropriate sample size in survey research. *Information technology, learning, and performance journal*, *19*(1), 43–50.

Bhandari, P. (2020). Sampling bias and how to avoid it: Types & examples. Scribbr. https://www.scribbr.com/methodology/sampling-bias/

Blumenthal, M., & Csernatoni, R. (2022). Computers on wheels: Automated vehicles and cybersecurity risks in europe. *Carnegie Europe - Carnegie Endowment for International Peace*. https://carnegieeurope.eu/2022/03/24/computers-on-wheels-automated-vehicles-and-cybersecurity-risks-in-europe-pub-86678

Blut, M., Wang, C., Wünderlich, N. V., & Brock, C. (2017). An integrative model of mobile app usage. *The International Review of Retail, Distribution and Consumer Research*, *27*(3), 245–265.

Boston Consulting Group. (2023). Profiting in the future of the automotive industry. https://www.bcg.com/publications/2023/profiting-in-the-future-of-automotive-industry

Boyer, J., & Kokosy, A. (2022). Technology-push and market-pull strategies: The influence of the innovation ecosystem on companies' involvement in the industry 4.0 paradigm. *Journal of Risk Finance*, *23*(5), 461–479. https://doi.org/10.1108/JRF-12-2021-0193

Bradley, T. (2022). Hackers target drivers as cyber attacks on cars rise 225 percent. *Express.co.uk*. https://www.express.co.uk/life-style/cars/1632500/hackers-target-drivers-cyber-attacks-cars

Bryman, A. (2016). *Social research methods* (5th ed.). Oxford University Press.

Burkacky, O., Deichmann, J., Klein, B., Pototzky, K., & Scherf, G. (2020). Cybersecurity in automotive: Mastering the challenge. http://dln.jaipuria.ac.in:8080/jspui/bitstream/123456789/3227/1/McKinsey%20Report%20-%20Cybersecurity-in-automotive-Mastering-the-challenge.pdf

Chin, K. (2023). Developing a culture of cybersecurity within your organization. https://www.upguard.com/blog/developing-a-culture-of-cybersecurity

Christensen, C. M. (1997, January). The innovator's dilemma. http://2ndbn5thmar.com/change/The%20Innovators.pdf

Christensen, C. M., Kaufman, S. P., & Shih, W. C. (2013). *Innovation killers: How financial tools destroy your capacity to do new things* (1st). Harvard Business Press.

Christensen, C. M., McDonald, R., Altman, E. J., & Palmer, J. E. (2018, August). Disruptive innovation: An intellectual history and directions for future research. https://doi.org/10.1111/joms.12349

Christensen, C. M., Raynor, M. E., & McDonald, R. (2015). What is disruptive innovation? *Harvard Business Review*, *93*(12), 44–53.

Cisco. (2024). 2024 cisco cybersecurity readiness index. https://newsroom.cisco.com/c/dam/r/newsroom/en/us/interactive/cybersecurity-readiness-index/documents/Cisco_Cybersecurity_Readiness_Index_FINAL.pdf

Cohen, D., & Crabtree, B. (2006). Qualitative research guidelines project.

Cybrary. (2022). Cybersecurity in connected autonomous vehicles. *Cybrary Blog*. https://www.cybrary.it/blog/cybersecurity-in-connected-autonomous-vehicles

Czerwiński, F. (2021, November). Current trends in automotive lightweighting strategies and materials. https://doi.org/10.3390/ma14216631

Daly, M. (2024). Biden administration to investigate national security risks posed by chinese-made 'smart cars'. *ABC News*. https://abcnews.go.com/Business/wireStory/biden-administration-investigate-national-security-risks-posed-chinese-107667001

Davies, N. (2023). 2023's top automotive cyber threats: Stay ahead & secure. *AT&T Cybersecurity Blog*. https://cybersecurity.att.com/blogs/security-essentials/the-top-8-cybersecurity-threats-facing-the-automotive-industry-heading-into-2023

Davis, F. D. (1993). User acceptance of information technology: System characteristics, user perceptions and behavioral impacts. *International journal of man-machine studies*, *38*(3), 475–487. https://doi.org/10.1006/imms.1993.1022

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science*, *35*(8), 982–1003. https://doi.org/10.1287/mnsc.35.8.982

Day, G. S. (1994). The capabilities of market-driven organizations. *Journal of Marketing*, *58*(4), 37–52.

de Arroyabe, I. F., Watson, T., & Angelopoulou, O. (2022). Cybersecurity in the automotive industry: A systematic literature review (slr). *Journal of Computer Information Systems*, *63*, 716–734. https://doi.org/10.1080/08874417.2022.2103853

Dede, G., Hamon, R., Junklewitz, H., Naydenov, R., Malatras, A., & Sanchez, I. (2021). *Cybersecurity challenges in the uptake of artificial intelligence in autonomous driving* (tech. rep.) (EUR 30568 EN). European Union Agency for Cybersecurity (ENISA) and Joint Research Centre (JRC). https://doi.org/10.2760/551271

Deloitte. (2022). The future of autonomous driving in the uk. https://www2.deloitte.com/uk/en/insights/focus/future-of-mobility.html

Deloitte. (2023). Global trends 2023: Direct lithium extraction. https://www2.deloitte.com/content/dam/Deloitte/br/Documents/ofertas-integradas/Deloitte-2023-GT-direct-lithium-extraction.pdf

Deloitte. (2024, January). *2024 global automotive consumer study | key findings: Global focus countries*. Deloitte.

DGITM/SAGS/EP. (2019, December). *Automated driving acceptance synthesis for g7* (tech. rep.) (Technical report). https://www.ecologie.gouv.fr/sites/default/files/Automated%20driving%20acceptance%20synthesis%20for%20G7.pdf

Doz, Y. L., & Kosonen, M. (2010). Embedding strategic agility: A leadership agenda for accelerating business model renewal. *Long Range Planning*, *43*(2-3), 370–382.

Dumitru, I.-A. (2022). Zero trust security. *Proceedings of the International Conference on Cybersecurity and Cybercrime (IC3)*. https://api.semanticscholar.org/CorpusID:248578977

Eisenhardt, K. M., & Martin, J. A. (2000). Dynamic capabilities: What are they? *Strategic Management Journal*, *21*(10-11), 1105–1121.

Elgazzar, K., Khalil, H., Alghamdi, T., Badr, A., Abdelkader, G., Elewah, A., & Buyya, R. (2022). Revisiting the internet of things: New trends, opportunities and grand challenges. *Frontiers in the Internet of Things*, *1*. https://doi.org/10.3389/friot.2022.1073780

Eliot, L. B. (2021). Serious concerns that ai self-driving cars cybersecurity will be a hacker leak like an open sieve. *Forbes*. https://www.forbes.com/sites/lanceeliot/2021/08/25/serious-concerns-that-ai-self-driving-cars-cybersecurity-will-be-a-hacker-leak-like-an-open-sieve/

ENISA. (2021). Enisa threat landscape 2021. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

EY. (2022). *Mobility consumer index wave 3*. https://www.ey.com/en_gl/insights/automotive/mobility-consumer-index-wave-3

Fowler Jr, F. J. (2013). Survey research methods. *Sage publications*.

Fraga-Lamas, P., & Fernández-Caramés, T. (2019). A review on blockchain technologies for an advanced and cyber-resilient automotive industry. *IEEE Access*, *7*, 17578–17598. https://doi.org/10.1109/ACCESS.2019.2895302

Gartner. (2023). Gartner forecasts global security and risk management spending to grow 14% in 2024. https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024

Gatlan, S. (2024). Tesla hacked again, 24 more zero-days exploited at pwn2own automotive 2024. *BleepingComputer*. https://www.bleepingcomputer.com/news/security/tesla-hacked-24-zero-days-demoed-at-pwn2own-automotive-2024/amp/

George, A. S., Baskar, D. T., & Srikaanth, P. B. (2023). Securing the self-driving future: Cybersecurity challenges and solutions for autonomous vehicles [Department of Physics, Crown University, Int'l. Chartered Inc. (CUICI) Argentina Campus, South America.]. *Zenodo*. https://doi.org/10.5281/zenodo.10246882

Ghazi-Tehrani, A. K., & Pontell, H. N. (2021). Phishing evolves: Analyzing the enduring cybercrime. *Victims & Offenders*, *16*, 316–342. https://api.semanticscholar.org/CorpusID:231947079

Gibbs, G. R. (2007). *Analyzing qualitative data* (Vol. 6). Sage.

Goldman Sachs. (2022, October). *Autonomous vehicles | the road ahead: New profit pool emerging* (Equity Research Report) (Contributing Authors: George Galliers, Mark Delaney, CFA, Eric Sheridan, Allen Chang, Jerry Revich, CFA, Jordan Alliger, Lincoln Kong, CFA, Chandramouli Muthiah, Kota Yuzawa, Fei Fang, Daniela Costa, Ben Miller, Kee Ryung Kim, Hiroki Muramatsu). Goldman Sachs.

Goldman Sachs. (2023a). Electric vehicles are forecast to be half of global car sales by 2035. https://www.goldmansachs.com/intelligence/pages/electric-vehicles-are-forecast-to-be-half-of-global-car-sales-by-2035.html

Goldman Sachs. (2023b, April). *Global metals & mining | direct lithium extraction: A potential game changing technology* (Equity Research Report) (Contributing Authors: Hugo Nicolaci, Paul Young, Nicholas Snowdon, Aditi Rai, Trina Chen, Joy Zhang, Yan Lin, Elise Bailey, Roy Shi, Nick Zheng, CFA). Goldman Sachs.

Guest, G., Bunce, A., & Johnson, L. (2006). How many interviews are enough? an experiment with data saturation and variability. *Field Methods*, *18*(1), 59–82.

Hannan, M. T., & Freeman, J. (1977). The population ecology of organizations. *American Journal of Sociology*, *82*(5), 929–964.

Helfat, C. E., & Peteraf, M. A. (2003). The dynamic resource-based view: Capability lifecycles. *Strategic Management Journal*, *24*(10), 997–1010.

Henrich, J., Heine, S. J., & Norenzayan, A. (2010). The weirdest people in the world? *Behavioral and Brain Sciences*, *33*, 61–135. https://doi.org/10.1017/S0140525X0999152X

Houghton, C., Casey, D., Shaw, D., & Murphy, K. (2013). Rigour in qualitative case-study research. *Nurse Researcher*, *20*(4), 12–17. https://bmcmedresmethodol.biomedcentral.com/articles/10.1186/1471-2288-13-72

Ingram, D. (2023). Self-driving cars are oftentimes victims in hit-and-run incidents. *NBC News*. https://www.nbcnews.com/tech/innovation/self-driving-car-waymo-cruise-uber-hit-run-accidents-rcna76857

Ismayilov, E. A. (2022). Cloud security: A review of current issues and proposed solutions. *Azerbaijan Journal of High Performance Computing*. https://api.semanticscholar.org/CorpusID:252960345

Itemis. (2023). Cybersecurity and autonomous vehicle systems. *itemis Knowledge-Center*. https://www.itemis.com/en/cybersecurity-and-autonomous-vehicle-systems

Jena, K. (2023). Zero-trust security models overview. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. https://api.semanticscholar.org/CorpusID:266877401

Joshi, A., Kale, S., Chandel, S., & Pal, D. K. (2015). Likert scale: Explored and explained. *British Journal of Applied Science & Technology*, *7*(4), 396. https://doi.org/10.9734/BJAST/2015/14975

Khatri, N., Shrestha, R., & Nam, S. Y. (2021). Security issues with in-vehicle networks, and enhanced countermeasures based on blockchain. *Electronics*, *10*(8). https://doi.org/10.3390/electronics10080893

Kim, K., Kim, J. S., Jeong, S., Park, J.-H., & Kim, H. K. (2021). Cybersecurity for autonomous vehicles: Review of attacks and defense. *Computers & Security*, *103*, 102150. https://doi.org/https://doi.org/10.1016/j.cose.2020.102150

Kim, W. J., & Lee, J.-D. (2009, May). Measuring the role of technology-push and demand-pull in the dynamic development of the semiconductor industry: The case of the global dram market. https://doi.org/10.1016/s1514-0326(09)60007-6

Klinedinst, D. (2016, August). On board diagnostics: Risks and vulnerabilities of the connected vehicle [Accessed: 2024-Apr-25]. https://insights.sei.cmu.edu/blog/board-diagnostics-risks-and-vulnerabilities-connected-vehicle/

KPMG. (2020). 2020 autonomous vehicles readiness index. https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2020/07/2020-autonomous-vehicles-readiness-index.pdf

Krause, C. (2024, May). *Amazon case study: Lessons from jeff bezos' leadership and innovation*. https://cdotimes.com/2024/05/23/amazon-case-study-lessons-from-jeff-bezos-leadership-and-innovation/

Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. *Educational and psychological measurement*, *30*(3), 607–610.

Krisher, T., & Dazio, S. (2022). Felony charges are 1st in a fatal crash involving autopilot. *AP News*. https://apnews.com/article/tesla-autopilot-fatal-crash-charges-91b4a0341e07244f3f03051b5c2462ae

Krosnick, J. A. (1999). Survey research. *Annual Review of Psychology*, *50*(1), 537–567.

Kshetri, N., & Voas, J. M. (2019). Supply chain trust. *IT Professional*, *21*, 6–10. https://api.semanticscholar.org/CorpusID:90263530

Kukkala, V. K., Thiruloga, S. V., & Pasricha, S. (2022). Roadmap for cybersecurity in autonomous vehicles.

Levinthal, D. A. (1991). Organizational adaptation and environmental selection-interrelated processes of change. *Organization Science*, *2*(1), 140–145.

Liang, G., Fu, W., & Wang, K. (2019). Analysis of t-test misuses and SPSS operations in medical research papers. *Burns & Trauma*, *7*, s41038-019-0170–3. https://doi.org/10.1186/s41038-019-0170-3

Lin, L. (2018). Bias caused by sampling error in meta-analysis with small sample sizes. *PLOS ONE*, *13*(9), 1–19. https://doi.org/10.1371/journal.pone.0204056

Luxner, T. (2023). Cloud computing trends and statistics: Flexera 2023 state of the cloud report. https://www.flexera.com/blog/cloud/cloud-computing-trends-flexera-2023-state-of-the-cloud-report/

Magaldi, D., & Berler, M. (2020). Semi-structured interviews. In *Encyclopedia of personality and individual differences* (pp. 4825–4830). Springer International Publishing. https://doi.org/10.1007/978-3-319-24612-3_857

Markit, I. (2022). Autonomous vehicle sales to surpass 33 million annually in 2040, enabling new autonomous mobility in more than 26 percent of new car sales, ihs markit says. https://www.businesswire.com/news/home/20180102005159/en/Autonomous-Vehicle-Sales-to-Surpass-33-Million-Annually-in-2040-Enabling-New-Autonomous-Mobility-in-More-Than-26-Percent-of-New-Car-Sales-IHS-Markit-Says

McKinsey & Company. (2023). Autonomous driving's future: Convenient and connected. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/autonomous-drivings-future-convenient-and-connected

McKinsey & Company. (2024). *spotlight on mobility trends*. https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/spotlight-on-mobility-trends

Mehta, A. (2022). France: Taxi driver files lawsuit against tesla after fatal crash in paris. *Sky News*. https://news.sky.com/story/france-taxi-driver-files-lawsuit-against-tesla-after-fatal-crash-in-paris-12571465

Mercedes-Benz. (2023). U.s. availability of drive pilot. https://group.mercedes-benz.com/innovation/product-innovation/autonomous-driving/drive-pilot-launch-usa.html

Miles, R. E., & Snow, C. C. (1984). Fit, failure and the hall of fame. *California Management Review*, *26*(3), 10–28.

MIT CSAIL. (2020). Explained: Levels of autonomy in self-driving cars. https://www.csail.mit.edu/news/explained-levels-autonomy-self-driving-cars

Mohsienuddin, S., Mohammad, S., & Lakshmisri. (2020). Security automation in information technology. https://api.semanticscholar.org/CorpusID:244868351

Möller, D. P. F., & Haas, R. E. (2019). *Guide to automotive connectivity and cybersecurity: Trends, technologies, innovations and applications: Trends, technologies, innovations and applications* (1st ed.). Springer Cham. https://doi.org/10.1007/978-3-319-73512-2

Morris, D., Madzudzo, G., & García-Pérez, A. (2020). Cybersecurity threats in the auto industry: Tensions in the knowledge environment. *Technological Forecasting and Social Change*, *157*, 120102. https://doi.org/10.1016/j.techfore.2020.120102

Nadella, S. (2017). *Hit refresh: The quest to rediscover microsoft's soul and imagine a better future for everyone*. Harper Business.

Nash, L., Boehmer, G., Wireman, M., & Hillaker, A. (2024). Securing the future of mobility. *Deloitte*. https://www2.deloitte.com/content/dam/Deloitte/be/Documents/strategy/Securing%20The%20Future%20Of%20Mobility.pdf

National Highway Traffic Safety Administration. (2021). Cybersecurity best practices for modern vehicles. https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/vehicle_cybersecurity_best_practices_01072021.pdf

Nobles, C., Burrell, D., Burton, S., & Waller, T. (2023, March). Driving into cybersecurity trouble with autonomous vehicles. https://doi.org/10.4018/978-1-6684-7207-1.ch013

Oladimeji, D., Rasheed, A., Varol, C., Baza, M., Alshahrani, H., & Baz, A. (2023). Canattack: Assessing vulnerabilities within controller area network. *Sensors*, *23*(19). https://doi.org/10.3390/s23198223

Oliver Wyman. (2019). Building the automotive industry of 2030. https://www.oliverwyman.com/our-expertise/insights/2019/jun/automotive-manager-2019/cover-story/building-the-automotive-industry-of-2030.html

Parliamentary Assembly of the Council of Europe. (2020, September). *Legal aspects of "autonomous" vehicles* (tech. rep.) (Technical report). https://assembly.coe.int/LifeRay/JUR/Pdf/DocsAndDecs/2020/AS-JUR-2020-20-EN.pdf

Pethő, Z., Török, Á., & Szalay, Z. (2021). A survey of new orientations in the field of vehicular cybersecurity, applying artificial intelligence based methods. *Transactions on Emerging Telecommunications Technologies*, *32*. https://doi.org/10.1002/ett.4325

Polaris Market Research. (2022). Self-driving cars market share, size, trends, industry analysis report, by component; by electric vehicle; by system; by mobility type (shared mobility, personal mobility); by region; segment forecast, 2022 - 2030. https://www.polarismarketresearch.com/press-releases/autonomous-vehicle-market

Porter, M. E. (1980). *Competitive strategy: Techniques for analyzing industries and competitors*. Free Press.

Prasetio, E. A., & Nurliyana, C. (2023). Evaluating perceived safety of autonomous vehicle: The influence of privacy and cybersecurity to cognitive and emotional safety. *IATSS Research*, *47*(2), 160–170. https://doi.org/https://doi.org/10.1016/j.iatssr.2023.06.001

Qu, S., & Dumay, J. (1995). The qualitative research interview. *Qualitative research in accounting & management*.

Robra, B., Pazaitis, A., Giotitsas, C., & Pansera, M. (2023). From creative destruction to convivial innovation - a post-growth perspective. *Technovation*, *125*, 102760. https://doi.org/10.1016/j.technovation.2023.102760

Rogers, E. M. (1962, January). Diffusion of innovations. https://journals.lww.com/jcehp/citation/1997/17010/diffusion_of_innovations.9.aspx

Rowley, J. (2012). Conducting research interviews. *Management Research Review*, *35*(3/4), 260–271. https://doi.org/10.1108/01409171211210154

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15). https://doi.org/10.3390/s23156666

Sandler, M. (2023). Autonomous vehicle cybersecurity: An overview. *CYRES Consulting*. https://www.cyres-consulting.com/autonomous-vehicle-cyber-security-overview/

Schmittner, C., & Macher, G. (2019). Automotive cybersecurity standards - relation and overview. In A. Romanovsky, E. Troubitsyna, I. Gashi, E. Schoitsch, & F. Bitsch (Eds.), *Computer safety, reliability, and security. safecomp 2019* (Vol. 11699). Springer, Cham. https://doi.org/10.1007/978-3-030-26250-1_12

Schumpeter, J. A. (1994). *Capitalism, socialism, and democracy*. Routledge.

Seetharaman, A., Patwa, N., Jadhav, V., Saravanan, A. S., & Sangeeth, D. (2021). Impact of factors influencing cyber threats on autonomous vehicles. *Applied Artificial Intelligence*, *35*(2), 105–132. https://doi.org/10.1080/08839514.2020.1799149

Sekaran, U., & Bougie, R. (2016). *Research methods for business: A skill-building approach* (7th ed.). Wiley.

Shah, V., & Ali, A. (2023). Effect of cyber vulnerabilities on the adoption of self-driving vehicles –a review. *3*, 43–49. https://doi.org/10.47893/IJSSAN.2023.1230

Simon, H. A. (1997). *Administrative behavior* (4th). Free Press.

Sirisup, N., & Petchmark, P. (2022). Factors affecting the acceptance of autonomous vehicle technology: A multiple regression analysis. *Contemporary Issues in Behavioral and Social Sciences*.

Stackpole, B. (2022). How to build a culture of cybersecurity. https://mitsloan.mit.edu/ideas-made-to-matter/how-to-build-a-culture-cybersecurity

Stagnaro, C. (2023). Cybersecurity: The key to autonomous driving. *InfraJournal*. https://www.infrajournal.com/en/w/cyber-security-the-key-to-automated-driving

Stedman, C. (2024). The ultimate guide to cybersecurity planning for businesses. https://www.techtarget.com/searchsecurity/The-ultimate-guide-to-cybersecurity-planning-for-businesses

TechVertu Cyber Security. (2024). Navigating cybersecurity challenges in driving technology. https://www.techvertu.co.uk/blog/cybersecurity-challenges-in-driving-technology

Teece, D. J. (2007). Explicating dynamic capabilities: The nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*, *28*(13), 1319–1350.

Teece, D. J., Pisano, G., & Shuen, A. (1997). Dynamic capabilities and strategic management. *Strategic Management Journal*, *18*(7), 509–533.

Tomorrow Bio. (2023). Challenges for mass adoption of driverless cars. *Tomorrow Bio Insights*. https://www.tomorrow.bio/post/challenges-for-mass-adoption-of-driverless-cars-2023-06-4603475547-iot

Tripsas, M., & Gavetti, G. (2000). Capabilities, cognition, and inertia: Evidence from digital imaging. *Strategic Management Journal*, *21*(10-11), 1147–1161.

TurnerIII, D. W. (2010). Qualitative interview design: A practical guide for novice investigators. http://www.nova.edu/ssss/QR/QR15-3/qid.pdf

UK Department for Transport. (2022, August). *Connected & automated mobility 2025: Realising the benefits of self-driving vehicles* (tech. rep.) (Technical report). https://assets.publishing.service.gov.uk/media/62ff438c8fa8f504cdec92df/cam-2025-realising-benefits-self-driving-vehicles.pdf

United Nations Economic Commission for Europe (UNECE). (2022). Framework document on automated/autonomous vehicles. https://unece.org/sites/default/files/2022-02/FDAV_Brochure%20-%20Update%20Clean%20Version.pdf

Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science*, *46*(2), 186–204.

Venkatraman, N., & Camillus, J. C. (1984). Exploring the concept of "fit" in strategic management. *Academy of Management Review*, *9*(3), 513–525.

Vicens, A. (2024). Leaked documents show how firm supports chinese hacking operations. *CyberScoop*. https://cyberscoop.com/isoon-chinese-apt-contractor-leak/

Walsh, S. T., Kirchhoff, B. A., & Newbert, S. L. (2002). Differentiating market strategies for disruptive technologies. *IEEE Transactions on Engineering Management*, *49*(4), 341–351. https://doi.org/10.1109/tem.2002.806718

Wang, X. (2021). On the feasibility of detecting software supply chain attacks. *MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM)*, 458–463. https://api.semanticscholar.org/CorpusID:245594987

Weiss, R. S. (1995). *Learning from strangers: The art and method of qualitative interview studies*. Simon; Schuster.

World Economic Forum (WEF). (2024, January). *Global cybersecurity outlook 2024* (Insight Report) (In collaboration with Accenture). World Economic Forum.

Appendix A: Outline of survey questions

Table 6: Survey Questions Outline

Q No.	Question	Question Type	Answer Options
General Familiarity and Perception of Autonomous Vehicles			
Basic information concerning the concept of autonomous vehicles was provided.			
1	Have you ever used or interacted with an autonomous vehicle?	Multiple choice	Yes; No; Prefer not to say
2	On a scale of 1 (not at all familiar) to 5 (very familiar), how familiar are you with the concept of self-driving cars?	5-point Likert scale	Not familiar at all (1) - Extremely familiar (5)
3	On a scale of 1 (not at all familiar) to 5 (very familiar), how familiar are you with the technology behind autonomous vehicles?	5-point Likert scale	Not familiar at all (1) - Extremely familiar (5)
4	Rate your agreement with these statements: - "Autonomous vehicles can improve road safety by reducing human error." - "I would feel comfortable riding in an autonomous vehicle." - "Autonomous vehicles will significantly change the way we travel. "	5-point Likert scale	Strongly disagree (1) - Strongly agree (5); Not applicable/Don't know
Levels of Autonomy in Self-Driving Cars			
Basic information concerning the different levels of autonomy was provided.			
5	Please indicate your willingness to adopt or use self-driving cars at each of the following levels of autonomy on a scale from 1 to 5, with 5 being the highest level of willingness (Levels 0 to 5).	Matrix question	1 - 5; Not applicable/Don't know
Cybersecurity Awareness and Concerns			
6	How concerned are you about the following cybersecurity risks in autonomous vehicles? - "Unauthorized access to personal data." - "Remote hijacking of vehicle controls." - "Vehicle safety compromised due to malicious software attacks."	Matrix question	Not concerned at all (1) - Very concerned (5); Not applicable/Don't know
7	Are you aware of any cybersecurity incidents involving autonomous vehicles?	Multiple choice	Yes; No; Not Sure
8	Rate your agreement with: - "Cybersecurity risks in self-driving cars are a significant concern for me." - "I trust the current cybersecurity measures in autonomous vehicles." - "The possibility of cybersecurity breaches deters me from adopting autonomous vehicles."	5-point Likert scale	Strongly disagree (1) - Strongly agree (5); Not applicable/Don't know
Levels of Autonomy in Self-Driving Cars After Cybersecurity Awareness and Concerns			
9	After reflecting on the cybersecurity concerns in the previous section, please indicate your willingness to adopt or use self-driving cars at each of the following levels of autonomy on a scale from 1 to 5, with 5 being the highest level of willingness (Levels 0 to 5).	Matrix question	1 - 5; Not applicable/Don't know
Adoption and Acceptance (TAM)			
10	Rate your agreement with: - "The benefits of self-driving cars outweigh their cybersecurity risks." - "If cybersecurity concerns were adequately addressed, I would prefer a self-driving car."	5-point Likert scale	Strongly disagree (1) - Strongly agree (5); Not applicable/Don't know

Table 6 – Survey Questions Outline (continued from previous page)

Q No.	Question	Question Type	Answer Options
11	This question aims to check if you are paying attention while reading the statements. Please answer this statement with 2	Quality Control Question	1; 2; 3; 4; 5
12	How important are the following factors when considering adopting self-driving cars? - Safety; - Cybersecurity; - Convenience; - Cost; - Environmental impact.	Rating scale question	0 to 100
13	If autonomous vehicles had a proven strong record of cybersecurity, how likely would you use one for daily commuting?	5-point Likert scale	Extremely unlikely (1) - Extremely likely (5); Not applicable/Don't know
14	What would increase your willingness to use self-driving cars?	Multiple choice (multiple selections possible)	Enhanced cybersecurity measures; Proven safety record; Lower costs; Personal enjoyment of technology
15	Would you be willing to pay more for enhanced cybersecurity features in a self-driving car, assuming the cost is the same as a traditional vehicle?	Multiple choice	Up to 10% more; Up to 20% more; Up to 30% more; I am not sure
Demographic and Background Questions			
16	What is your age group?	Multiple choice	Less than 18; 18-24; 25-34; 35-44; 45-54; 55-64; 65+
17	What gender do you identify with?	Multiple choice	Male; Female; Non-binary/Third gender; Prefer not to say
18	Which country are you from?	Multiple choice	Portugal; France; Spain; Italy; Germany; Switzerland; Belgium; the Netherlands; Denmark; Norway; Sweden; United Kingdom; United States; Other (can be specified)
19	What is the highest level of education you have completed?	Multiple choice	Less than high school; High school graduate; Professional degree; Bachelor's degree; Master's degree; Doctorate or higher
20	What was your household income (in Euros) before taxes in the past year?	Multiple choice	Less than €20k; €20k-39.999k; €40k-59.999k; €60k-79.999k; €80k-99.999k; €100k-149.999k; More than €150k; Prefer not to say
21	What is your political affiliation or orientation?	Multiple choice	Conservative; Liberal; Moderate; Non-affiliated; Other; Prefer not to say
22	What is your primary mode of transportation?	Multiple choice	Personal vehicle; Public transportation; Walking/Biking; Ridesharing; Other
23	Do you currently hold a valid driver's license?	Multiple choice	Yes; No; Prefer not to say

Appendix B: Expert Interviews

.1 Interview scripts

The following script outlines a set of questions that were posed to the various experts during interviews. It is important to note that, as these were semi-structured interviews, some questions were adjusted based on each expert's area of expertise.

1. In your experience, what are the most recent trends in the auto sector?

2. Could you please rank them from the most to the least impactful?

3. In your experience, what are the most pressing cybersecurity concerns in the auto sector today?

4. Could you rank these concerns in terms of their potential to influence consumer decisions regarding self-driving cars?

5. How do you perceive the materiality of cybersecurity issues when it comes to the public's willingness to adopt self-driving cars?

6. How do cybersecurity issues in the auto sector compare to those in other industries in terms of complexity and urgency?

7. Are there cybersecurity challenges that you believe are unique to the auto sector, especially concerning self-driving technology?

8. In the field of self-driving cars, would you say the cyber threats are more significant, less, or just different from conventional vehicles?

9. Could you rate the current cybersecurity standards in the automotive sector on a scale of 1-10, specifically in terms of compliance and effectiveness?

10. On a scale of 1 to 10, how would you assess the auto industry's readiness to manage cybersecurity risks associated with self-driving cars?

11. What mitigation strategies do you think are most critical for countering cybersecurity threats to self-driving cars?

12. Are there lessons or strategies from other sectors that you believe could be adapted to improve cybersecurity in the automotive field?

13. What mitigation strategies do you think are most critical for countering public opinion concerns regarding cybersecurity threats to self-driving cars?

14. Based on our discussion, do you feel that cybersecurity concerns are currently a major barrier to the adoption of self-driving cars?

.2 Summary of interview 1: AW

What do you believe are the most pressing cybersecurity concerns in the automotive sector today?

AW: Privacy is a significant concern, especially with the potential collection of information for other purposes. For example, Chinese cars might gather intelligence from US citizens' vehicles. This is a legitimate concern, especially if you work for a Fortune 500 company and discuss sensitive technology in your car. It could be problematic if the car manufacturer, particularly a Chinese company, can listen to your conversation.

Another concern is the safety of the driver, especially given the life-and-death nature of driving. If you let a smart car drive for you, it needs to be highly secure in predicting, choosing, and making the right decisions based on the data it has. I believe these two issues — privacy and safety — are the primary concerns.

How would you rank these concerns?

AW: The most crucial concern is safety. In cybersecurity, there is the CIA triad, which is fundamental to web security: confidentiality, integrity, and availability. Confidentiality aligns with privacy, ensuring things remain confidential.

Maintaining your car's integrity and availability is essential to ensure it operates as intended without interference. This integrity aspect is vital for the vehicle's functionality. Safety involves protecting the car from unauthorized access or alterations, preventing anyone from taking control and manipulating it. While privacy is also important, the safety and preservation of life take precedence over privacy concerns.

How do cybersecurity issues in the automotive sector compare to other industries in terms of complexity and urgency?

AW: Cybersecurity is essential in many fields, but it is especially crucial for cars, as it can affect life and death. Other industries, such as healthcare, also have life-and-death implications. It is not easy to compare, but I believe it is vital in the automotive industry — perhaps even more

so than in sectors like banking. While cybersecurity in banking is essential because it concerns money, life is more important. So, compared to an industry like banking, cybersecurity in the automotive sector is probably more critical because it directly involves people's lives. However, that does not mean cybersecurity in banking is unimportant; it is just vital in the automotive industry.

What is the expert perception of the materiality of cybersecurity issues when it comes to public perception?

AW: People have varying perspectives on cybersecurity based on their field knowledge. Some might be overly concerned about cybersecurity issues, while others might be too lax. It's challenging to generalize what people believe, but generally speaking, cybersecurity is being taken more seriously, and investing in it is becoming increasingly common. Cybersecurity was not widely discussed ten years ago; only the most tech-savvy individuals could speak about it. However, many people consider cybersecurity a concern and take it seriously today.

People are now more concerned about adopting new technologies, especially as these technologies increasingly integrate with daily life. Autonomous driving, for example, involves relinquishing control to AI, which can be intimidating. We are at a crucial moment in humanity's development where, in some aspects, we are ceding control to AI. Are people more concerned about adopting new technologies? I think they are. However, we are in an exciting time with AI becoming so involved in our lives, and it is natural to feel a bit apprehensive about its growing influence and control.

What mitigation strategies are the most critical for countering cybersecurity threats to self-driving cars and potential lessons or strategies from other sectors that could be adapted to improve cybersecurity in the automotive field?

AW: Limiting remote access to cars is important. Remote access remains a significant concern. Ideally, car manufacturers should prevent this type of access. Even in cases where remote access is necessary, such as for software updates in Tesla vehicles, it should be highly restricted. No one should have broad remote control over your car, as this creates vulnerabilities.

If a company like Tesla were hacked, malicious actors could potentially take control of vehicles. Remote access should be strictly controlled or avoided altogether. Additionally, when manufacturing cars, it is crucial to ensure that they are configured correctly and that no one can alter the configurations.

Do you believe cybersecurity concerns will affect the adoption of self-driving cars?

AW: The success of autonomous driving depends more on the quality of the AI model than on cybersecurity concerns. While there may be cybersecurity concerns, I think creating a highly secure solution to prevent remote access to the car and ensure that no one can reconfigure or change the car's settings is possible. Improving the AI model will likely be crucial to the success of autonomous vehicles, and I think security issues can be managed effectively. However, I am not an expert in the automotive industry, so this is just my perspective.

.3 Summary of interview 2: AR

What do you believe are the most pressing cybersecurity concerns in the automobile sector today?

AR: I work with industrial control systems in the transport sector, primarily focusing on train controls and infrastructure. When looking at other sectors, the treatment of systems is not vastly different. A CSA (cybersecurity analyst) in a factory or oil refinery would find similar principles across sectors, including rolling stock for trains and buses.

There is a trend toward standardization and increased interoperability, which can reduce both costs and complexity for malicious actors. This trend also involves increased exposure to Internet services, which we need to account for.

Many believe systems are currently safe due to their complexity. Each attack now needs to be engineered for a specific scenario, device, or system. However, as standardization evolves, systems become more aligned and integrated, making attacks cheaper and easier, similar to what we saw with PCs.

What is the expert perception of the materiality of cybersecurity issues when it comes to public perception?

AR: Until a major cyberattack on industrial applications causes loss of life, I do not foresee the public having a strong awareness of the issue. If an attack of this magnitude occurs, public awareness and adoption of cybersecurity measures will likely increase rapidly. Typically, people do not consider cyberattacks on their vehicles, but demonstrations have shown how easy it is to hack into a modern car without a key, as critical vehicle functions can be accessed by the correct CAN bus and reverse engineering. Most people are not aware of this vulnerability.

How would you rate the current cybersecurity standards in the automotive sector?

AR: On a scale of 1 to 10, I would rate the current cybersecurity standards in the automotive sector relatively low, perhaps around 2 or 3. The standards will drastically improve as we move from traditional systems to more IP-based ones.

What is the uniqueness of cyber threats in the automotive industry?

AR: You will not find a universal hacking tool that can target all models from different manufacturers. If a vehicle manufacturer uses the same IT infrastructure across models, it might be possible to develop an attack for that specific model range. Due to limited hacking capabilities in vehicles, implementing attacks is challenging. The vehicle's communication systems, like the gateway using GSM or 4G, are connected to the media unit rather than the vehicle's critical systems.

How ready is the automotive industry to manage cyber attacks?

AR: Regarding self-driving cars, three approaches exist. The first involves making decisions offsite, the second allows the vehicle to handle straightforward tasks while offloading complex tasks to a data center, and the third involves the vehicle making all decisions internally.

Relying on offsite infrastructure increases exposure to external communication. Using an encrypted link directly to the data center can mitigate this. The vehicle still needs capabilities to validate data integrity and safe-list commands within the onboard unit (OBU).

How do cyber threats in the automotive industry compare to other sectors?

AR: The challenges are broadly similar across sectors. Vehicles can be particularly lucrative targets due to their widespread presence, allowing malicious actors to target an entire fleet. Vehicle cybersecurity issues are similar to those in other industrial applications but often involve limited computing power and power consumption.

What are the most critical mitigation strategies for countering cybersecurity threats to self-driving cars?

AR: Isolating critical systems and establishing validation between critical and less critical assets is a good starting point. Using virtual containers within systems can be beneficial, as well as validation at each stage of the value chain.

Devices that communicate directly with the car, such as fobs over a 2.4 GHz transmission, pose significant risks and need to be addressed.

Are there potential lessons or strategies from other sectors that could be adapted to improve cybersecurity in the automotive field?

AR: In industrial applications, including vehicle systems, we rely on established cybersecurity standards like ISO/IEC 62443. System design should be based on risk analysis, accepting a certain level of risk and establishing countermeasures to meet the targeted security level.

Do you believe cybersecurity concerns will affect the adoption of self-driving cars?

AR: I do not believe cybersecurity concerns are the primary barrier to adopting self-driving cars. There are many larger hurdles to overcome first. The general public is not fully aware of the cybersecurity issues in traditional vehicles. Modern vehicles share similar technologies with self-driving cars, such as brake-by-wire systems, showing that cybersecurity is not a unique hurdle for self-driving cars compared to modern automotive design.

.4 Summary of interview 3: EC

What are the most pressing cybersecurity concerns in the auto sector today? How do they influence consumer decisions about self-driving cars?

EC: I have a somewhat pessimistic view of cybersecurity in technology, shaped by my experience in incident response. The main concern now is the security of IoT devices, like smart home appliances, which track user data. This issue extends to autonomous vehicles that rely on communication with central systems and other cars. These vehicles must be viewed as endpoints requiring robust security, similar to mobile devices and computers. Security measures must encompass the entire ecosystem, not just the vehicle.

For instance, autonomous vehicles have OBD ports for diagnostics that can be exploited. Also, cars with emergency buttons already communicate with central servers. Ensuring encryption of this data, both in transit and at rest, is crucial. Supply chain security is another concern, as components come from various global sources, posing risks of malicious insertions.

Authentication and trust in the vehicle's communication are vital as attackers quickly adapt to new technologies. Thus, autonomous cars need redundant systems to bypass tampered data and maintain safety. Ultimately, transparent monitoring and robust certifications are essential to build consumer trust.

How material are cybersecurity issues in the public's willingness to adopt self-driving cars?

EC: The average consumer doesn't prioritize cybersecurity. They are generally unaware of the

strict cybersecurity laws being implemented. It's the responsibility of governments to enforce these laws and of manufacturers to comply. Consumers focus on vehicle brand and color rather than security features. However, security professionals and economic operators must ensure these vehicles are safe.

In essence, while consumers may not think about cybersecurity daily, state regulation and company compliance are crucial. This ensures the vehicles are secure without impacting the consumer's purchase decision.

How do cybersecurity issues in the auto sector compare to other industries? Are there unique challenges for self-driving technology?

EC: My view is technology-agnostic; cybersecurity concerns in the auto sector are similar to those in IT or OT. Autonomous vehicles are endpoints with specific security needs. Currently, IT monitoring is straightforward, but industrial OT environments are more challenging due to outdated systems.

For autonomous vehicles, the challenge is monitoring control centers and the cars themselves. Real-time data collection and ensuring secure communication are crucial. Direct attacks on vehicles are possible, like using OBD writers to install malware. However, these are similar to existing IT and OT security challenges.

How would you rate the current cybersecurity standards in the automotive sector? How ready is the industry to manage cybersecurity risks for self-driving cars?

EC: Unfortunately, many sectors, including automotive, implement security controls mainly for compliance rather than actual security. The automotive industry, driven by profitability, follows legal mandates but often lacks effective security measures.

Companies are not equipped for 24/7 monitoring due to high costs. Subcontracting can lead to gaps in security due to a lack of specific context. Thus, companies start with compliance and progressively enhance security as incidents occur. Effective readiness is lacking, as being compliant doesn't always mean being secure.

To improve this, the concept of "security by design" should be integrated from the start. However, this is challenging for companies with long-established infrastructures. The focus should be on minimizing damage without halting operations, akin to managing a constantly burning train.

What critical strategies are needed to counter cybersecurity threats to self-driving cars? Can lessons from other sectors be adapted?

EC: Autonomous vehicles must be treated as endpoints, similar to mobile devices and PCs. Robust endpoint security and data encryption are essential. Supply chain security, redundant systems, and strong authentication mechanisms are critical.

Lessons from the aviation industry, which uses strict component controls, can be adapted. IT and OT sectors offer insights into monitoring and prevention systems. Implementing data loss prevention (DLP) mechanisms, which are common in corporate environments, can ensure secure data access and transport. Drawing from the IT sector, placing Network Intrusion Detection Systems (NIDS) or Intrusion Prevention Systems (IPS) in-vehicle communication networks can help detect and prevent malicious activities. These measures, along with continuous education on cybersecurity practices, will enhance the resilience of autonomous vehicles.

Do you think cybersecurity concerns are a major barrier to the adoption of self-driving cars?

EC: While significant, cybersecurity concerns are not seen as a major barrier by consumers. They prioritize brand reputation, cost, and convenience over security features. However, governments and manufacturers must establish stringent regulations and standards to ensure safety and build trust. Consumers rely on manufacturers and regulators to address cybersecurity risks. Robust measures, transparent monitoring, and strict compliance will enhance consumer confidence in autonomous vehicles. As these standards become more rigorous, they will help mitigate risks and foster a safer environment for adopting self-driving technology.

The path to secure autonomous vehicles involves a multi-faceted approach. By learning from other industries and integrating robust security measures, we can create a safe ecosystem for self-driving cars. This will not only protect consumers but also encourage wider adoption of this transformative technology.

.5 Summary of interview 4: PG

What are the most urgent cybersecurity concerns in the automotive sector currently?

PG: I think these concerns are generic to the entire market, so they also apply to the automotive market. The theft of personal data is a significant concern. Vehicles accumulate a lot of information, such as biometric data and vehicle tracking. Hacker attacks, whether ransomware,

malware, or others, are another classic concern. Cars use a lot of technology, including many radars and sensors. Interference can affect many cars, causing chaos. Unauthorized remote access to the vehicle is also a major concern. These seem to be the three biggest concerns before buying an autonomous vehicle.

Could you rank these concerns in terms of their potential to influence consumer decisions regarding autonomous cars?

PG: First is remote access or unauthorized access to the vehicle, second is hacker attacks, and third is data theft. Although data theft is worrying, it does not compromise the physical integrity of people or vehicles.

How do you perceive the materiality of cybersecurity issues when it comes to the public's willingness to adopt autonomous cars?

PG: Working in cybersecurity, I am cautious about purchasing an autonomous car due to the potential threats. We know there are no 100% secure systems; each one has vulnerabilities. This technology has grown quickly, and there may be some rough edges. I believe this evolution bears similarities to the development of smart TVs. People will either ignore the risks and adopt the technology or understand the cybersecurity issues and resist adopting these technologies.

However, buying a car is not the same as buying a television because this issue can jeopardize their physical integrity and people are becoming aware of these risks. The news frequently reports on attacks on companies, including those in secure sectors like healthcare. If large companies with robust security systems can be attacked, it should be easier for a car to be attacked, especially since increasing cybersecurity measures would make the vehicle more expensive. For all these reasons, I think people will be cautious.

Are there cybersecurity challenges unique to the automotive sector, especially concerning autonomous driving technology?

PG: For the most part, a system is a system, whether it is a car, a train, or a hospital. However, the automotive sector can cause physical harm, which can lead to accidents involving drivers, pedestrians, or other vehicles, resulting in significant and widespread damage. Vehicles operate on public roads, and many things can happen there.

Could you evaluate the current cybersecurity standards in the automotive sector, assigning a score from 0 to 10, and assess the readiness of the automotive industry to manage these risks?

PG: My knowledge of the current cybersecurity standards in the automotive sector is limited to what's common across all industries. Regarding specific standards unique to the automotive industry, I believe the initial challenges will be immense. Hackers are always ahead of those on the defense side, and now, with artificial intelligence, they have gotten ahead again. I would rate the current situation around 6 or 7 on a scale of 1 to 10.

Would you say that the cyber threats are smaller, greater, or just different from conventional vehicles, or are they similar?

PG: The level of complexity is similar to that of an autonomous car; maybe this one is a bit more complex. Current cars already have systems similar to those in autonomous vehicles; they just lack full driving autonomy. Some cars already allow you to let go of the wheel in traffic queues. So, these are small things, not fully autonomous driving, but they already have some autonomy and are concerning.

What are the mitigation strategies most critical to counter cybersecurity threats to autonomous cars? Are there lessons or strategies from other sectors that could improve automotive cybersecurity?

PG: The mitigation strategies will initially be the same as those in other sectors, such as banking, healthcare, and telecommunications. Adopting secure development policies integrates security into all project phases. Other measures include vulnerability assessments, risk analysis, audits, stress testing, and quality control. Ensuring suppliers implement security measures is crucial. Regulations specific to the automotive sector, similar to those in banking and healthcare, should be established. A regulatory body to facilitate the exchange of information between entities is fundamental.

What mitigation strategies are most critical to address public concerns about cybersecurity threats to autonomous cars?

PG: Regulation, such as standards like ISO 27001, ensures compliance with specific security policies. Companies with these certifications strengthen consumer confidence and are subject to periodic audits. This is crucial until there is a specific certification for these companies.

Do you consider cybersecurity concerns a potential barrier to adopting autonomous cars?

PG: Yes. Working in cybersecurity, we are aware of hacker attacks and other threats, giving us a more cautious perception of automation. The general public is becoming increasingly aware of cybersecurity risks. As long as cybersecurity insecurity persists, having cars drive us with-

out strong security guarantees poses significant challenges. However, some people will adopt, ignoring these risks.

.6 Summary of interview 5: JF

What are the most urgent concerns regarding cybersecurity in the automotive sector today?

JF: The current car has several dozen processor units on board, and a state-of-the-art vehicle has over a hundred million lines of code. Cybersecurity attacks can appear at many levels. The connectivity aspect brings new problems, and in cybersecurity, we never know where attacks are coming from. There are direct and indirect attacks, and our defenses are often only for known attacks. The problems arise with unknown attacks. To create systems tolerant to unknown failures, called Byzantine faults, we need to have the airplane model, which is highly redundant. However, we will not have that level of redundancy in cars due to cost constraints.

Some European standards and United Nations working groups are addressing these concerns. It is up to manufacturers to have rigorous policies, both in system construction and monitoring during operation. Detecting intrusions, identifying problems, and resolving them will prevent attacks from escalating. Consumers are interested in knowing if there were attacks and how companies handled them, seeking a certain level of transparency. Traditionally, many industries hide cybersecurity issues until catastrophic attacks become visible.

How do you perceive the materiality of cybersecurity problems in the public's disposition to adopt new technology like AVs?

JF: Cybersecurity will be vital because it is linked to critical safety systems. Cybersecurity is a component of overall safety, and people will adopt cars if they prove to be safe as a whole, including cybersecurity. The vehicle needs to be safe, and that includes preventing attackers from taking control.

How do you compare cybersecurity problems in the automotive sector with other sectors in terms of complexity and urgency? Are there cybersecurity challenges unique to the automotive industry, especially concerning AVs?

JF: The automotive sector is particularly difficult for cybersecurity because a car has dozens of components from various manufacturers, leading to numerous cross-implications. Cybersecurity in the automotive sector is almost the worst-case scenario, and adding connectivity and

over-the-air updates worsens the problem. Unique challenges include the diversity of software components and maintaining integrity. The car brand will be responsible for ensuring the security of autonomous communication technology. Incorrect data or sensor readings can deceive the software, affecting safety.

Cybersecurity challenges in the automotive sector are significant. Autonomous driving adds complexity when we have connectivity, as the more intelligent a technology is, the more challenging it becomes to maintain security. Theories in computer science address this issue, with systems assuming they will be attacked and surviving the attack. However, such systems need to be highly redundant, which is not feasible for cars.

How would you assess the automotive industry's readiness to manage these cybersecurity risks associated with AVs?

JF: It depends on the type of attack. The automotive and software industries are still in a complicated phase for most brands. Examples include Volkswagen's struggles with software. In the European Union, regulations are stricter than in other regions, which limits market entry but ensures higher standards. I would say the readiness of the automotive industry is close to a score of 9 or 10, as it is a top priority.

What mitigation strategies do you consider most critical to combating cybersecurity threats to autonomous cars?

JF: Sharing experiences among brands is crucial. By creating a database of attacks and incident information, brands could anonymize data and share attack strategies, promoting transparency without revealing specific details. This approach helps prevent the same issues from reoccurring in different brands.

Are there lessons or strategies from other sectors that you believe could be adapted to improve cybersecurity in autonomous cars?

JF: Drawing inspiration from critical systems industries like aviation and rail is useful. However, cars require a balance between innovation and safety. The market and society must decide the acceptable level of risk. There is more tolerance for human error than for robot error. The problem with new technologies is that they work well until the first incident occurs, leading to public apprehension and political pressure.

What mitigation strategies do you consider most critical to address public concerns about cybersecurity threats to autonomous cars?

JF: Transparency and rewarding ethical hacking are important. Companies should offer prizes to those who attack the system and disclose issues to the company rather than publicly. This builds consumer trust and ensures continuous improvement in security.

Do you consider cybersecurity concerns potentially a barrier to adopting autonomous cars?

JF: Yes. Cybersecurity can be a showstopper. Many projects worldwide, including autonomous drones, have not progressed due to cybersecurity concerns. Autonomous vehicles could follow a similar path. Technologically, everything is ready, but cybersecurity prevents further advancement. Public reaction to initial incidents will be critical in determining the future of technology.

.7 Summary of interview 6: PR

What are the most pressing cybersecurity concerns in the auto sector today? How do they influence consumer decisions about self-driving cars?

PR: The main concern is the potential for physical assets, like cars, to be remotely controlled, leading to dangerous situations. Additionally, cars are valuable, making them prime targets for attackers. Remote control increases the attack surface and potential consequences, making ransomware a significant threat.

Could you rank these concerns in terms of their potential to influence consumer decisions regarding self-driving cars?

PR: Resilience is crucial. Vehicles should be able to defend themselves and manage attack consequences. System resilience, involving redundancy like voting systems, is increasingly applied to autonomous vehicles. Companies like Tesla combine automotive and IT expertise to enhance vehicle software, which introduces cybersecurity issues but also improves safety through software updates.

How do you perceive the materiality of cybersecurity issues when it comes to the public's willingness to adopt self-driving cars?

PR: There is still skepticism about electric and autonomous cars. Most people choose cars based on brand, color, and aesthetics rather than technology. Information on car cybersecurity is not widely available, and even if it were, few would know how to interpret it. The market is evolving, but currently, cybersecurity is not a major consideration for consumers. As the technology matures and awareness increases, this may change, making cybersecurity a more

significant factor in purchasing decisions.

How do cybersecurity issues in the auto sector compare to those in other industries? Are there unique challenges for self-driving technology?

PR: Autonomous vehicles operate in urban environments, making malfunctions significant. The sheer number of vehicles adds to the complexity. Compared to factory robots, which can malfunction within a controlled environment, cars directly affect the physical world. Heavy vehicles can be as dangerous as bombs, facilitating terrorist attacks remotely. This makes the situation more critical than many other cybersecurity issues, requiring comprehensive security measures to protect public safety.

Are cyber threats more significant, less, or just different from conventional vehicles?

PR: Autonomous cars have more issues due to their technology. They must address both cybersecurity and privacy. Autonomous cars communicate with other cars and infrastructure, aiming for zero accidents by removing human error. However, mechanical or cybersecurity issues can still cause severe consequences. This interconnectedness and reliance on data make them more vulnerable to sophisticated cyber-attacks, necessitating advanced security protocols.

Could you rate the current cybersecurity standards in the automotive sector on a scale of 1-10 in terms of compliance and effectiveness?

PR: Manufacturers have been paying great attention to cybersecurity since interconnecting cars. Today, almost all vehicles have SIM cards for commands. Quantifying this concern is challenging, but I would give a high rating based on current knowledge. Some issues remain, like using HTTP instead of HTTPS, but overall, manufacturers are significantly concerned and investing in security. However, continuous improvements and stricter regulations are necessary to keep pace with evolving threats.

On a scale of 1 to 10, how would you assess the auto industry's readiness to manage cybersecurity risks for self-driving cars?

PR: The industry is not fully prepared because fully autonomous vehicles don't truly exist yet. In San Francisco, there are two operators limited to specific areas. Cars like Tesla collect extensive road data for autopilot functions, but full autonomous driving has not yet been achieved. The focus is on developing the technology, but readiness is still lacking. As the technology progresses, industry readiness will improve, but we are currently in the early stages.

What mitigation strategies are most critical for countering cybersecurity threats to self-driving cars?

PR: Resilience to attacks is crucial, involving internal decision-making based on data. This includes cybersecurity and physical attacks on sensors. Attacking a sensor with a laser could disrupt the vehicle's perception, making sensor redundancy important. Cybersecurity attacks could create traffic congestion. Ensuring the resilience of autonomous vehicles against such attacks is crucial, as these scenarios can significantly impact traffic flow and safety.

Are there lessons from other sectors that could improve cybersecurity in the automotive field?

PR: Lessons from traditional software cybersecurity and processor security can be applied to autonomous vehicles. These vehicles are like multiple computers processing data. Established practices in traditional software cybersecurity and processor security are being implemented in autonomous vehicles. Artificial intelligence also plays a key role in teaching cars to drive like humans, improving their decision-making and safety. However, cybersecurity measures must address potential consequences, balancing resilience and decision-making speed to ensure safety without introducing latency.

Do you feel cybersecurity concerns are a major barrier to the adoption of self-driving cars?

PR: While the public doesn't currently prioritize cybersecurity in vehicle choices, this will change as autonomous vehicles become more prevalent. Manufacturers will need to provide detailed cybersecurity information. The interconnected nature of these vehicles makes them vulnerable, driving the need for robust security measures to protect against threats. As awareness and technology advance, cybersecurity will become a significant factor in consumer decisions, pushing manufacturers to invest in more comprehensive security solutions.

.8 Summary of interview 7: ES

In your experience, what are the most recent trends in the automotive sector?

ES: Cars are implementing trends that have sparked significant debates. The most notable is the mandatory speed limiter, where cars recognize speed limits via cameras and sensors and automatically adjust speed. This has caused debate, as older and newer vehicles will coexist on the road. For example, a car overtaking a truck may brake when entering a speed limit zone, which could be dangerous. There needs to be a balance between technology and human action.

Car-to-car connectivity is another trend, allowing drivers to receive information about traffic and road conditions. This will take time to implement, as mixed systems will coexist initially. Eventually, there will need to be regulatory control for connectivity among all brands. Additionally, electric cars also face connectivity challenges. Tesla has its own charging system, while European systems use Type 2 or CCS connectors. Standardizing these systems is necessary for universal communication among brands.

Could you please rank these trends from the most to the least impactful?

ES: Mandatory speed limiters first, then car-to-car connectivity.

In your experience, what are the most pressing cybersecurity concerns in the automotive sector today?

ES: The universality of communication language and standardization are significant issues. Universal language eases connectivity but increases cybersecurity risks. If hackers learn to access one brand, they can access all others. Users are currently more interested in infotainment and driver assistance systems than in understanding the risks of connectivity. Vehicle communication raises privacy concerns as users resist technologies tracking their routes while enjoying services like Waze. Remote control features, like keyless entry, are popular but vulnerable to cyberattacks. For example, Mercedes cars communicate with the manufacturer for maintenance updates, sharing data that hackers could exploit.

Users are unaware their cars share information with manufacturers, making them susceptible to cyberattacks. Features like remote control for locking, unlocking, and preheating the car are convenient but increase security risks. Autonomous driving features, like emergency braking, can also cause issues. A colleague experienced sudden braking on a bridge due to air displacement from a passing train, causing an accident because the following car was unprepared for the stop.

Among the automatic and cybersecurity mechanisms we discussed earlier, which do you think are the main problems, ranking them from most to least important?

ES: Hacking is the most serious concern, as it could control the car's movement and cause unintended actions. Determining responsibility for such incidents is an ongoing discussion. Regulations will come through EU directives, ensuring vehicles meet safety standards, as the EU has been proactive in pressuring manufacturers to comply with safety features.

How would you rate, on a scale of 0 to 10, the current standards in the automotive industry

regarding cybersecurity, compliance, and effectiveness? Also, is the automotive industry prepared for a large-scale cyberattack?

ES: If asked, car manufacturers would say they are prepared, but I think not. There is a significant discussion about "my car, my data". Manufacturers argue that secrecy is necessary to minimize cyberattack risks, but the EU believes it hinders competition. No industry is fully prepared for a large-scale cyberattack, as even major players like Vodafone and Microsoft have been targets. The industry claims this secrecy reduces competition in after-sales by not divulging system details.

What could be crucial mitigation strategies to address public concerns about cybersecurity potentially?

ES: There should be a regulatory body guaranteeing security. People will sacrifice privacy if they see added value in return. Transparency is important, but realistically, it often boils down to money — for example, safety tests like Euro NCAP influence car purchases and insurance costs in Germany. However, in Portugal, car purchases are more emotional. Transparency and regulatory measures affect costs and consumer choices.

Do you think cybersecurity issues will affect the adoption of AVs?

ES: It will depend on whether brands generalize automation. The industry drives advancements, not customers. Brands must ensure they do not have cybersecurity problems to protect their reputation. For example, if Porsche had issues with its acceleration component, it would be a significant problem. People will accept connectivity and automation as they become available, driven by EU directives rather than consumer interest. Most users I know dislike and turn off features like lane-keeping and cruise control, which are mandated by EU directives.

Basically, automation and connectivity advancements will enhance safety and come from the industry. Significant opposition will only arise from numerous incidents. Although there have been news reports about Tesla's problems, high-end cars like Mercedes usually receive less attention, while minor issues with cheaper cars cause bigger uproars.

.9 Summary of interview 8: JB

In your experience, what are the most recent trends in the automotive sector?

JB: Recent trends in the automotive sector include the growing popularity of electric and hybrid vehicles, the development of autonomous driving technology, the integration of connectivity

and driver assistance technology, the use of lighter and more sustainable materials, and the rise of vehicle sharing and mobility services. These trends are shaping the automotive industry, influencing vehicle design, construction, and usage.

Could you rank them from most impactful to least impactful?

JB: The most impactful trend is the popularity of electric cars, followed by autonomous driving technology, the integration of connectivity and entertainment systems, and finally, the emergence of new business models such as vehicle sharing and pay-per-use features.

In your experience, what are the most urgent cybersecurity concerns in the automotive sector today?

JB: The most urgent concerns include protecting autonomous driving and driver assistance systems, ensuring customer data security, and preventing cyberattacks that could affect road safety. Monitoring and resolving vulnerabilities in infotainment and wireless systems is also crucial. Continuous evaluation of the value chain, including components, software, and services, is essential as well.

Could you rank these concerns in terms of their potential to influence consumers' decisions regarding autonomous cars?

JB: The most pressing issues are data privacy breaches, unauthorized remote control of vehicles, and failures in autonomous systems that could endanger passenger safety. Addressing these vulnerabilities is critical to building consumer trust and encouraging the adoption of autonomous technologies.

How do you perceive the materiality of cybersecurity issues when it comes to the public's willingness to adopt autonomous cars?

JB: Cybersecurity is crucial for public acceptance of connected technology, especially autonomous vehicles. The security of personal information and vehicle safety are significant concerns for consumers. Automotive companies must ensure the security of autonomous driving systems and convey confidence to consumers, as cybersecurity issues directly influence purchase decisions and the adoption of autonomous cars.

Are there cybersecurity challenges you consider unique to the automotive sector, especially regarding autonomous driving technology?

JB: Yes, unique challenges include the risk of vehicle control being compromised and access

to sensitive information through connected systems. Integrating advanced technologies like AI and ML adds complexity. V2X interactions and extensive supply chains for components are also fundamental factors.

Could you evaluate the current cybersecurity standards in the automotive sector on a scale from 1 to 10, specifically in terms of compliance and effectiveness?

JB: I would rate manufacturers highly, at 9.5, the supply chain at 7, and the service chain at 5. Compliance with standards from ISO, SAE, and NIST is essential. Relevant standards include ISO 26262 for functional safety, ISO/SAE 21434 for cybersecurity in road vehicles, SAE J3061 for developing cybersecurity in road vehicles, and NIST SP 800-53 for security controls. TISAX is also important for information security among automotive suppliers.

How would you rate the automotive industry's readiness to manage cybersecurity risks associated with autonomous cars on a scale from 1 to 10?

JB: I would rate manufacturers at 9.5, the supply chain at 7, and the service chain at 4.

What mitigation strategies do you consider most critical to combat cybersecurity threats to autonomous cars?

JB: Critical strategies include end-to-end encryption to protect communications, implementing firewalls and intrusion detection systems, secure software development practices, and regular updates with security patches. Educating users about vehicle security and collaborating among manufacturers, governments, and stakeholders to establish robust security standards are also essential. Lastly, legislation should support periodic inspections and prevent tampering.

What mitigation strategies do you consider most critical to address public concerns about cybersecurity threats to autonomous cars?

JB: Addressing public concerns requires making vehicle ignition dependent on manufacturer updates, using end-to-end encryption, implementing firewalls and intrusion detection systems, and employing robust software security techniques. Regular updates of vehicle systems are crucial, as well as educating users about maintaining security and fostering collaboration among stakeholders to establish and share security standards.

Based on our discussion, do you believe cybersecurity concerns are potentially a barrier to adopting autonomous cars?

JB: Yes, cybersecurity is a legitimate concern that can be a barrier to adopting autonomous cars.

The industry must ensure that autonomous cars are protected against cyber threats to address consumer concerns and encourage adoption. Transparency and collaboration among infrastructures, governing entities, and the value chain are essential to build trust in the technology.

.10 Summary of interview 9: CR

In your experience, what are the most recent trends in the automotive sector?

CR: The most significant trend is electric mobility. The widespread use of electric cars is the number-one trend, with brands focusing on achieving better ranges and values. Sustainability is part of this process as well, with resources used to make cars greener and less polluting. There is also digitalization and automation, both in car manufacturing and user experience. These components are critical, as factories require fewer workers, resulting in entirely different products. Additionally, car sharing, disrupted by the pandemic, is expected to see new business models as people only use cars part-time.

Could you rank them from most impactful to least impactful?

CR: The order would be electric mobility, followed by sustainability, digitalization and automation, and finally, car sharing.

In your experience, what are the most urgent cybersecurity concerns in the automotive sector today? Could you rank these concerns in terms of their potential to influence consumer decisions regarding autonomous cars?

CR: Hacking is the primary concern. The lack of security and the significant risk of an external entity altering technology or the manufacturing process are crucial factors. If a factory is attacked, it can be shut down, causing incalculable damage. The scarcity of specific components and parts makes the situation more vulnerable, as manufacturers might opt for dubious suppliers due to market shortages, with war problems, lack of components, and new technologies exacerbating these issues and affecting cybersecurity. Additionally, companies and individuals are not adequately prepared for this technology, aggravated by its ease of use and a lack of understanding of the model itself. These are the top concerns that could affect the market and should be the main focus.

Could you evaluate the current cybersecurity standards in the automotive sector on a scale of 1 to 10, specifically regarding compliance and effectiveness? How would you rate the automotive industry's readiness to manage cybersecurity risks associated with autonomous

cars on a scale of 1 to 10?

CR: With current products, preparation is shallow. We occasionally test phishing emails on our internal user database, and many people fall for them. These are signs that people are not prepared to protect themselves, their activities, or their cars, leading to significant factory costs. Even if it depends on the people, the protection level is generally shallow, around 2, 3, or 4.

And the sector itself, is it prepared to protect itself in the event of a large-scale attack?

CR: Based on what we hear in the media, incidents would quickly become known if they occurred. It does not appear that cyberattacks are primarily focused on this industry. The lack of attacks does not mean they are well-protected; it may just be that this industry has not been a significant target. Cyberattacks and defenses are likely more concentrated on more profitable businesses. While the automotive sector involves a lot of money, it is not necessarily the most profitable. Some companies are more likely to be attacked and perhaps less protected.

How can cybersecurity concerns impact the public's willingness to adopt autonomous cars?

CR: If cybersecurity issues in cars are highlighted too much, people will stop wanting cars with that level of autonomy. Privacy concerns will be significant as people worry about being tracked, their conversations monitored, and their activities observed. There is also the fear of the car breaking down, being rerouted, or causing accidents. To accept higher levels of autonomy, there needs to be a substantial shift in mindset and assurance of security. It may be better not to highlight these issues too much to avoid creating fear. If concerns arise, measures should be in place to address them.

And in terms of mitigation strategies, which do you think are most important to both combat cybersecurity threats and address public concerns about these threats, especially for the future of autonomous vehicles?

CR: Critical strategies include not focusing too much on potential problems without hiding them. Control solutions should provide continuous security checks and alarms. Encryption and security measures are essential to prevent breaches, ensuring no corruption in the connections between the central system and the cars. Securing or creating highly specialized software that is less accessible to the public is important, though it might be more expensive. Standardization of technologies, especially with regulations, is also crucial to ensure different brands' vehicles can communicate and understand each other's actions.

Based on our discussion, do you think cybersecurity concerns are potentially a barrier to

adopting autonomous cars?

CR: The unknown always creates fear. Concerns such as the risk of cars being hijacked or bringing more insecurity can be significant barriers, like the charging time was (and still is) when mentioning electric cars. To gain public acceptance, autonomous cars must offer much more security than they do today. These concerns are a significant barrier to adopting and manufacturing autonomous cars. Therefore, more research is needed to address new challenges. Developing a secure, impenetrable communication network for autonomous cars is crucial. The challenge might be more straightforward than expected, but the unknown can be both a problem and a concern.

.11 Summary of interview 10: FM

In your experience, what are the most recent trends in the auto sector nowadays? If you could rank them from the most to least impactful also.

FM: I mean, definitely AI. In all honesty, I would rate this as the number 2. I would rank autonomous driving as the trend number 3. And most likely, the most significant trend or factor in automotive right now is infotainment. So, anything UI/UX-related that you can experience in the cockpit.

In your experience, what do you think are the most pressing cybersecurity concerns or threats in the auto sector today?

FM: First, there is IP theft, which is not on a car-related level but anything that you might steal from an OEM like Mercedes-Benz, BMW, or Porsche. So, cybersecurity is massive, and hundreds of people are working internally and externally to protect the IP. That is a significant concern. On the car-related level, there have not been too many hacks on individual cars, so this might become more pressing with the broader use of autonomous driving. However, cybersecurity has yet to make a significant impact.

There is a split between the rest of the world and China regarding data privacy. In most countries, data protection on an individual level is critical. However, in China, people are more willing to give up data for good service. So, the importance of data privacy depends on where you are in the world.

How do you perceive the materiality of cybersecurity issues when it comes to public willingness to adopt self-driving cars?

FM: It depends on the region. Studies from McKinsey show that the Chinese are much more willing to adopt new technology with less fear of cybersecurity issues, whereas in Europe and the US, there is more fear. Cybersecurity can be an obstacle for some people in these regions when purchasing an autonomous car, but it is less of a factor in China. Given that China represents a significant portion of the global car market, this difference is essential to consider. So, it is always a matter of China versus the rest of the world, with sometimes conflicting opinions.

Are there any cybersecurity challenges that you believe are unique to the auto sector, especially concerning self-driving technology?

FM: I would say that, as of today, companies invest more in developing autonomous driving systems than cybersecurity. Companies will need to invest more in cybersecurity as we approach the widespread implementation of autonomous driving (around 2026/2027/2028). Right now, the investment focuses more on the development of technology. In the future, cybersecurity will become a more prominent issue, and therefore, cybersecurity investments must grow as the number of autonomous vehicles on the road increases.

How would you rate the current cybersecurity standards in the auto sector on a scale of 1 to 10, specifically in terms of compliance and effectiveness? And how would you assess the readiness of the auto industry to manage cybersecurity concerns, namely associated with self-driving cars, on a scale of 1 to 10?

FM: I would give both a rating of 7 for different reasons. For IP theft, big OEMs are well-prepared and comparable to tech companies, but there is always room for improvement. Autonomous driving and cybersecurity are developing issues that will become more significant in the future. Currently, the protection for the few autonomous vehicles on the road is quite good, but this will need to scale up as more vehicles are deployed. So, while the current readiness is sufficient, the industry must prepare for future challenges.

What mitigation strategies do you think are most critical for countering the cybersecurity threats to self-driving cars?

FM: You would probably have to ask an expert on cybersecurity for detailed strategies. However, continuous security checks, encryption, and secure connections between the central system and the cars are generally essential. As autonomous vehicles increase, more sophisticated security measures will be necessary.

What mitigation strategies do you think are the most critical for countering public opinion

concerns regarding this cybersecurity threat to self-driving cars?

FM: It is all about trust in the end. You give up the steering wheel, and it is not just about cybersecurity; it is about many other factors, such as accidents and how the car behaves. The key is to ensure that, at a very high level of reliability, nothing goes wrong. It is like a good referee in football — if you do not notice them, they are doing a good job. Similarly, autonomous driving should work seamlessly without causing issues. The more cars that work well, the better the public perception will be. So trust is crucial, and it comes from many vehicles working reliably.

Do you feel that cybersecurity concerns can potentially be a major barrier to the adoption of self-driving cars?

FM: No, I do not think so. It is still too early in the process. Right now, the focus is on getting the technology up and running. Cybersecurity is one of the aspects that will become more critical later, but I do not see it as a significant showstopper for the technology at this stage.

.12 Summary of interview 11: LS

What are the most recent trends in the auto sector?

LS: The focus is on low-level automation functionalities such as automatic cruise control, emergency braking, and lane assist. Over-the-air (OTA) updates are increasingly relevant, ensuring vehicles stay updated without service center visits. Multimedia systems in cars are also key, with many companies working on data handling and integration. Lastly, robotaxis are gaining attention, aiming for fully autonomous vehicles providing taxi services without human drivers.

Ordering by impact, would it be the order you mentioned?

LS: Yes, probably in that order. From the OEM perspective, OTA updates might be more relevant, while from the user's perspective, multimedia aspects could be more significant. So, the order is likely low-level automation, OTA updates, in-vehicle multimedia, and robotaxis.

What are the most pressing cybersecurity concerns in the auto sector today? How do they influence consumer decisions about self-driving cars?

LS: The primary concern is data penetration attacks, such as manipulating road markings or attacking vehicle cameras, leading to incorrect interpretations. Another issue is attacks on the vehicle's operation, turning it into a remote-controlled car. These concerns can significantly impact consumer decisions.

Could you rank these concerns in terms of their potential to influence consumer decisions regarding self-driving cars?

LS: The order would be the opposite: first, attacks on vehicle operation, and then data attacks. Actuation concerns are more immediate for consumers as they directly affect vehicle control and safety.

How do you perceive the materiality of cybersecurity issues when it comes to the public's willingness to adopt self-driving cars?

LS: It's about the effect on the user. An autonomous car is like a smartphone with smart functionalities. Accidents resulting from cybersecurity issues will be noticeable to customers and influence their decisions. If an incident happens, it becomes a pivot point for users to decide against adopting the technology. The visibility of these issues, such as news reports on hacking incidents, can significantly sway public opinion.

How do cybersecurity issues in the auto sector compare to those in other industries in terms of complexity and urgency?

LS: Low-level automation functionalities are similar to those of consumer electronics, such as smartphones. However, many vehicle components might not be as rigorously tested for cybersecurity. Specialized attacks can exploit communication protocols, affecting multiple systems. Higher levels of autonomy will pose unique challenges, requiring vehicle actions to be explainable and creating a significant grey area in cybersecurity.

Could you rate the current cybersecurity standards in the automotive sector on a scale of 1-10 in terms of compliance and effectiveness?

LS: I would estimate a 6 out of 10. We adhere to development guidelines and programming standards, especially in critical systems. However, there is room for improvement in cybersecurity readiness and adherence to guidelines. Industry-wide collaboration and more stringent regulations could help enhance these standards.

On a scale of 1 to 10, how would you assess the auto industry's readiness to manage cybersecurity risks for self-driving cars?

LS: It varies by brand. Tesla, for example, uses OTA updates extensively. Overall, the automotive sector is behind, and I would rate it a 5. More recent vehicles show improvement, but the industry still has a long way to go. Consistent updates and proactive measures are essential for

improving readiness.

What mitigation strategies are most critical for countering cybersecurity threats to self-driving cars?

LS: Rapid response and highly advanced support infrastructure with 99.9% uptime are critical. As already mentioned, development guidelines and test-driven development are essential, ensuring continuous testing and secure system functionality. Ensuring the infrastructure is state-of-the-art and reliable is also paramount for maintaining security.

What mitigation strategies are most critical for countering public opinion concerns regarding cybersecurity threats to self-driving cars?

LS: Effective marketing is key. Tesla, for example, benefits from the personality cult around Elon Musk, which helps its marketing. Proving safety through clear communication and quick responses to problems is essential. For instance, demonstrating safety effectively through real-world testing and transparent communication can address public concerns.

Do you feel cybersecurity concerns are currently a major barrier to the adoption of self-driving cars?

LS: Yes, it is a concern, but manageable. A major incident, like a fleet halt or an accident, would be a clear signal for the public to be cautious. However, gradually introducing autonomous functionalities is the right approach. It allows us to address cybersecurity issues progressively, making the transition smoother and safer. While a concern, it can be managed over time, ensuring a safer adoption of self-driving cars. Building public trust through continuous improvements and transparent practices is essential for the successful adoption of this technology.

.13 Summary of interview 12: JS

What are the most recent trends in the auto sector?

JS: Currently, software-defined vehicles are highly popular, with numerous companies proposing solutions. Mixed criticality, running both critical and non-critical software on the same hardware, is gaining interest. Cybersecurity remains significant, especially with UNECE regulations R.155 and R.156 prompting manufacturers to prioritize it. Other prominent topics include telematics, cloud processing, edge processing, and generative AI. Additionally, new interaction methods with vehicles, such as V2X mobility, are crucial for addressing autonomous vehicle challenges.

Ordering by impact, would it be the order you mentioned?

JS: From a technical perspective, mixed-criticality is very important. Software-defined vehicles will likely be crucial for consumers, allowing for feature upgrades like smartphones. V2X and supporting infrastructure are essential for full autonomy and mobility, enhancing safety and traffic management. So, mixed-criticality, software-defined vehicles, and V2X infrastructure are the most impactful issues.

What are the most pressing cybersecurity concerns in the auto sector today?

JS: The massive exploitation of vulnerabilities is a major concern. If a vulnerability is found, it could allow control of an entire fleet of vehicles, turning them into weapons. Data privacy and security are also critical, especially with more cameras inside vehicles. These concerns can significantly impact consumer decisions.

Could you rank these concerns in terms of their potential to influence consumer decisions regarding self-driving cars?

JS: The massive exploitation of vulnerabilities is the most important issue to address. My focus is on protecting human life, so this is my top concern. Data privacy and security are also important but come second to preventing large-scale vehicle control.

How do you perceive the materiality of cybersecurity issues when it comes to the public's willingness to adopt autonomous cars?

JS: Generally, I don't think cybersecurity will be a major concern for consumers. People trust smartphones with personal data, so they might view autonomous cars similarly. If incidents involving human lives occur, there might be hesitation, but overall, urban adoption of autonomous cars will likely be positive.

Are there cybersecurity challenges that you believe are unique to the auto sector, especially concerning self-driving technology?

JS: Autonomous driving technology is relevant across sectors, including railways and aeronautics. Vehicles, however, are "unstructured assets" operating in uncontrolled environments, presenting unique challenges. Core cybersecurity issues are similar across sectors, but vehicle-specific challenges require tailored solutions.

Could you rate the current cybersecurity standards in the automotive sector on a scale of 1-10 in terms of compliance and effectiveness?

JS: Compliance is generally satisfactory, especially among premium OEMs. However, effectiveness is relatively low due to the sector's focus on safety-critical aspects, hindering quick changes. Overall, I would rate the automotive sector around a 5 out of 10, with more progress needed in responding to issues.

On a scale of 1 to 10, how would you assess the auto industry's readiness to manage cybersecurity risks for self-driving cars?

JS: Readiness varies. During development, readiness to consider cybersecurity risks is around a 3 or 4. For incident response, readiness is significantly higher, around an 8 or 9, due to active industry efforts, information sharing, and extensive research. By the time fully autonomous vehicles are common, readiness should be robust.

What mitigation strategies are most critical for countering cybersecurity threats to self-driving cars?

JS: Key strategies include recognizing and responding to normal and abnormal behaviors and creating randomness in memory locations to counter exploits. Fail-safes and behavior-driven modes are essential to prevent systems from operating with too much autonomy. Ensuring robust infrastructure and adhering to strict development guidelines are also crucial.

What mitigation strategies are most critical for countering public opinion concerns regarding cybersecurity threats to self-driving cars?

JS: Certification efforts provide a trusted seal of quality. People rely on certifications like the Euro NCAP safety ratings and the CE mark. The European Union and the US are developing cybersecurity certification marks, helping reassure the public that autonomous vehicles meet necessary standards and addressing their concerns effectively. These efforts will be critical in building consumer confidence.

Based on our discussion, do you feel that cybersecurity concerns are currently a major barrier to the adoption of self-driving cars?

JS: Not until a major problem occurs. There will always be early adopters, and technology is highly valued. Trust in brands will play a crucial role, as some brands will inspire more confidence in cybersecurity, contributing to their overall perception of reliability. Cybersecurity will be a factor in reliability rather than a direct barrier to adoption. As the industry matures, it will increasingly emphasize the importance of cybersecurity in its marketing and consumer education efforts.