

Charles University

Faculty of Social Sciences

Institute of Political Studies

Diploma Thesis



Bc. Jan Balaš

Next Generation Mobility Ecosystem: New Security Challenges Within Cyberspace

Praha 2022

Supervisor: doc. PhDr. Vít Štrátecký, M.Phil., Ph.D.

Declaration

I declare that I have prepared the diploma thesis independently, that I have duly cited all the sources and literature used and that the thesis was not used in another university study or to obtain another or the same title.

Prague, 29th January 2022

Jan Balaš

Key words:

Car security, Cybersecurity, New mobility

Word Count:

110 278

Abstract

This paper aims to introduce the topic of cybersecurity in automotive as another domain within the connected world. However, it does not go into technical details. It is rather a guide for the wider audience, and for those who would like to build on this topic in the future and need something to start with. For this reason, it looks for both the similarities and specifics with other domains. By finding common characteristics within the connected world, the reader is then able to classify the topic of cybersecurity in automotive. The main goal, however, is to find the specifics. After the introduction and explanation of the general terms, parameters and phenomena specific for automotive are then highlighted. The main parameters, on which the similarities and specifics are shown, are data problematics and cooperation between public and private actors. As a measure of success of this paper will be the ability of the reader, after reading the whole paper, to describe what are the current challenges in automotive cybersecurity and understand its importance of securing it in the future.

TABLE OF CONTENTS

1	INTRODUCTION	1
2	CONNECTED WORLD	3
2.1	INTERNET OF THINGS	4
2.2	VALUE OF OUR DATA	5
2.3	BUSINESS AND POLITICAL PURPOSES	7
3	CYBER SECURITY IN THE CONNECTED WORLD	9
3.1	ATTACK VECTORS: TYPOLOGY OF CYBERATTACKS	10
3.2	STATE OR PRIVATE ACTOR? (PUBLIC-PRIVATE PARTNERSHIPS)	14
3.2.1	<i>Communication and Cooperation Aspect</i>	<i>18</i>
4	CYBER SECURITY IN THE AUTOMOTIVE WORLD	20
4.1	NEXT GENERATION MOBILITY	20
4.2	CONNECTED VEHICLES	22
4.3	SPECIFICS OF THE AUTOMOTIVE WORLD	26
4.3.1	<i>Data Driven Specifics</i>	<i>27</i>
4.3.2	<i>PPP in the Automotive World</i>	<i>28</i>
4.3.3	<i>UNECE</i>	<i>29</i>
5	THE VIEW FROM ŠKODA AUTO PERSPECTIVE	32
5.1	ŠKODA AUTO: BRIEF INTRODUCTION	32
5.2	MAIN CYBERSECURITY OBJECTIVES ACCORDING TO ŠKODA AUTO	32
5.3	INTERNALS OF ŠKODA AUTO: A HANDS-ON APPROACH	38
5.3.1	<i>Key Fob Vulnerability</i>	<i>38</i>
5.3.2	<i>Infotainment Vulnerability</i>	<i>39</i>
6	CONCLUSION	40
7	BIBLIOGRAPHY:	43
8	LIST OF ABBREVIATIONS:	46
9	LIST OF FIGURES:	46

Preface

Connected world, internet of things, cybersecurity, software, hackers. Those are some words, chosen from many, which pop up when you would ask me to describe the world, we are now living in. I decided to work in this field and do research, starting with this thesis. I believe that cybersecurity in automotive is an important topic as more cars on our roads are connected, which also means vulnerable to cyber-attacks. The paper aims to walk the reader throughout the respective chapters by explaining the cybersecurity topic. Firstly, a brief introduction will be performed by explaining the basics of the connected world and cyberspace. For this reason, publications describing general terms and conditions will be used. As the paper will continue, so will the text become gradually more detailed. In the second half of the thesis, mainly official guidelines and standards (UNECE, Škoda Auto, ENISA, NUKIB) will be used. As the topic of cybersecurity in automotive is still new, one of the main goals of the thesis is to maintain the attention of readers throughout the whole paper to ensure a sufficient level of comprehension of the text.

1 Introduction

“The future is now, and it means that you don’t build cars per se, you create systems and build the rest around it. The car needs to take you home and stop by your favorite restaurant without you even physically paying, you just take the food and go.” (Mr. Ondřej Černý, Škoda Auto [oral interview], November 2021). Infotainment will be the most important part of the car for the customers if it is not a reality already in some parts of the world. The mobility ecosystem is evolving faster than ever. Automakers, but most importantly customers seem not to focus on the technical details of their vehicle in the first place, but on the quality and convenience of its systems. Automakers are racing in providing better and faster services, which require more control units, computer chips and in general more data from the people. However, with its rapid development comes the other side of the coin, which is the cybersecurity topic.

This thesis aims to present the cybersecurity topic to a wider audience with its focus on the automotive world. It is not then designed to technically oriented people, who might find some of the statements vague or incomplete. As it is written within Political Science Studies at Charles University, for more convenience for the readers, a rather narrative than descriptive approach will be used. For this purpose, the thesis will not go into technical details to maintain coherence and readability. Complex and difficult sections of the paper will be mostly explained by giving examples and by providing pictures and summarized tables. There is a lot of shortcuts in the text, which requires the reader to carefully follow them throughout the paper, or to use “*8 List of Abbreviations*”. In general, the thesis aims to present a new topic, which is on the edge of scope of Security Studies at Charles University. Therefore, a coherently and clearly written text is vital to ensure correct understanding of the problematic.

The topic of vehicle cybersecurity is relatively new but belongs to one of the most important issues within cybersecurity that our generation and most likely even the next generations will face. The reason behind its importance is that cars are just another domain which belongs to the instruments of the so-called connected world. The era of smart technologies makes our lives easier, faster, funnier and in general more convenient. We as users are giving away data about ourselves so we feed the algorithms and thus consequently improve these “smart helpers”.

The focus on automotive is not random. Most of us have noticed how fast the automotive world is changing. Combustion engines are slowly leaving us (especially in Europe) and electricity as a fuel for our engines comes with great glory. Equipment such as collision warning, lane assist, vehicle to vehicle communication, vehicle to infrastructure communication, automatic emergency braking and others seem to pave the road for another level of a driver's convenience, and it is the phenomenon of autonomous vehicles. Autonomous vehicles and intelligent transport systems, at the time of writing the thesis (2022), are still some years away from a massive penetration to our roads, but they deserve a certain level of pre-evaluation in this paper too. The future trend is becoming obvious, our cars (and other things around us) will get smarter and more convenient in exchange for our data and the ever-increasing cyber risks, which go along with the development. To sum up, the main question that this thesis asks is, where does the automotive world stand within the framework of the connected world and cybersecurity. What are the similarities and what are the specifics of this domain? Cybersecurity in the automotive is an unexplored territory, especially within the field of security studies. That is the main reason why it deserves a broad and understandable explanation, so the other scholars can build upon it and answer further questions that this topic will bring in the future.

The paper is divided into 4 main chapters. The first chapter called "Connected world" is the gate to the whole problematics. A vehicle is just another domain in the connected world. Together with mobile phones, laptops, smart watches and other devices share similar vulnerabilities and challenges. That is why it is important to put it in the big picture and introduce the connected devices as one big ecosystem with its characteristics. This chapter will, apart from introducing the "connected world" topic, give the audience a grip over why this topic is important, what are the pros and cons of being connected and the value of our data.

The second chapter called "Cyber security in the Connected World" looks in more detail into the issue of securing connected devices. Here the reader will find answers to questions like, how can we secure our systems, what are the attack vectors, possible entry points, or what instruments do the attackers use when trying to hack a device. Lastly, a private-public partnership debate will be introduced. Here, the problem of communication and cooperation between private and public actors will be touched.

“Cybersecurity in the Automotive World” jumps straight into the problematics of connected cars, intelligent transport systems and autonomous vehicles. The most important part of this chapter will be to make the audience clear about the specifics of this domain. The main focus will be on the data issues, public-private partnership in the automotive and cybersecurity regulations which concern the automakers.

In the last chapter called “The View from Škoda Auto Perspective” the approach of Škoda Auto and its cyber security practices will be introduced. Theorization of cybersecurity topics is important, so we are able to see it in wider picture, but praxis is what makes it interesting. We will learn about the strategies, processes but also about the challenges that Škoda Auto has to face. The aim of this chapter is to peek under the hood of the cybersecurity automotive world and see a real-life example of issues, challenges, prospects and procedures exercised by the biggest Czech vehicle manufacturer.

2 Connected World

If we would go back in time (related to western countries 10 years and more) we would talk about computer criminality, computer security, or computer attacks. Today we use the prefix “cyber” instead. It is true, that back then the main instrument for entering cyberspace¹ were computers. Now we have many instruments to enter it: mobile phones, watches, tablets, televisions, but also washing machines, refrigerators, or thermostats. Basically, anything that can communicate through TCP/IP² or other protocols with other devices is a cyberspace apparatus. For most of us, these are well known as smart devices (Smejkal 2018, p. 19). Our lives have been rapidly changed by the connectivity opportunities which were designed for our convenience. For us, who are living in the modern world, smart devices became an integral part of our everyday life. If it is just reading news on our mobile phones, searching for goods in e-shops, chatting with our friends, video-calling with our colleagues, or measuring bodily functions, we all are more or less connected, even if we realize it or not (NHTSA 2015, p. 1).

¹ Cyberspace is a virtual reality which has no end or beginning and is dependent on material technological devices

² TCP/IP is a set of communication protocols used to communicate within the internet network

For cyberspace is typical interaction, globality and data sharing. The modern trend forces us to connect from anywhere to whatever place with/through whichever instrument. This urge to be connected was, without doubt, accelerated with the covid19 pandemic, which forced us to stay at home and thus consequently spend more time on our devices to stay in touch with our friends, but sometimes also to be able to order necessary goods for our survival. Another consequence of the pandemic was that many people had to work from home. Many companies and institutions like universities admirably managed to overcome these difficulties through various means that enabled the employees/students to stay in touch with their colleagues and superiors and to be able to finish their tasks in general. And it works vice versa as well, more people nowadays are bringing their own laptops or mobile phones to company information systems, which brings its own sort of convenience, such as bigger flexibility but also challenges and threats, such as data breaches and difficult implementation of company security measures. This phenomenon is called “BYOD” (Bring Your Own Device), and is an integral part of another phenomenon, which will be introduced in the next subchapter – the internet of things (Smejkal 2018, p. 19).

2.1 Internet of Things

Internet of things (IoT) is a term that most of us came across with. The term IoT is frequently used rather recently, however, it has been with us for more than 20 years, when it was introduced by the Massachusetts Institute of Technology describing radio frequency identification infrastructures (Wortmann and Flüchter 2015, p. 221). Currently, the IoT is being related to every day physical things using an electronic device. An admirable technological development enabled us to make those electronic devices smaller, but most importantly cost-effective for commercial use. As the internet itself developed from being used only by a few IT experts to billions of users nowadays, internet embedded into various things is showing a rapid growth in commercial usage as well. Connecting the physical world with the information world through everyday objects is an enticing tool that offers many opportunities and is becoming available to a broader scale of people (Kopetz 2011, p. 308).

We can visualize the internet of things as a network which consists of objects that are equipped with their own systems. These systems, or let us say an intelligence,

allows them to communicate with other objects that are embedded with their own intelligence, but also with human beings, or clouds/backends³ (Xia, et al 2012, p. 1101). To be precise, let us firstly imagine “the thing”, for example a watch that is the core hardware⁴ component. If we want it to be called a smart watch and not just a casual watch, we will then need to accompany it with sensors, which will allow the connectivity. The connectivity has to be operated and managed. For this purpose, we will need a device software. After we put these things together, we have our watch ready to get connected with a compatible friendly object. To tell us if our watch and the other object are compatible together, we need a protocol. The protocol is a form of communication that the device’s libraries use to talk to each other to verify themselves. When our watch communicates, we are halfway there, we just need to be able to read the information that is being communicated. For this, we need an application to be developed, which will show us the information in the desired form. If it is an application in a watch, a mobile phone, or a screen in your car, we usually talk about frontend (the things we can see). However, we can communicate also with backend (the things we cannot see). Let us imagine it as a cloud or any data storage, where the data from our watch are stored (steps, sleeping schedule, heart rate, etc.). This communication between backend (data storage) and frontend (application on our watch) enables us to be a part of the connected world (Wortmann and Flüchter 2015, p. 223).

For better illustration, please see an animated example of a smart device (in this case a smart home) from 2001, given in a humorous way: *The Simpsons. Treehouse of Horror XII* (7:25 – 14:43), or a shorter version (0:48 – 3:30).

available at: <https://www.youtube.com/watch?v=PjILhU4RtKc>

2.2 Value of Our Data

A connected world is a space for data sharing, but also for data acquisition. Data about a targeted person or a group of people, such as GPS location, information about assets, property, favorite places, or shopping preferences are called personal data (Smejkal 2018, p. 230). This kind of personal information has a special place within

³ Clouds/backends are mainly used for data management and are not directly accessible by the users

⁴ Hardware x software - what I can touch (solid components) x what I cannot touch (programs)

other data because they are closely related to a specific person and its protection is granted in most democratic countries as one of the fundamental rights (Ibid, p. 238). There are multiple reasons for this protection, starting with the philosophical claim that humans are not just numbers, however, we have other aspects too. The acquisition and potentially the manipulation of our personal data could be (mis)used by others for achieving their political, economic, or other goals, especially when the acquirer would use only a particular section of the personal data. Such data, or fractions of them (once acquired) can be arbitrarily stored, shared or combined as the person or the system wants (Ibid, p. 239).

Our data can be easily used for both good and ill purposes. There are some clear examples of good and ill usage. As for good, we could point to the improvement of algorithms on our smart watch, thanks to them the applications on it run faster and are tailored to our needs and preferences. As for ill usage, we can imagine an identity theft used for payments, fake profiles, or a resale to a third party. In other cases of personal data acquisition and usage, it is not that crystal clear. There are some grey areas where ethics, legislation and attribution issues meet. Especially due to legislation and attribution shortcomings, cybersecurity is sometimes called a new wild west and is one of the biggest challenges for policy makers to set the boundaries and differentiate what is allowed and what is not. This discussion is, without doubt, very important, but also complicated and would require a bigger part than just a chapter. For more information on this topic, please see for example:

THE ECONOMIST. America Rethinks its strategy in the Wild West of cyberspace. The Economist, 2020.

Available here

or ZWITTER, Andrej. Big data ethics. Big Data & Society, 2014.

Available here

For ill or good, data can be gathered from one or many sources. “In the IoT workload, for example, data is ingested from thousands of different data sources at once.” (Meehan et al 2017, p. 4). The data collector then sorts and distributes them accordingly with the help of libraries, which send the right messages to other systems to cooperate. We can imagine those messages in a simple way like: “store this data into data storage”, “check if this system is compatible”, or “run this process again”

and many others. Once the data is collected and labeled correctly, it needs to be stored in backends/clouds for further usage (Ibid, p. 5). Every piece of data is making the whole system faster and smarter. We could call the system of processes an algorithm.

Algorithms play a crucial role in our lives. Even our brains are guided by algorithms to solve everyday situations. Moreover, they also help us in cyberspace. They help us to separate what is and what is not relevant for us, and to find our preferences by navigating through massive databases full of information. We can imagine them as search engines that, within a second, find the particular article (among million others) that we wanted to read, or “robots” that are highlighting relevant content on social platforms and hiding the other content, that we would most likely consider boring or not interesting. Or to put it into the technical language: algorithms are procedures that transform input data into the desired output, based on relevant calculations (Gillespie 2014, p. 1-2). The algorithms that can help us the most and have the biggest impact on our everyday life are those based on our personal data, which are composed of our activities, preferences, favorite locations and expressions. The more info about ourselves we give to them, the better they are at selecting what is “the best for us” from huge data corpuses. And our mobile phones, smart watches, connected cars, the internet and other electronic devices are generating data every day. Every time we use one of the before mentioned gadgets, we “throw away” our personal data, leaving traces of our lives (Becerril 2018, p. 72).

2.3 Business and Political Purposes

In the previous chapters we introduced the topic of the connected world, devices within them and data, which drive the whole system. By reading those chapters, one might assume that the connected world serves mainly us (the general public) to make our lives more convenient. However, the connected world offers its services also to the world of business and politics. As for the business world, data is “the new oil” for the companies (Carruthers and Jackson 2019, p. 10). This refers to the importance of targeting your marketing policy to a particular group of potential customers, analyzing the efficiency of processes, employees and policies that the company carries out. Another benefit is that the companies are able to compare their performance levels with the concurrence or with the national/international standards that the company wants to meet or even outdo. Data became a fundamental part of

every company and the ability to read them and work with them properly is a decisive variable in the world of business, full of competitive companies.

This process is known as “data-driven business transformation”. For some organizations, this process has to start from the very beginning of the organization’s life, these are called data-driven organizations. For instance, Bolt, Skyscanner, Airbnb or any organization that compares costs for insurance, housing, car rental or flight tickets, are based on the data they have to gather. The more data they gather the more fortune these companies can make just by making these data available for the consumers. The rest is called data-enabled organizations. These companies would not inherently need to gather a big amount of data for their survival, however, by using them, they can better utilize their assets to achieve the company goals (Ibid, p. 11). The more advanced this utilization is, the more efficient and sensible the further steps of the company will be in the future. This transformation of the business world is inevitable and is well reflected by the number of companies that help other businesses to achieve their goals by showing them how to gather and work with their data properly. The benefits are numberless: “improved efficiency and productivity, faster and more effective decision-making, better financial performance, competitive advantage, improved customer experience, improved customer acquisition and retention, and identification and creation of new revenue streams” (FinancesOnline 2021). According to analytics company MicroStrategy, 59% of organizations around the world use big data analytics (Borba 2020, p. 21).

Now let us move from the private sphere to the public one. On the (geo)political level, one of the biggest advantages of available data and the connected world, in general, is the freedom of speech and the possibility to read uncensored articles even in subversive countries like China, Iran, or Russia. This advantage is widely used by the dissent in such countries. Nevertheless, even in the Western world, which we deem to consider as uncensored, when a media platform would start falling into censorship or disinformation, the internet usually steps in. This almost limitless freedom of speech is, however, a double-edged sword. On one hand, the dissent is able to read pro-democratic material from all around the world, on the other hand, it is a hub for terrorists and other malign actors too. Potential terrorists can use encrypted communication channels, lure new members or read instructions on how to assemble a bomb (Simcox 2020, p. 2). Recently, we witnessed how powerful these

tools can be when falling into wrong hands. Islamic State (IS) used social media to spread fear among the enemies by showing videos, where the IS followers are decapitating war prisoners or showing shelves full of fruit and other commercial goods to demonstrate how wealthy the potential follower would become to lure them (Střítecký and Špelda 2017, p. 68-69).

As it was outlined, the connected world is a space full of opportunities. It makes our lives easier and more fun, helps businesses to grow and oppressed groups to express their ideas and beliefs. However, it is also a space for harmful groups or individuals to perform their activities. It also raises concerns about data privacy and possible misuse of it. The list of threats and opportunities that the connected world can bring to us would be endless. In general, with great power comes great responsibility - in this case the responsibility to mitigate the threats and harmfulness of the connected world. This fate carries one of the fastest growing industries nowadays – *The Cybersecurity*.

3 Cyber Security in the Connected World

“The release of atomic energy has not created a new problem. It has merely made more urgent the necessity of solving an existing one”. At the first glance, this quote from Albert Einstein has nothing to do with cybersecurity. However, it refers to a problem of understanding what cybersecurity is. Basically, the problem lies in understanding cybersecurity as something new but at the same time applying the old security rules and measures and solving ever existing problems disguised under a new coat. Problems such as personal responsibility for private data, OEM⁵'s responsibility for quality products, or ignorance of the rules (of cyberspace) in general have been with us longer than when the term “cyberspace” was firstly released by William Gibson in 1982, and even way longer back (Kolouch et al 2019, p. 35-39).

The years 2020, 2021 and beginning of 2022 highlighted the importance of cybersecurity through various instances. Covid19 and the subsequent lockdowns showed our dependance on smart devices and the Russian-Ukrainian conflict raised the awareness of cyberattacks as the mass media started to inform about it more often

⁵ Original equipment manufacturer

(Anonymous, Russian state-supported hacker groups, Wiper virus⁶). Národní úřad pro kybernetickou a informační bezpečnost (NUKIB)⁷ released its annual document with cybersecurity statistics and trends stating that in the Czech Republic, there was an increase from 217 reported incidents in 2019 to 468 incidents in 2020. As for the example, Czech citizens will most likely remember the attacks on the hospital in Brno (Fakultní Nemocnice Brno) or the psychiatric hospital in Kosmonosy (Psychiatrická nemocnice Kosmonosy (NUKIB 2020, p. 3). In 2022, national (cybersecurity) agencies reported a growing number of attempts to scan ports of governmental organizations and critical infrastructure. It has been assumed that this could have a connection to the Ukrainian crisis, where the attackers are preparing the ground for cyberattacks. Many agencies report about the increasing number of cyberespionages, DDoS⁸ and ransomware attacks and warn about the possibility for targeted attacks designed for Ukrainian targets such as *wiper*, to spill over to other countries as well (NUKIB 2022 Varování, p. 1-2) and (NUKIB 2022 Upozornění).

3.1 Attack Vectors: Typology of Cyberattacks

According to Webster's dictionary, cybersecurity is a set of measures that protect computer systems from an unauthorized access, or attacks. From the previous chapters we know that "cyber" does not concern only computers and so it is in cybersecurity as well. The platforms for possible attacks and the attacks themselves are way more diverse (Kolouch et al 2019, p. 42-43). For better understanding of what falls under cybersecurity, we need to know its three basic elements, which are people, technologies and processes (Ibid, p. 57). **People** mentioned first is not a coincidence. Even when you would have perfectly secured systems from the technical point of view, you cannot secure the behavior of people within the connected world. That is why many attack vectors try to use the vulnerability of people's minds. One good example are the attacks aiming at users of internet banking.

⁶ Malware attack erasing (wiping) data from targeted device

⁷ National Cyber and Information Security Office – Czech institution dealing with cyber Security topics and others related to cyberworld.

⁸ Distributed denial of service attack: an attack when a target is shutted down by receiving too many commands (example could be too much visits to a targeted website during a limited amount of time)

1. *Phishing*: The attacker is sending emails, which are masked as official emails from the bank. Such an email usually requires you to fill in your details like the PIN code of your credit card, passwords or any other safety data that could help the attacker to gain access to your money. Some emails, especially those from the past, were usually easy to uncover because of their weak language and phrases. Modern phishing emails, on the other hand, are of a high-level quality of language but also graphic design that more or less matches the official emails sent by the bank. The sad truth is that some people fall even into those less sophisticated, sometimes even banal attempts.
2. *Pharming*: Here the attacker uses malicious programs that infect your device. These programs are then able to redirect you from the official website of the bank to a fake one, which can be 100% unrecognizable for the ordinary user. The user then fills in the required data thinking that it is the official login portal, but in fact he gives away his personal data and consequently loses his money.
3. *Skimming*: Copying your credit card using a special copying device (usually installed on/in an ATM).
4. *Vishing*: Similar to phishing attacks but using phone calls with automatically generated or authentic voices to fake you into thinking you are talking to your bank consultant or a relative. Similar to phishing and vishing attacks are *smishing* attacks, the only difference is that the attacker uses SMS messages. The aim is again to force you to give away your personal data.

There are other existing variants such as trashing, bailing or wangiri, but the main 4 should be enough for the sake of illustration (Smejkal 2018, p. 191-192). Cyberattacks aiming at people are so popular, because usually it is easier to hack a person than to hack a system. Moreover, to send a phishing email does not require you to have expert IT knowledge and it does not take that much effort. Plus, the attacker can purely use his creativity, which is endless like the naivety and ignorance of the ordinary users (NUKIB 2022, Strategické organizace, p. 3).

The other element within cybersecurity is **technology**. Here we can imagine any device that serves as the instrument to enter the connected world (PC, mobile phone, or the smart watch mentioned in the previous chapters) but also services,

applications, or network providers (WiFi, Cellular⁹, LAN¹⁰). When we talk about securing the technology, we usually mean the proper development of the device and its components, plus securing the quality of it during the whole lifecycle of the device. When we say a proper development and securing the quality, we mean a set of given procedures that are following requirements, usually set by an authority (laws, norms, regulations). These procedures are executed through for instance:

1. Detection systems and threat platforms, which detect any deviations from the standard.
2. Protection against malicious programs and codes (firewalls, antivirus and antispam programs).
3. Technologies monitoring activities of the ICT¹¹ elements and users (Kolouch et al 2019, p. 60).

There are many other tools to ensure a healthy and secure environment for your devices. Nevertheless, these measures alone are not enough. To make the full circle, we need to focus on the third element of cybersecurity as well, which are the processes. Processes are activities or operations, which the respective person or a company has to apply, so the users can safely use the technology (devices). These operations are numerous, and each user or producer chooses which operations are most suitable and/or cost-effective.

For better illustration, the examples could be:

1. Asset and risk management
2. Authorization and authentication
3. Corrective actions analysis
4. Penetration tests
5. Internal and external audits
6. Cybersecurity trainings (Kolouch et al 2019, p. 61-62).

⁹ Cell radio network

¹⁰ Local Area Network

¹¹ Information and communication technologies

If we introduced examples of attacks aiming at people, we should reveal attacks aiming directly at the ICT devices as well. These attacks do not aim to use the vulnerabilities of people's minds but the vulnerabilities of the attack surfaces of the ICT systems. Before breaking down the kinds of threats on ICT systems, we have to mention that there are numerous kinds of attacks depending on the effort, or the goal of the attacks (money, data, control of the device, espionage), but also according to the level of expertise or equipment which is needed to break in, and whether it concerns critical infrastructure, personal data, hate speech, child pornography, or others (Kim, K. et al. 2021, p. 5-6). There would not be enough space in the whole thesis to explain and typologize them all. For the purpose of better understanding the cybersecurity topic in general and then cybersecurity in automotive, only some attack vectors have been chosen, which are more common than the others, especially in the automotive world:

Advanced Persistent Threat (APT) – an attack aiming to stay undiscovered for a longer period of time, usually to mine data.

Denial of Service attack (DoS, Distributed Denial of Service attack (DDoS), Jamming interference (Wireless Denial of Service WDoS) – kinds of attacks whose aim is to shut down or at least disrupt the functionality of the targeted device.

Malware (Virus, Worm, Trojan horse) – programs causing malicious (unwanted) actions.

Ransomware – type of a malware that the attacker uses to block/shut down a device and then ask for a ransom to repair it.

Spyware – a type of malware used to spy on people or devices.

Man-in-the-middle attack (MITM) – a situation when an attacker position himself in the middle of two endpoints (user, application) to read or alter the communication.

Zero-day Exploit – a kind of an attack using the new/unknown vulnerabilities (newly released software, actualization) (ENISA, Threat Landscape, 2021, p. 18).

It is worth noting that even when we would have secured all of the three elements, that does not mean that our systems are 100% secure. Absolute cybersecurity is the holy grail that is, at least for now, an utopia to achieve. Cybersecurity is a very complex set of procedures that differentiate according to desired functions that the system should produce. Not all systems require the same level of security, naturally, some targets are more interesting for the attackers (data or monetary-wise) than the others. As the processes of securing our assets against cyber-attacks are so complex, so are the philosophical approaches on how to do it right. One of the questions that the cybersecurity experts have to face is the discussion, of whether a state or a private actor should be responsible for the protection of people and property in the connected world (Dr. Miriam Dunn Cavelty, Cybersecurity expert [oral interview], January 2022).

3.2 State or Private Actor? (Public-Private Partnerships)

State or private actor? This debate started mainly in the 80s and early 90s with the spread of communication technologies during the so-called information revolution. Back then and even earlier, the network of communication technologies consisted primarily of the government-controlled ones. This started to change in the 80s and 90s as a larger part of the network began to belong to private companies (Burgess 2010, p. 159). Nowadays, the private sector is considered a key stakeholder. That is mainly due to the fact that it controls a big part of the infrastructure (cables, transmitters, amplifiers, microcontrollers, electronic control units and other hardware components, together with the software they develop). Even the final products are assembled and then sold by private companies (Farrand and Carrapico 2018, p. 6). This fact was reflected by the authorities and the trend in the last century was to de-bureaucratize the public services and promote privatization (Cavelty and Suter 2009, p. 180). The shift was somehow natural, on one hand, the state is considered the main security provider in the eyes of the public, and states are usually not retreating from this position. On the other hand, shifting some responsibilities to the private sector seemed like the right approach, as the private sector had the biggest operative capacities.

This shift prepared the ground for the so-called public-private partnerships (PPP). PPP is a neo-liberal concept applied mainly in the 90s in the US. PPP was

used as an instrument to outsource public services from the state to private companies in order to help to secure the critical infrastructure (Cavelty and Suter, p. 180). Critical infrastructure protection (CIP) is a key topic in developed countries. Critical infrastructure can mean any major communication or control systems, whose disruptions could mean major economic consequences by damaging property or endangering human safety (Bossong 2017, p. 53). An example of critical infrastructure is the energy sector (electricity generation plants, pipelines), manufacturing facilities or transportation systems. Within the critical infrastructure, the whole problematics of the PPP are very well noticeable. To take the energy sector as an example, any disruptions of energy supply or nuclear plant accidents would be attributed to the state. Nevertheless, their embedded systems, microchips, software, and smart grid management are usually in the hands of private companies (Dr. Miriam Dunn Cavelty, Cybersecurity expert [oral interview], January 2022). With globalization and interconnectivity, such disruptions or incidents have a cross-border character, which puts even more importance on building robust and cybersecure ICT networks. The trend of the recent and the upcoming years is making these challenges even more urgent. Improved operations and services in the ever-growing networks increase the attack surface, threat landscape, but also the motivation of attackers to penetrate the systems and then shut it off or to demand ransom for leaving them (ENISA, Critical Infrastructures and Services).

It is clear that both the private and public sectors have to work together and cooperate in order to mitigate the threats. It is not a question of if, but rather how to make the cooperation work. As it was mentioned earlier, this concept is called a public-private partnership. However, as one can imagine, such collaboration is not always perfect. As the PPP evolved, it started to become heterogeneous as it included health, education, art, and other industries which did not necessarily share the same fears and goals and thus consequently created an environment where it was impossible to make clear and unified policies. The whole PPP evolved into an environment full of contracts signed between individual actors, which ensured bilateral cooperation. This heterogeneous environment is also supported by the fact that private and public actors do not always share their goals, thus making the eventual cooperation and trouble-shooting problematic. In cybersecurity, like in other industries, it is important to have a clear policy that all the actors follow. That

is not always possible because of the nature of the business environment. Firstly, it is the state and its legislature who create laws, rules and policies to increase (cyber)security. However, for private companies, these laws, rules and policies are embodied or at least considered as limitations and restrictions which are reducing the potential monetary gains (ENISA 2011 Desktop Research, p. 38).

According to Myriam Dunn-Cavelty and Manuel Sutter in their article “*Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection*”, the main limitation of the PPP lies in 5 problems. Firstly, the problem of establishing a relevant information-sharing model. This is one of the most mentioned issues because the state has limited instruments on how to monitor whether the private actors share all information and if they do, it is difficult to prove that the character and amount of information are sufficient for common troubleshooting. Second, public and private sector cooperation is endangered by different interests. Naturally, both private and state sectors have different backgrounds and cannot fully understand each other’s initiatives and perspectives. This lack of understanding leads to major limits in the cooperation network. Third, because of the state’s capacities, PPP can only work when the state is in direct contact with a limited number of enterprises (usually the big ones). When we talk about cybersecurity, it is important to secure the whole supply chain, not only the end of it. To understand this point, imagine again our smart watch. It is not enough to work together only with the company, which assembles the watch but also with tier-1, tier-2 and other (sub)suppliers, which develop the software and control units for the final product. When there is an issue in just one line of code in software, it creates vulnerabilities for the whole device. When we would use the example of critical infrastructure, let us pick a hypothetical fully automated buses that use artificial intelligence to navigate themselves. It is not enough to secure only the buses themselves but also the environment in which the buses will drive through. When the traffic lights are not working properly, or if the navigation systems have been manipulated, the whole system stops working properly as everything is connected into one ecosystem. Fourth, the involvement of governments limits rather than advances the possibility for international cooperation. Large companies operating at the international level usually do not find it difficult to cooperate with experts from other companies and to adhere to government restrictions. The problem is that the

respective governments are not that successful in this field. The companies have to then adhere to both national and international legislation. This does not mean that such an environment is unbearable, however, this schism is not perfect for cooperation. Fifth is the problem of allocation of responsibilities within PPP. In general, the expectations on security are on one hand very high towards the state, on the other hand, the private sector does not want to allow the state to peek under the hood and check the fulfillment of their processes and functions. The state is usually allowed to coordinate and stimulate the policies and the nature of the cooperation, nevertheless, the companies hesitate to allow them to scrutinize and check the inner processes (Cavelty and Suter 2009, p. 183-184).

The state is in the private-public partnership seen as the bad guy. This is supported by the fact that experts from the field like IT engineers, system developers, or even white/black hat hackers do not have much faith in the state at all. As for the IT engineers, this is sometimes caused by the fact that in the private sector there are more educated or more skilled experts than in the state structures. This is simply because private companies can offer higher salaries and opportunities than the state, thus attracting the best from the field (Lt.Col. Ivo Zelinka, Czech Army [oral interview], November 2021). That is why the more skilled part of connected world experts is in the private sector and does not trust the state experts. They simply believe that the state does not understand the problem on the desired level. The other, maybe not that clear of a reason, is the hacker subculture itself, which portrays itself as anti-government. This subculture consists of people who are downloading movies and games from the Pirate Bay¹², hacking and tuning their cars by rewriting the memories in the electronic and engine control units or creating internet markets within the dark web¹³ and the deep web¹⁴ to sell/buy forbidden stuff. This sort of people is naturally against the classical state system full of rules restricting and punishing the aforementioned behavior. It is worth to note, that these people are usually not guys in black hoodies operating from the basement. These people are well-educated engineers – math, programming language or law experts who, in their free time upload the stolen movie or create a website on how to install programs for

¹² Pirate Bay is a platform for uploading and downloading (usually stolen) data such as movies or games

¹³ Darkweb – Intentionally hidden part of the internet

¹⁴ Deepweb – Part of the internet not accessible by conventional search engines

free. They do it, because they are simply able to do so, they can execute codes or assemble devices - skills that regular people usually do not have (Dr. Miriam Dunn Cavelti, Cybersecurity expert [oral interview], January 2022).

This chapter served mainly to introduce the public/state debate with its basic characteristics and limitations. As you might already understand from the brief introduction of the public/state debate, the crucial (if not the most important) variable regarding this topic is the cooperation and communication aspect.

3.2.1 Communication and Cooperation Aspect

Not only in cybersecurity but in real life in general, for any kind of cooperation and collaboration it is important to have a mutual trust. It does not matter, whether it is private-private, private-public, or public-public, maintaining the same level of trust between the actors is often challenging. In the previous chapter, some limits to such cooperation, using the example of the PPP concept, were explained. There are many others that would be worth mentioning, such as the lack of human resources in the cooperation apparatus, promotion of the PPP within small and medium enterprises, which have limited leverage over the agenda, insufficient budgets and others (ENISA 2017, PPP, p. 5-6). However, let us now focus on the advantages that such partnerships provide.

The first and main driving force is the economic side. Many companies hope that by cooperating with the government, it will help them earn a good reputation within governmental channels, moreover, there is the possibility to receive important information regarding regulations on time (or even before), so they have leverage over the competitors. From the government's point of view, it helps them to better understand the necessities on how to protect the businesses because they can see it from another perspective, which would be otherwise hidden. This information helps to save public money that would be used for essential research (ENISA 2011, Good Practice Guide, p. 17-18).

The other driving force is the regulatory requirements. In some cases, it is vital when the private sector leaves the legislation agenda solely to the state. This does not work every time, but especially for the companies that are novices to the market or are in the phase of entering it, it is handy when one authority sets clear rules that everybody sticks to. In other cases, however, especially for big companies that are

already in the market for a longer time, it is a welcomed opportunity to provide inputs to new legislations, or even work together with the government to develop new cybersecurity strategies (Ibid, p. 19-20).

Another driving force is the social aspect. Both the public and private sector are pushing the cybersecurity topic as something that has the highest priority. One might argue that in some cases, this is done artificially. The government and respective political parties and politicians want to show that they care about this issue just to win the votes. Private enterprises push the topic to scare the population and then sell their cybersecurity products to them. Artificially or not, social interest is an important driving force in forming partnerships. There are of course other driving forces that help/force the actors to cooperate, such as the supra-national regulations (EU, OSN) (ENISA 2017, PPP, p. 11). For more info, please see Figure 1 in the attachment.

In the previous chapters we introduced the connected world, what are the positives and negatives of being connected and what questions/challenges the connected world brings to us. In the second chapter we explained the importance of securing the connected world, thus the cybersecurity topic. Now we know the basics about cybersecurity, what the attack vectors are and what could possibly happen when securing the connected world would be underestimated. However, what was the core of the previous chapters was to outline the main challenges and problems that the connected world and cybersecurity bring to our lives. To sum up, first of all, it is the problem of data privacy. On one hand, it is important to secure our personal data against potential misuse by criminals. On the other hand, to move further and make systems even more convenient, we have to feed them with data so the algorithms can operate. Another challenge that was pointed out was the public-private partnership debates, which are crucial for the future development of cybersecurity. Last but not least, from the challenges that were chosen for this paper, is the communication and cooperation aspect. Such challenges are present in both cybersecurity in general, but also in the cybersecurity in automotive. Let us now then focus on the automotive domain to introduce it and point to characteristics that are specific for it.

4 Cyber Security in the Automotive World

Chapter four could be divided into two parts. The first part builds on the previous descriptions, plus introduces the automotive domain within cybersecurity. Its clear understanding is crucial for making sense out of the second part. The second part aims to answer the question: what are the specifics of the automotive domain. So far, the thesis aimed to classify the automotive domain as a part of the connected world and cybersecurity, and to find common phenomena with other domains. The second half of chapter four, however, focuses on specifics rather than similarities.

As the number of connected vehicles increases, so does the number and variety of cyber-attacks. From 2016 to 2019, the number of cyber incidents in the automotive industry increased more than 7 times (to almost 200 incidents per year) (Kulda 2020, p. 2). This information tells a lot about how important cybersecurity is in the automotive world. However, it is still somehow difficult to imagine how is it possible that the number of incidents grows so rapidly. This chapter explains that the number of attacks increase mainly due to ever-increasing interconnectedness. It will also examine the path that the automotive world is following and what the next years in the automotive world could look like. For this purpose, intelligent transportation systems and autonomous vehicles were chosen, as they have the potential to change the whole automotive environment with regard to cybersecurity (Ibid, p. 3). Within the subchapter “*Autonomous vehicles*” we will also learn about the most common vehicle attack vectors. This will help us to understand how complex and diverse and therefore vulnerable our vehicles are, thus highlighting the importance of securing them. At the end of the “*Cybersecurity in the Automotive World*” chapter will be introduced the main specifics that automotive has in relation to cybersecurity. Specifically, it will mention data, the PPP and cooperation in general, and lastly the regulations that are specific for vehicle manufacturers.

4.1 Next Generation Mobility

Intelligent Transportation Systems (ITS) and modern vehicles in general are becoming an integral part of road transport. The growth of its own intelligence and its importance is also connected with its higher vulnerability to cyber-attacks. The more the system is connected, the larger the attack surface is. Moreover, the

disadvantage of interconnectivity is that it is easier to aim at more targets with only one attack. For example, a successful attack on the backend could lead to an attack on the whole fleet of vehicles. This happened already during an infamous incident from 2014 carried out by an attacker called Sun Hacker. By a remote attack, Sun Hacker managed to change the content of information boards on highways in four different states in the USA. In the same year, a group of IT experts from Michigan managed to compromise almost 100 intelligent traffic lights and change their signals (Jacobs 2014).

The ITS plays a big role in securing the continuity of road transport and its importance will grow even more with time. Previous chapters explained, how important data are and that the smart systems cannot properly work without them. And in road transport this applies even more. While today it is more of a useful complement for road users, in the future it is very likely to be the key element. Timely and accurate information provided by the ITS is a prerequisite for the development of autonomous vehicles that will depend on machine processing of data from the surrounding environment (Huq et.al 2017, p. 5-6). That means that as much data as possible will be needed from all of us and our behavior on the roads to make the future mobility design possible. The ITS is used mainly to inform drivers through information boards, speed limitation, blocking access to certain sections, but also for monitoring and controlling traffic in tunnels. To streamline the operations of the ITS, the need arose to connect these systems both with each other and with vehicles themselves and therefore the cooperative intelligent transport systems projects began to emerge. So far, the fully connected and complex ITS system has not been implemented yet. Nevertheless, in the near future (2030+), it is expected for the ITS to start operating in big cities where the infrastructure is ready for it (Festag 2014, p. 168).

With the growing interconnectivity comes the higher vulnerability to cyber-attacks. That is due to two main reasons. Firstly, as the network gets bigger, so do multiply the entry points to the systems. Second, as the ITS and autonomous driving is becoming an integral part of our lives and its importance is growing, so does the appeal to attack it. To understand it, let us imagine a pickpocket who tries to steal wallets from his victims. It is easier for them to operate in crowded places, such as squares or bus stations where people and their wallets abound. Moreover, the more

targets, the higher is the chance that the pickpocket will “hit the jackpot” by stealing a wallet full of money. So far, the attacks against the ITS are rather rare and when they happen, it is usually by ethical hackers who try to point out vulnerabilities of the systems (Kelarestaghi et.al 2018, p. 80-81).

4.2 Connected Vehicles

Like any connected device, vehicles also can be compromised, and an attacker can remotely control virtually any digital component of the vehicle. This can give the attackers full control of the vehicle and endanger the safety of the user, as well as other road users. The complex ecosystem of modern cars creates a vast cyber-attack area with millions of potentially affected endpoints and users. For illustration, the original Volkswagen Golf from the 1970s had 400 lines of code that secured the operation of the car. The new Volkswagen Golfs have more than 100 000 000 lines of code (Marek Bělka, Škoda Auto [oral presentation], March 2022). In addition, vehicle systems are evolving, and new services or capabilities can bring with them additional entry points for potential attackers. This is a major concern for the road safety as the number of connected vehicles continues to grow. Connected vehicles are estimated to account for a quarter of all passenger cars in the world by 2023 (Upstream Security 2021). The impacts of cyberattacks on connected vehicles can lead to:

- Obtaining unauthorized physical access to vehicles
- Manipulation of the vehicle control
- The use of electronic vehicle control units for malicious cyber activity
- Theft of sensitive personal data
- Blackmailing victims through ransomware (McKinsey & Company 2020, p. 11).

There would not be enough space in this paper to name all of the entry points where the attacker could get in. For an illustration, here is a short list of the main attack vectors/surfaces: The potential ways into a vehicle according to “*The Car Hacker’s Handbook: A Guide for the Penetration Tester*”, written by Craig Smith:

Cellular
<ul style="list-style-type: none">• Access the internal vehicle network from anywhere• Exploit the application in the infotainment unit that handles incoming calls• Access the subscriber identity module (SIM) through the infotainment unit<ul style="list-style-type: none">• Use a cellular network to connect to the remote diagnostic system<ul style="list-style-type: none">• Eavesdrop on cellular communications<ul style="list-style-type: none">• Jam distress calls• Track the vehicle's movements• Set up a fake Global System for Mobile Communications (GSM) base station
Wi-Fi
<ul style="list-style-type: none">• Access the vehicle network from up to 275 meters away or more• Find an exploit for the software that handles incoming connections<ul style="list-style-type: none">• Install malicious code on the infotainment unit<ul style="list-style-type: none">• Break the Wi-Fi password• Set up a fake dealer access point to trick the vehicle into thinking it is being serviced<ul style="list-style-type: none">• Track the vehicle
Key Fob
<ul style="list-style-type: none">• Send malformed key fob requests that put the vehicle's immobilizer in an unknown state. (The immobilizer is supposed to keep the vehicle locked so it can't be hotwired. We need to ensure that it maintains proper functionality.)<ul style="list-style-type: none">• Actively probe an immobilizer to drain the car battery<ul style="list-style-type: none">• Lock out a key• Capture cryptographic information leaked from the immobilizer during the handshake process<ul style="list-style-type: none">• Brute-force the key fob algorithm<ul style="list-style-type: none">• Clone the key fob• Jam the key fob signal• Drain the power from the key fob
Tire Pressure Monitor Sensors (TPMS)
<ul style="list-style-type: none">• Send an impossible condition to the engine control unit (ECU), causing a fault that could then be exploited

<ul style="list-style-type: none">• Trick the ECU into overcorrecting for spoofed road conditions• Put the TPMS receiver or the ECU into an unrecoverable state that might cause a driver to pull over to check for a reported flat or that might even shut down the vehicle<ul style="list-style-type: none">• Track a vehicle based on the TPMS unique IDs• Spoof the TPMS signal to set off internal alarms
Infotainment Console
<ul style="list-style-type: none">• Put the console into debug mode<ul style="list-style-type: none">• Alter diagnostic settings• Find an input bug that causes unexpected results<ul style="list-style-type: none">• Install malware to the console• Use a malicious application to access the internal CAN bus network• Use a malicious application to eavesdrop on actions taken by vehicle occupants• Use a malicious application to spoof data displayed to the user, such as the vehicle location
USB
<ul style="list-style-type: none">• Install malware on the infotainment unit<ul style="list-style-type: none">• Exploit a flaw in the USB stack of the infotainment unit• Attach a malicious USB device with specially crafted files designed to break importers on the infotainment unit, such as the address book and MP3 decoders<ul style="list-style-type: none">• Install modified update software on the vehicle• Short the USB port, thus damaging the infotainment system
Bluetooth
<ul style="list-style-type: none">• Execute code on the infotainment unit<ul style="list-style-type: none">• Exploit a flaw in the Bluetooth stack of the infotainment unit• Upload malformed information, such as a corrupted address book designed to execute code<ul style="list-style-type: none">• Access the vehicle from close ranges (less than 90 meters)<ul style="list-style-type: none">• Jam the Bluetooth device
Controller Area Network (CAN)
<ul style="list-style-type: none">• Install a malicious diagnostic device to sent packets to the CAN bus• Plug directly into a CAN bus to attempt to start a vehicle without a key

- Plug directly into a CAN bus to upload malware
- Install a malicious diagnostic device to track the vehicle
- Install a malicious diagnostic device to enable remote communications directly to the CAN bus, making a normally internal attack now an external threat

As the table above shows, there are many entry points, through which an attacker can enter our vehicle. All of them have their own specifics. An attack through one entry point does not give the attacker a full scale of operations that they can carry out. It depends on their goals they want to achieve. When the goal is to steal the car, then an attack through a key fob would seem like the best option. However, if the goal of the attacker is to spy on the vehicle user, then cellular, infotainment console or TPMS would most likely be used. Some of the entry points overlap with the functions that could be misused. This is mainly due to the interconnectedness of the whole vehicle ecosystem, where usually more parts of the vehicle need to cooperate to execute a command. Another inference that we could make from the table is that all the entry points require different effort by the attacker to penetrate the vehicle. For example, a TPMS requires to disassemble the whole vehicle, even the control unit itself. This does not call only for highly educated expert, but also for the attacker to first buy, borrow or steal the car to know, how it gets disassembled in the first place. A Wi-Fi or Bluetooth attack, on the other hand, has the advantage for hackers that they do not have to physically get to the car. As for Bluetooth, the attack range is within 90 meters. For Wi-Fi it could be up to 275 meters (Smith 2016, p. 7-9).

It is important to note that this is just a basic level on which we can identify the attack surfaces. Nevertheless, it is rather general, so the reader can have an idea. If we would like to understand it in more detail and identify specific threats, we would need to break-up the aforementioned attack vectors. As an example, a `wpa_supplicant` (Wi-Fi daemon¹⁵) could be used. The version of Wi-Fi alone does not tell much about the possible damages, which could happen when an attacker would misuse its vulnerability. However, when breaking-up the whole Wi-Fi system, one can focus on particular elements within it. For example, when we focus on the `wpa_supplicant`, the list of potential damages becomes shorter (Ibid, p. 10). We then

¹⁵ Provides Wi-Fi connectivity

need to know which is its version. In the case it is an older one, our car can then connect to malicious access points because it is lacking the newest security mechanisms. That would work not just for cars but also for almost any other device using a WAN¹⁶. In general, to understand the potential vulnerabilities and weaknesses, one has to have deep knowledge about all the components and its respective parts to be able to analyze it. The more we break it up the more information we can get about our device and its potential entry points and attack vectors (Ibid, p. 11).

4.3 Specifics of the Automotive World

So far, the paper explained that our cars are just a part of the connected world. Moreover, we introduced what are the attack vectors and possible weak entry points to hack our vehicle, thus briefly outlining its specific cybersecurity challenges. Nevertheless, so far, the aim was mostly to find a common ground with other connected devices to look for common characteristics. In this chapter, we will now focus on the specifics that the automotive world has within cybersecurity in the connected world.

Firstly, it is important to mention the biggest and most obvious difference, which is the fact that any car security incident can directly lead to injuries or even death of its passengers and other traffic participants. So far, when we would talk about cybersecurity incidents, we would mostly speak about an indirect harm to people. To give an example, let us recall the cyberattacks on Estonia from 2007. Series of DDoS attacks shut down, apart from the government websites, also the banking sector and other services (TRAYNOR 2007). Allegedly, for several minutes it was impossible to call an ambulance because the connecting servers were down. Some might argue that not being able to call an ambulance when having a heart attack would be a clear consequence from the cyber-attacks. However, this is not a direct harm to human beings, or at least it is difficult to prove it. Anyway, this debate on what is and what is not a direct harm is not an exact science and various people will have various opinions on this topic. However, in the automotive world it is clearer than in the other domains. To give an example, when somebody would hack a car and disable breaks,

¹⁶ Wide Area Network – large computer network

which would lead into a car crash, then we can easily feel the connection between the cause and the consequence. This example is rather straightforward, in other cases when the attacker would target other components in the car, we would most likely have to come back to the original direct/indirect discussions. For instance, when the attackers would switch off the lights, suddenly play loud music or start moving the wipers. During all of these instances, a driver could get distracted and crash his vehicle. Whether the aforementioned scenarios would be labeled as a direct harm or not, the specific of automotive is still valid. There is no other connected device that most of us use every day, whose malfunctions can immediately lead to life threatening situations.

4.3.1 Data Driven Specifics

In this paper, and especially in the chapter “*Connected World*”, we came across the problem of data (value of our data, data sharing, personal data). In general, when we would briefly sum up, we could point mainly to the problem of giving away enough data, so our devices are getting smarter, but also securing them to protect our privacy. In the automotive domain, however, such balancing has a new dimension. The specific is that in the automotive, the data is inherently needed for the operation of the intelligent transport systems (ITS), autonomous vehicles (AV) and connected vehicles (CV) in general. All the ITS, CV and AV gather as much data as possible from its surroundings to operate properly. Without having a complete database about its surroundings, such means of transport would become erroneous. It is evident that any error that would lead into a traffic incident would consequently make people anxious about connected and self-driving vehicles. If we want to live in a future where public transport, taxis and private vehicles are driving themselves, then those vehicles have to be 100% accurate and reliable.

In the chapter “*Value of Our Data*” we explained how the algorithms work. If we want them to reach the 100% accuracy, we have to feed them with as much data as possible. That basically means, that our data is endangered. Data about our driving habits, driving history, sudden reactions during incidents, but also our behavior on the streets as pedestrians. Such information about behavior of the drivers and traffic rules in general must be extensive to become reliable. However, there is no one clear policy published by the authorities, not even by the private sector on exactly which

kind of data is needed and how is this data going to be acquired. This statement does not mean that the authorities, developers, or automakers are secretly doing something illegal to get our data. There are still, of course, both the national and international laws regarding data privacy that the aforementioned have to follow. Plus, the aim of this chapter and this paper in general is not to raise legal questions. Actually, the paper just wanted to demonstrate the specific of automotive, where the whole future mobility ecosystem is urgently dependent on data that will be acquired from us. Moreover, it will be necessary to do so, in order to ensure the security of passengers in the future.

4.3.2 PPP in the Automotive World

A certain space in this paper was granted to a communication and cooperation aspect and to the public-private partnership in general. Firstly, it is important to note that the automotive does not have any specific rules or policies that would be considerably different than in the other domains. In most cases, the automotive world shares with the other domains both the advantages and shortcomings resulting from such partnerships that were explained in the chapter *State or Private Actor?*. OEMs have to adhere to both the national and international legislation and comply with the homologation requirements. However, there is one specific that we could point out. The automotive is the only domain, in which the OEMs have to receive certificates, which have to prove that the vehicles are cyber-secure. Most of the goods that we buy, must obtain certain certificates, otherwise they could not be sold. A cybersecurity certificate, however, is something unique for the automotive. Without such certificate, a car manufacturer is not allowed to sell its vehicles. This forms a cooperation between the private and public sector, which is based on strict compliance with rules. Any deviation from the standards results in severe consequences for the automakers.

This does not apply for the whole world equally, there are different authorities in different regions with their own rules and standards. As for the purpose of this paper, only the UNECE¹⁷ regulations will be introduced. For info, to whom does the UNECE regulations concern, please see Figure 2 in the attachment. Another note is

¹⁷ United Nations Economic Commission for Europe (56 member states)

that also within the UNECE, the countries are not on the same level of cybersecurity preparedness. Even when they fall under the same authority embodied by the United Nations, the deployment of cybersecurity measures has different time schedules in the respective countries. For example, the necessity to obtain cybersecurity certificates already applies in some European countries (since 2022). However, Russia, for example, is postponing its deployment until the local OEMs are ready to fulfill the requirements (UNECE 2021, Implementation of R155, p. 2).

4.3.3 UNECE

United Nations Economic Commission for Europe is one of the regional programs within the United Nations established in 1947. One of the fields where the UNECE operates is the cybersecurity. The main purpose was to come up with a shared framework, which will encourage competition but also set common and clear standards that the OEMs within the UNECE will follow. Such rules should ensure reliability, continuity, and safety of critical infrastructures, concerning the transport means as well. These standards are then tested by both the internal and external auditors, which later decide, whether the vehicle is cyber safe and whether it is able to operate on our roads (UNECE 2021, Addendum 154, p. 4). Every company is then ordered to have at least one external recertification audit a year, which ensures that the company still adheres to the standards. An important part of the whole process is that the company regularly informs the relevant authorities about cyber incidents that the manufacturer had to face (NUKIB 2022, Hlášení incidentů, p. 2). Here are still some weak spots when we talk about reporting of cyber incidents. Unfortunately, there is not a unity on which incidents have to be reported and which not. Different countries and automakers still haven't agreed on terms. For example, there is no clear understanding on what a cyber incident is and how to frame it. It will be vital for both public and private actors to have the same understandings to improve such cooperation in cybersecurity. Nevertheless, despite the unclarities regarding reporting to authorities, there are as well policies, which are already in operation. This paper analyzes two of them – CSMS and SUMS, which are directly concerning cybersecurity in automotive.

4.3.3.1 CSMS

The CSMS stands for Cyber Security Management System. Sometimes we can also see a R155 shortcut as well, which refers to UN Regulation No. 155. In the official United Nations agreement is written that: “CSMS concerns the Adoption of Harmonized Technical United Nations Regulations for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these United Nations Regulations” (UNECE 2021, Addendum 154, p. 1).

In other words, it describes how cybersecurity of the vehicles must be managed and controlled throughout the whole lifecycle of the vehicle. The whole lifecycle is a crucial part of the aforementioned sentence. It means that the whole process starts by developing the very first component which will be used and continues until the “end of life” of the whole vehicle. If any moment of the lifecycle would be underestimated from the security point of view, it would endanger the operability of the vehicle and potentially the whole fleet of vehicles. OEMs have to ensure detection of the cybersecurity incidents as well as to prepare the appropriate response to it. This requires especially proper monitoring and detection of possible threats, but also creating hypothetical scenarios and actively preparing solutions for it (Škoda Auto, Koncernová směrnice 2020, p. 1).

4.3.3.2 SUMS

The SUMS stands for Software Update Management System, and again sometimes you can encounter the official United Nations shortcut – R156. Software updates are vital for any connected vehicles. Software updates do not only improve infotainment applications or change the ambient color inside the vehicle, but they are also used for error corrections. As it was mentioned before, modern cars have around 100 000 000 lines of code, which means that it is basically impossible to have a software, which is without flaws. Such flaws can be detected by the vehicle manufacturer during penetration tests or uncovered by hackers who found the vulnerabilities first. In both cases a software update is needed to mitigate the potential risks (Škoda Auto, Koncernová směrnice 2020, p. 1).

The SUMS sets rules on how such updates should be performed. The OEMs have the responsibility to ensure that the updates are safe and that they are

documented, so the owner of the car or potentially the workshop employees know which version the car is using. Proper documentation ensures that other incompatible updates would not be installed (Škoda Auto, Koncernová směrnice 2020, p. 2). Such updates can be performed either remotely (over the air updates) or in authorized workshops. Over the air updates (OTA) are in 2022 only approaching its full deployment as the majority of software updates is being carried out by authorized workshops (Škoda Auto, Cybersecurity Strategy 2022, p. 14). The OTA is an interesting tool for repairing cars with its own cybersecurity advantages but also challenges. For more information, please see *5.2 Main Cybersecurity Objectives According to Škoda Auto*.

Now let us go back briefly to the PPP and cooperation and communication aspect. As it was explained, such partnerships and cooperation in general is based on mutual trust. In the automotive but in other domains as well, this is not always easy to establish. As it was shown on the UNECE example, a certain level of trust can be established through certifications and audits, at least when we talk about cybersecurity. These rules, set by the public actor, are clear and the automakers had enough time to prepare for its deployment. This does not mean that the UNECE scenario with cybersecurity certificates is the perfect PPP model. However, it builds a certain level of trust between the actors. Due to confidentiality issues, it is not possible to deeply analyze such partnerships to see its pros and cons and possible spaces for improvement. Nevertheless, the aim of this part of the paper is to answer the research question and describe the specifics of cybersecurity in the automotive domain in relation to the PPP. The main specific that this paper points out, is the necessity to obtain cybersecurity certificates to be able to operate on the market. It will be interesting to see, whether this trend will serve as a good example for other regions than the UNECE and potentially for other domains than the automotive one.

The cybersecurity topic is not perceived in the same way in different parts of the world, especially when we talk about the processes which should ensure it. Obviously, such disparity prevails also within the respective car brands. Every company has its own perfect model. There would not be enough space in this paper to analyze and compare them all. However, for us to better understand how cybersecurity is perceived and exercised by an automaker, let us now focus on one particular brand and its perspective, which is Škoda Auto.

5 The View from Škoda Auto Perspective

In this chapter we will introduce Škoda Auto as a vehicle manufacturer. After a brief introduction will follow a declassification of cybersecurity objectives according to the company. Here the reader will find how the whole cybersecurity topic is perceived by the biggest Czech vehicle manufacturer and also what are, according to Škoda experts, the biggest cybersecurity challenges that the company is facing or will face in the future. Finally, a real-life cybersecurity incidents that Škoda Auto had to solve, will be introduced.

5.1 Škoda Auto: Brief Introduction

Škoda Auto belongs with other brands (Audi, Volkswagen, Porsche, Seat, Lamborghini, Bentley) to the Volkswagen (VW) Group. It was acquired in 1991 when VW Group bought 30% of the shares of Škoda Auto. However, the history of Škoda Auto reaches way further into the past. We could find its origins in 1895, when Václav Laurin and Václav Klement started to assemble their first bicycles and motorbikes. The first car left the factory of Laurin and Klement in 1905, and its name was Voiturette A (see figure 3). Next important milestone is the year 1925 when Laurin and Klement merged with the engineering company Škoda. Next huge milestone, as already mentioned before, happened in 1991 when the VW Group bought the 30% share, which happened to be consequently a 100% share in 2000.

Škoda Auto is based in Mladá Boleslav, however, it has other manufacturing sites around the world as well (Slovakia, Germany, Ukraine, Russia, India, Algeria, China) and sells its cars currently in more than 100 countries (Vošvrda 2020, p. 39 - 41).

5.2 Main Cybersecurity Objectives According to Škoda Auto

The main cybersecurity objective, according to Škoda Auto, is the customer and brand protection. A car is an important part of our lives, some use it every day to go to work and then back home. We as customers have to be sure that our car is secure (from all possible angles) when we are driving our friends and relatives. Moreover, our car is not the only one on the road, a hypothetical accident is influencing its surroundings and might cause collateral damage. That goes along with the brand

protection. Every accident on the road is influencing opinion of others about the quality of the car. By securing its customers, the company secures its own good name on the market as well (Škoda Auto, Cybersecurity Strategy 2022, p. 2).

To succeed in securing both, Škoda Auto set 4 main pillars that serve as the success factors for the cybersecurity management. The first and the most important success factor is the **qualification** of its employees. In the previous chapters, we outlined that the majority of cyberattacks aim at the human factor, which is always more or less vulnerable. The qualification through regular workshops and trainings helps to form trained professional teams that can easily respond to new cyber-attacks. It is a matter of course that this includes random tests of the employees by sending SPAM and phishing emails, so the employee has to recognize them and consequently report them to the authority or the relevant department. This practice is a common policy to ensure at least the basic cybersecurity awareness within the company. This applies not only to the automotive sector, or to the companies that have something to do with cybersecurity topics, but also for the other enterprises that use smart devices in their business routine. Such practices, together with monitoring current trends and implementing latest measures, ensure safe handling of data and security of the networks.

Skilled personnel is the third pillar and the core of the internal security. The company then has to ensure that the employees are using modern **technology** to carry out their tasks properly. These technologies can have various forms (newest software, threat intelligence platforms, database management, IT server management, automatization processes) but, in general, they are helping the employees to monitor more objects, detect more precisely and react faster. In Škoda Auto and in the whole VW Group, the newest technology is the vital component for mitigating possible threats.

Third pillar is the **cooperation**. Cooperation includes both horizontal and vertical approach. By horizontal approach is meant the information sharing within the company on the level of the respective teams. As for Škoda Auto, this means the quality department, which covers the whole vehicle conformity. Development department is responsible for developing both hardware and software components that the vehicles are equipped with, or the components from suppliers that are being used. IT department with its highly skilled personnel repairs current vulnerabilities,

such as data leakages or backend malfunctions. Legal department is responsible for contract compliance, phishing attacks, such as fake sites at web or social platforms, or is responsible for communication with actors from outside the company. Aftersales department ensures the proper communication with customers. It makes sure that all inquiries or complaints are received and consequently solved. It also manages the process of calling the vehicles to workshops and repairing damaged components. Last but not least, is the outside monitoring department, which monitors new trends around the world in order to be in the picture of the current threat landscape.

Vertical cooperation is done at three different levels. The first is the one within Škoda Auto, where the car security team works together with the car security board which has the decisive competence. The second level is within the VW Group. All brands are responsible for sharing relevant information with other group members. This information sharing is done regularly, and its main aim is to have as much information about the cases that the other brands solve as possible. This helps to solve the issues faster by the fact that more experts know more than one. The third level is reporting to authorities. In the majority of developed countries, such reporting is done to their respective authorities, which differ in every country. In the Czech Republic, these authorities are primarily NÚKIB and the Ministry of Transport. Within all the levels, such cooperation works from both sides. Information is shared vis a vis, which helps to work on common goals. Within Škoda Auto and the whole VW Group, such data-sharing and common approach help to secure the customers and the brand as well. As for the relationship of the company and authorities, the cooperation is mutually beneficial. As it was explained in the chapter “*Communication and Cooperation Aspect*”, the private actor gets the newest legislative info and is able to be a part of the formulations of new laws and regulations. The public actor, on the other hand, gets to know the procedures in the private sector, which is valuable knowledge because it saves public money, which would be otherwise spent on research to understand the problematics.

The last pillar is the **reaction**. Reaction capabilities stand at the end of the whole chain and are the outcome of the common work of employees to mitigate threats. Vehicle manufacturers are responsible for fast reactions and response, and its preparedness 24 hours a day, 7 days a week. Under the reaction we can imagine a

various set of procedures. This can include for example system updates, which correct erroneous software, shutting down unfunctional applications, or reporting incidents to police to arrest the attackers.

These four pillars are, according to Škoda Auto, the basic instruments to secure the vehicle. There are many other inner policies which have to be applied to increase the capabilities to monitor, detect and react. Worth mentioning is the process after the threat is mitigated and the case is solved. This process is called **lessons learned** and is primarily about the retrospective reflection of the cases. The main reason for this is to prevent recurring incidents, and to improve the responsiveness to vulnerabilities and incidents. This includes not only the actual attacks on the company, but also internal penetration tests, which are important to ensure the inner awareness about the vulnerabilities. Penetration tests are carried out by experts from different fields to help investigate cybersecurity incidents and potential weak spaces that the attacker could use and affect the company products (Ibid, p. 3).

As it was highlighted in the previous chapters, as the whole connected world gets bigger and more connected, it is expected by the experts that the number of cyberattacks will increase in the future as well. As for the automotive world, this concerns the majority of vehicles that will be produced in the future. As it was mentioned before, according to NÚKIB, in 2023 every fourth vehicle on the road will be a connected one. It was also shown what are the attack vectors and what vulnerabilities they include. In the future, it is expected that the cyberattacks will be mainly on the ECUs, infotainment, or backend servers. Some attacks are more severe than the others, according to the customer perspective, the ones aiming at the ECUs, infotainment and key fobs are the most damaging. An affected ECU can stop your car from starting itself, unfunctional infotainment leads to major inconveniences (maps, music, heating) and potential data leakage about your driving history and the history of your vehicle in general. Such data (sensitive personal data as well) could be later sold to a third party by the attacker. Attacks on key fobs usually lead to a theft of the whole vehicle (Ibid, p. 11).

This development is well reflected by the authorities, which come up with timely solutions through an updated legislation. Such regulations concern the whole lifecycle of the vehicle from the development phase to the end of service of the car. Before, the paper introduced mainly the UNECE authority, however, regulations and

recommendations are coming from different sources. This applies especially when the company aims to sell its products worldwide, then it has to adhere to many different homologation requirements. Vehicle conformity and homologation requirements of the vehicle together with its parts have to be met in order to register any new vehicle. Without such compliance, the vehicles are not allowed to our roads. To achieve this, the vehicle manufacturer has to bear in mind both the international and national legislations. International legislation usually ensures the vehicle conformity as a whole, whether it has proper software updates downloaded, follows emission standards and the vehicle safety in general. International regulations embodied by the central authority like the UNECE, the EU or others, post those regulations in international languages to be clear to all respective regions. National legislation, on the other hand, primarily concerns the parts of the vehicle. Every country has more or less different legislation than the other. Whether it is telecommunication rules, labeling rules (waste, quality) or recommendations on how and where the vehicle manufacturer posts information relevant to its customers (location of workshops, registration conditions). All of the devices and parts that the vehicle uses have to comply with such rules (Ibid, p. 15).

According to Škoda Auto, there are four major challenges that the automotive, and potentially other sectors, will have to face. First, it is the phenomenon of autonomous vehicles. These types of vehicles will depend much more on connectivity than the current vehicles, which means that they will be more vulnerable to cyber threats. In addition, they will increase the communication with other vehicles and the road infrastructure. The ability to receive and respond adequately to information from the environment is one of the fundamental differences between the traditional and the autonomous cars. A single successful attack on the communication layer can affect the control of all vehicles communicating with each other. For this reason, communication technologies are expected to be the target of cyberattacks much more frequently than the other vehicle components. With the development of autonomous driving, the threats associated with the use of artificial intelligence and machine learning will also become increasingly significant. Autonomous vehicles use different types of sensors to monitor the surrounding environment. The obtained data is processed by systems using AI, which continuously evaluate the current situation and send commands to relevant ECUs controlling the vehicle. An attack on

AI systems essentially allows the attacker to manipulate the vehicle's controls. Any defect in the evaluation of surrounding objects can cost human lives and endanger the trust of public towards the autonomous vehicles.

The second challenge is connected to new cybersecurity standards and regulations. As the automotive industry shifts towards connected cars and smart mobility, an added element of vulnerability arises. This means that the new standards and regulations will be published more frequently in the future to react adequately to emerging trends. Vehicle manufacturers will be then responsible for their timely implementation, which is a challenging topic. Most vehicle manufacturers have their own regulations which are more or less on a similar level with the international ones. Škoda Auto is not an exception, even without the international standards, the company would still follow cybersecurity processes to secure its vehicles. Examples of the international regulations are numerous, to name some: UNECE (R155, R156, R157) or ISO/SAE 21434 and ISO/IECE 27000 family (Ibid, p. 13).

Third, the online remote updates (ORU) or the over the air updates (OTA). Such service is a wireless delivery of a new software, firmware¹⁸, or other data to vehicles. These updates are necessary to ensure that the car has the newest and best performing software versions without the need for the customer to visit the workshop, which is, without doubt, more convenient. Nevertheless, these benefits create a new world of opportunities for attackers. They could attempt to corrupt the software update kits with malware and enter the vehicle system to steal personal data or even take physical control of the vehicle.

Fourth, the modern electronic control units. Some ECUs communicate with the outside world as well as the internal vehicle network. These ECUs pose the biggest security risk to vehicles and their passengers, because they are the ideal entry points for cyber-attacks. Moreover, modern vehicles are able to communicate with other devices through wired or wireless interfaces such as USB, Bluetooth or Wi-Fi. ECUs are diverse and have different roles in the vehicle, and as much as they differ from each other, so grows the attack surface and its vulnerabilities and possibilities for the attacker to manipulate them (Ibid, p. 14).

¹⁸ A software managing the operation of an embedded system (mobile phones, cameras, traffic lights)

This has been an introduction on what are the future cybersecurity challenges from the point of view of Škoda Auto, what are its policies and processes to ensure a high-level of cybersecurity preparedness. Moreover, a look into the future on what could be the challenges in the horizon of 10+ years was provided. However, even with the high-level cybersecurity preparedness, the cyber-attacks on its vehicles are still possible. For the illustration, a real-life example of vulnerabilities of Škoda vehicles will be shown.

5.3 Internals of Škoda Auto: A Hands-on Approach

In 2016, Colin Urquhart, Xavier Bellekens, Christos Tachtatzis, Robert Atkinson, Hanah Hindy and Amar Seeam published a paper “Cyber-Security Internals of a Skoda Octavia vRS: A Hands on Approach”, which evaluates weak entry points of Škoda Octavia vehicle. Precisely, it describes vulnerabilities of key fobs, ECUs and the infotainment. In this chapter, only the key fobs and infotainment vulnerabilities will be described. As mentioned in the chapter *Attack Vectors*, key fobs are an ideal entry point for attackers when they aim to steal the vehicle. Infotainment, on the other hand, is ideal for spying on the vehicle owner and data theft. It was also explained that every attack vector has its own characteristics, which are influencing the skills, expertise, number of instruments and generally the effort that the attacker has to spend to break in. As it will be shown, to misuse the key fob vulnerability, one has to have high level of technical expertise. Therefore, the description will be rather technical, which means as well more demanding for the reader to understand it. The infotainment vulnerability does not require such high level of expertise, however, it would be still challenging for general public to perform a successful attack. By describing this vulnerability, the paper wants to show the audience what kind of harm it can cause when somebody would break it.

5.3.1 Key Fob Vulnerability

First of all, it is worth noting that the development of key fobs has come a long way to improve the level of security. The main step forward is the shift from a fixed code to a rolling code. The difference between these two is that a fixed code re-uses the same code throughout the whole lifecycle of the key/vehicle. Which means that once the attacker figures it out, he is then able to unlock the vehicle anytime he wants.

A rolling code is changing the frequencies every time the vehicle is unlocked (Urquhart, et.al 2016, p. 3). This step forward, however, did not make the key fobs unbreakable, it just made the whole process of stealing the car more difficult. The attacker now has to figure out how works the algorithm, which is changing the frequencies. To perform it, one has to record the communication between the key and the car. For this purpose, a Software Defined Radio (SDR) is used to consequently replay the code to enter the car. Regarding the Škoda Octavia example, a scan showed that the key is using frequencies between 434.383 MHz and 434.466 MHz (see figure 4) (Ibid, p. 4). The security system then asks the key fob to provide the frequency level, if it is matching then it shows 1 and the car opens itself. If not, then 0 and the car stays locked.

Unfortunately for the attackers, it is not that simple just to read the code and then execute it. The hacker has, at the same time, introduce a noise, which prevents the car from recognizing the transmission (Ibid, p. 4). By creating the noise and covering the width of the key fob, it forbids the car to receive the transmission, but it also makes sure that the process does not get de-authenticated and consequently ceased (see figure 5). This process allows the hacker to scan the signal. Nevertheless, because of the noise, when the signal would be now executed, the vehicle would not accept it. The hacker has to filter down the noise from the captured signal and then adjust the frequency and transition width. The SDR is then able to send the correct signal to the vehicle and gain full access to it. This method by-passes the security mechanisms and can be re-used anytime the attacker wants. Apart from Škoda Octavia, other vehicles using the same security mechanisms were affected too (Kia Venga, Volvo v40, Ford Focus) (Ibid, p. 5). This vulnerability was then mitigated by further encrypting the communication between the key fob and the vehicle, so the attacker can not scan it with ordinary instruments available to the public.

5.3.2 Infotainment Vulnerability

As explained before, the car infotainment is a potential source of data about the vehicle and the vehicle user. One could assume, that this concerns only data, such as mileage, GPS location, crash data or current vehicle speed. Nevertheless, it is important to understand that the infotainment is gathering data from all the devices that ever connected to the car via USB, Bluetooth or WiFi. The article describes, how

the experts scanned the car ports of the infotainment with a port scanner Sparta. Most of them correctly demanded proper certificates to allow the communication, however, there were some, which failed to do so (see figure 6) (Ibid., p. 6). Port 15361 responded to requests without checking the certificates, which resulted into an unsecured communication between the car and the technicians. They were then able to gather personal data about the vehicle user(s). Such data included the entire call history, songs that were played and full read access to the phone. Moreover, an attacker could execute commands to the infotainment to create backdoor to gather more data in the future, remaining undetected (Ibid., p 6). Only professional workshop employees could then uncover it by analyzing it through an OBD port¹⁹.

Both the key fob and infotainment vulnerability require high level of technical expertise, certain amount of time (days, potentially weeks) and a professional equipment. That means that the amount of possible damage is maybe disturbing, but the attack is rather unlikely to be performed. That is also due to the fact, that there are still cheaper and generally more simple ways of how to steal a car or data. Nevertheless, these vulnerabilities are still existing, and it is up to the attackers to use them or not. There are many other attack vectors, concerning different parts of the vehicle, which could be targeted. Some of them least challenging than the ones described before. Even though, cybersecurity experts are actively working on mitigating the threats, a 100% security is, so far, an utopia to achieve. The more the (automotive) world will be connected, the more cyber-attacks we will be facing in the future. The aforementioned vulnerabilities were introduced in a simple way to make it readable for the wider audience. For those, who are interested in this topic and would like to know the technical background, together with other attack vectors like the OBD or the ECU, please read the whole article available [HERE](#).

6 Conclusion

This thesis presented the cybersecurity topic to a wider audience with focus on the automotive world. To make the readers clear about the topic, it was firstly explained that the automotive domain is just another part of the so-called connected world with similar characteristics and rules. After explaining the basics, the thesis

¹⁹ On-Board Diagnostics is used to access vehicle's computer to perform diagnostics.

then moved to introducing of two concepts, which are prevalent in cybersecurity. These two were data problematics and cooperation and communication within public-private partnership concept. Data and the PPP were introduced and briefly evaluated for the purpose to later show specifics of the automotive domain within cybersecurity of the connected world. The chapter “Specifics of the Automotive World” is the core of the whole paper. The author answers the research question by showing the specifics, which help the reader to understand where does the automotive domain stand. To sum up, two main specifics were found, which deserve attention and possibly a further analysis. In the first place, regarding the data problem, it was shown that modern cars and the whole intelligent infrastructure will be very demanding. The question of data privacy/feeding algorithms remains. However, for the connected cars to operate safely, it is vital to have as much info about its surroundings as possible. That consequently means, that more data about us and our driving habits will be needed, to make the whole concept of the future mobility possible. The paper does not further evaluate on this data challenge question, it only outlines the problem and adds a future outlook.

As for cooperation, communication, and the PPP concept, the automotive domain shows an interesting approach on how to build trust between the public and the private actor. The vehicle manufacturers (UNECE members) have to acquire cybersecurity certificates to receive a permission to sell cars. A cybersecurity certificate, for mass-produced products, is something unique within the connected world. This specific allows both sides to form a relationship built on pre-set rules, which are then complied. The compliance is examined by both the internal and external audits and then by the annual re-certification audits. All members of the UNECE have to follow the same rules. The only exception is that the member countries can, in some cases, move the dates of effectiveness, which ensures that the local OEMs and generally the infrastructure is ready for it. The paper does not portray this approach like the ideal form of the PPP. However, it highlights its positives, which help to build trust between the two actors. As it was explained, a trust is the cornerstone when building cooperation. Additionally, the paper mentioned the reporting to authority concept, which should ensure common awareness about the current threat landscape. Nevertheless, it is still in its development phase and has to wait for the respective parties to agree on terms of such concept.

Lastly, Škoda Auto and its inner cybersecurity policies and forecasts were presented to readers. Such presentation showed the perspective of a vehicle manufacturer, which has to operate in the automotive cybersecurity within the connected world. This gave readers the opportunity to see the presented topic from another perspective. By another perspective is meant the more process-oriented approach than the theoretical one. This was then supported by providing real-life cyber incidents that Škoda Auto had to face.

Future mobility ecosystem remains an unexplored territory, which deserves more detailed analysis from different perspectives and with focus on different aspects. A thorough research should then answer some questions, together with raising new ones. This will be vital for establishing a safe future mobility ecosystem.

7 Bibliography:

BECERRIL, Anahiby Anyel, et al. *The value of our personal data in the Big Data and the Internet of all Things Era*. 2018.

BORBA, Marcus. *Automated Machine Learning Improves the Roi of Data Science Initiatives*. MicroStrategy: Analytics and Mobility, 2020.

BOSSONG, Raphael. *Critical infrastructure and critical information infrastructure protection: the new frontier of the EU*. Challenges and Critiques of the EU Internal Security Strategy: Rights, Power and Security, 2017.

BURGESS, J. Peter (ed.). *Handbook of new security studies*. Routledge, 2010.

CARRUTHERS, Caroline; JACKSON, Peter. *Data Driven Business Transformation: How to Disrupt, Innovate and Stay Ahead of the Competition*. John Wiley & Sons, 2019.

DUNN-CAVELTY, Myriam; SUTER, Manuel. *Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection*. International Journal of Critical Infrastructure Protection, 2009.

ENISA. *Critical Infrastructures and Services*. European Union Agency for Cybersecurity. Available at: <https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services?tab=details>.

ENISA. *Cooperative Models for Effective Public Private Partnerships: Good Practice Guide*. European Union Agency for Cybersecurity, 2011, ISBN: 978-92-9204-054-3.

ENISA. *Desktop Research Report: Cooperative Models for Effective Public Private Partnerships*. European Union Agency for Cybersecurity, 2011, ISBN: 978-92-9204-055-0.

ENISA. *ENISA Threat Landscape 2021*. European Union Agency for Cybersecurity, October 2021.

ENISA. *Public Private Partnerships (PPP): Cooperative models*. European Union Agency for Cybersecurity, 2017, ISBN: 978-92-9204-241-7.

FARRAND, Benjamin; CARRAPICO, Helena. *Blurring public and private: cybersecurity in the age of regulatory capitalism*. In: Security Privatization. Springer, Cham, 2018.

FESTAG, Andreas. *Cooperative intelligent transport systems standards in Europe*. IEEE communications magazine, 52.12, 2014.

FINANCESONLINE. *70 Relevant Analytics Statistics: 2021/2022 Market Share Analysis & Data*. FinancesOnline: Reviews for Businesses 2021.

- GILLESPIE, Tarleton. *The relevance of algorithms*. Media technologies: Essays on communication, materiality, and society, 167.2014: 167, 2014.
- HUQ, N., Vosseler, R. & Swimmer M. 2017. *Cyberattacks Against Intelligent Transportation Systems Assessing Future Threats to ITS*. Trend Micro 2017. Available at: <https://www.computing.es/sitesresources/files/839/02.pdf>.
- JACOBS, S. 2014. *Researchers Hack Into Michigan's Traffic Lights*. 2014. Available at: <https://www.technologyreview.com/2014/08/19/171586/researchers-hack-into-michigans-traffic-lights/>.
- KELARESTAGHI, Kaveh Bakhsh, et al. *Intelligent transportation system security: hacked message signs*. SAE International Journal of Transportation Cybersecurity and Privacy, 1.11-01-02-0004, 2018.
- KIM, K. et al. 2021. *Cybersecurity for autonomous vehicles: Review of attacks and defense*. Computers & Security, Volume 103, 2021, ISSN 0167-4048. Available at: https://www.sciencedirect.com/science/article/pii/S0167404820304235?dgcid=rss_sd_all.
- KOLOUCH, Jan et al. *Cybersecurity*. CZ.NIC, Praha 2019, ISBN 978-80-88168-31-7.
- KOPETZ, Hermann. *Internet of things*. In: Real-time systems. Springer, Boston, MA, 2011.
- KULDA, Tomáš. *Kybernetická bezpečnost v automobilovém sektoru: Kdy budeme moct věřit svým autům?*. Pricewaterhouse Coopers Česká republika: Cyber & Privacy, 2020.
- MEEHAN, John et al. *Data Ingestion for the Connected World*. CIDR, 2017.
- NHTSA. *NHTSA and Vehicle Security*. United States Department of Transportation, 2015. Available at: <https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity>.
- NUKIB. *Hlášení Kybernetického Bezpečnostního Incidentu*. Národní úřad pro kybernetickou a informační bezpečnost, Brno, 21.2.2022.
- NUKIB. *Upozornění na výskyt nového destruktivního malware typu wiper*. Národní úřad pro kybernetickou a informační bezpečnost, Brno, 25.2.2022.
- NUKIB. *Varování před hrozbou kybernetických útoků na strategické organizace v České republice*. Národní úřad pro kybernetickou a informační bezpečnost: 2384/2022-NÚKIB-E/350, Brno, 25.2.2022.
- NUKIB. *Varování v souvislosti s ekonomickými sankcemi spojenými s Ruskou federací*. Národní úřad pro kybernetickou a informační bezpečnost: 3381/2022-NÚKIB-E/350, Brno, 21.3.2022.
- SIMCOX, Robin. *Cyber Security: Head 2 Head Debate*. Social Science for Schools. Economic & Social Research Council, 2020.

ŠKODA AUTO. 2020. *Automobilový systém řízení kybernetické bezpečnosti (CSMS) a systém řízení aktualizací software (SUMS) ve společnosti*. Koncernová směrnice Škoda Auto (with consent of the author - Jan Červenka).

ŠKODA AUTO. 2022. *Cybersecurity Strategy Automotive 2030*. Škoda Auto (with consent of the head of GQS dep. – Mr. Štický).

SMEJKAL, Vladimír. *Kybernetická kriminalita: 2. rozšířené a aktualizované vydání*. Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2018, ISBN 978-80-7380-720-7.

SMITH, Craig. *The car hacker's handbook: a guide for the penetration tester*. No Starch Press, 2016, ISBN-10: 1-59327-703-2.

STRÍTECKÝ, Vít; ŠPELDA, Petr. *Establishing the Complexity of the Islamic State's Visual Propaganda*. Central European Journal of International & Security Studies, 2017.

TRAYNOR, Ian. *Russia accused of unleashing cyberwar to disable Estonia*. The Guardian, 2007. Available at: <https://www.theguardian.com/world/2007/may/17/topstories3.russia>.

UNECE. 2021. *Addendum 154 – UN Regulation No. 155*. United Nations Economic Commission for Europe, E/ECE/TRANS/505/Rev.3/Add.154, 2021. Available at: <https://unece.org/sites/default/files/2021-03/R155e.pdf>.

UNECE. 2021. *Implementstion of UN Regulation No. 155 (Cybersecurity) – paragraph 5.3.5. – Proposal for a Resolution*. United Nations Economic Commission for Europe, Document 1, Session B, 2021. Available at: <https://unece.org/sites/default/files/2021-07/Document%201.pdf>.

UPSTREAM SECURITY. 2021. *Upstream Security Releases 2021 Automotive Cybersecurity Report*. Team Upstream, 2021. Available at: <https://upstream.auto/press-releases/2021-report/>.

URQUHART, Colin, et.al. *Cyber-Security Internals of a Skoda Octavia vRS: A Hands on Approach*. IEEE, vol. 7, pp. 146057-146069, 2019.

VOŠVRDA, Daniel. *Analýza faktorů ovlivňujících strategii firmy při vstupu na zahraniční trhy*. Diploma thesis, Škoda Auto Vysoká Škola, O.P.S., 2020.

WORTMANN, Felix; FLÜCHTER, Kristina. *Internet of things*. Business & Information Systems Engineering, 57.3, 2015.

XIA, Feng, et al. *Internet of things*. International journal of communication systems, 25.9: 1101, 2012.

8 List of Abbreviations:

IoT	Internet of Things
UNECE	United Nations Economic Commission for Europe
CSMS	Cyber Security Management System
SUMS	Software Update Management System
DDoS	Distributed Denial of Service
PPP	Public Private Partnership
AI	Artificial Intelligence
ECU	Electronic Control Unit
CIP	Critical Infrastructure Protection
OBD	On-Board Diagnostics
OEM	Original Equipment Manufacturer
LAN	Local Area Network
WAN	Wide Area Network
WiFi	Wireless Fidelity

9 List of Figures:

Figure 1: Reasons (public and private) to participate in a PPP

Figure 2: Members of the UNECE

Figure 3: Voiturette A

Figure 4: Frequency confirmation between a key fob and a car

Figure 5: Noise goal

Figure 6: List of open points to a vehicle

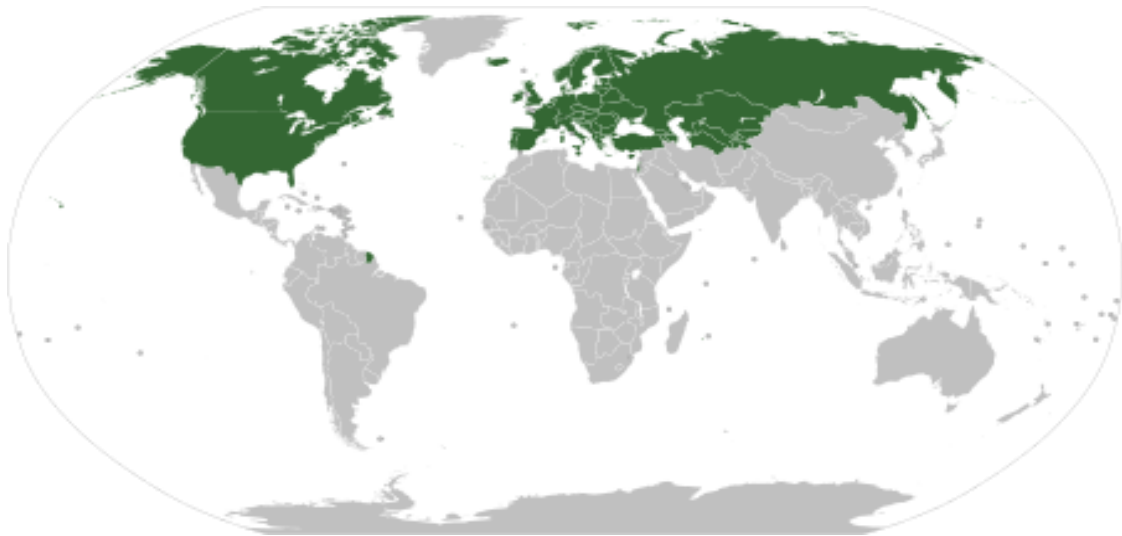
Figure 1

PRIVATE SECTOR REASONS TO PARTICIPATE IN A PPP	PUBLIC SECTOR REASONS TO PARTICIPATE IN A PPP
Access to public funds	Better understanding of Critical Infrastructure Information Protection (CIIP) and industry in general
Opportunity to influence national legislation and obligatory standards	Possibility to create synergies between different initiatives of private sector
Access to public sector knowledge and confidential information (EU legislation, fighting cybercrime)	Access to private sector resources (e.g. valuable experts), which makes it is easier to set up standards and good practices
Assurance that the products delivered through PPP are of good quality, as it is guaranteed by the government	
Sharing knowledge, experiences and good practices	
Helping to achieve resilience in the cyber ecosystem	
Increase the trust between public-public, private-private and public-private – PPP allows to meet different people and get to know them; because of that, it allows to have better information and proactive attitude in case of crisis	
Getting direct and credible contacts with other organisations	

Table 1: Motivations to participate in a PPP

Source: ENISA

Figure 2



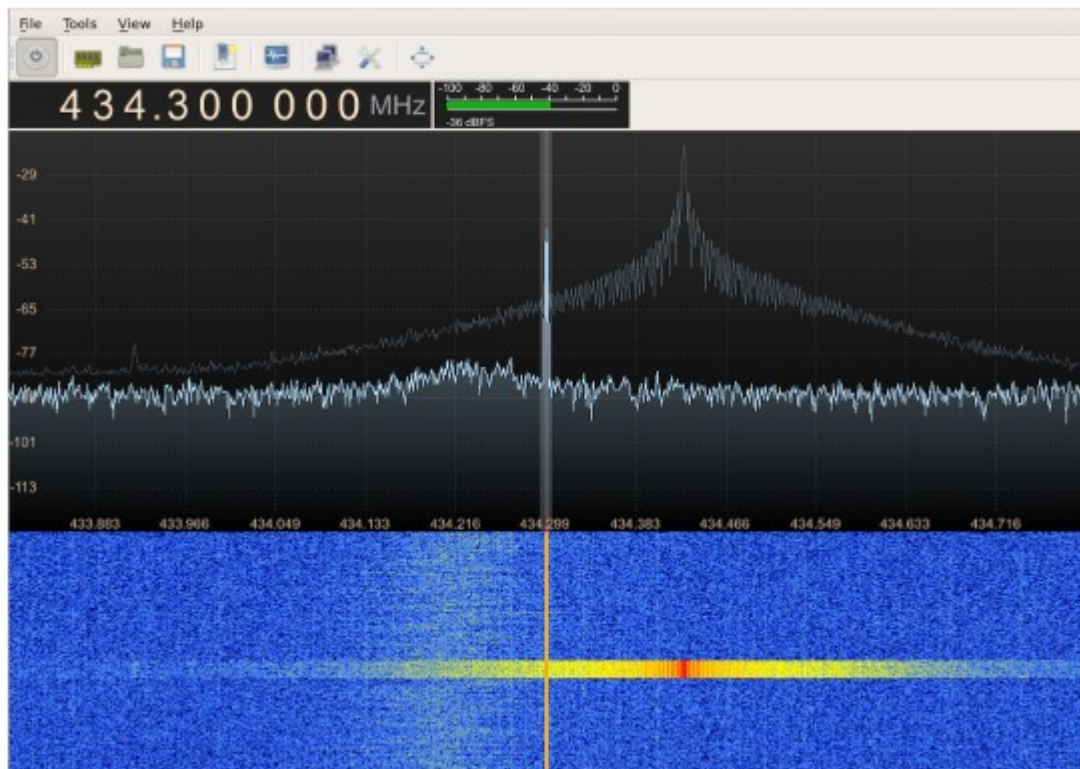
Source: Wikipedia

Figure 3



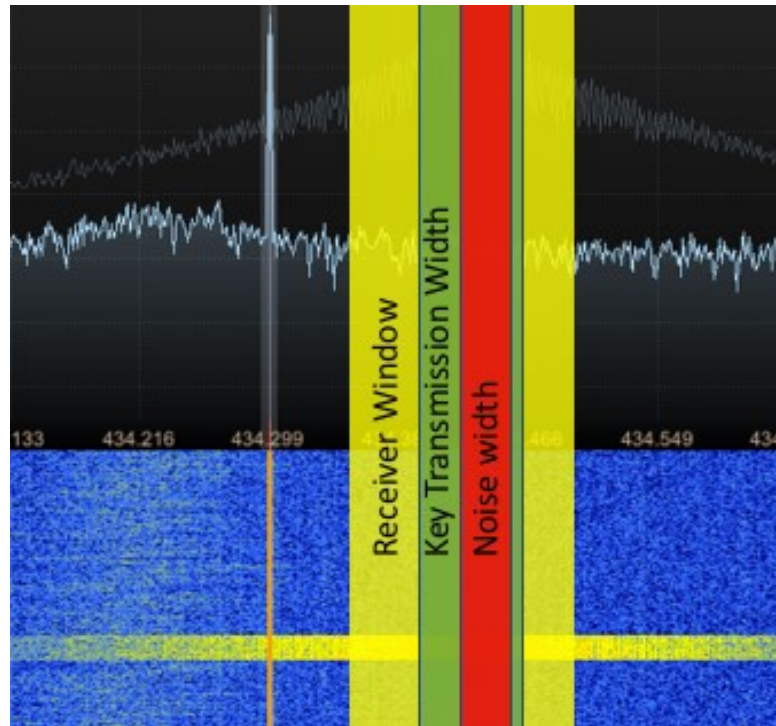
Source: Škoda Space

Figure 4



Source: Cyber-Security Internals of a Skoda Octavia vRS: A Hands on Approach

Figure 5



Source: Cyber-Security Internals of a Skoda Octavia vRS: A Hands on Approach

Figure 6

Port	Protocol	State	Name	Version
1234	tcp	open	hotline	
15361	tcp	open	unknown	
25010	tcp	open	unknown	
49101	tcp	open	sip	(SIP end point; Status: 501 Not implemented)
54321	tcp	open	unknown	

Source: Cyber-Security Internals of a Skoda Octavia vRS: A Hands on Approach

Název diplomové práce v českém jazyce:

Ekosystém Mobility Nové Generace: Nové Bezpečnostní Výzvy v Kyberprostoru

Abstrakt v českém jazyce:

Tato práce si klade za cíl představit téma kybernetické bezpečnosti v automobilovém průmyslu jako další doménu v propojeném světě. Nezachází však do technických detailů. Je to spíše návod pro širší publikum a pro ty, kteří by na toto téma rádi v budoucnu navázali a potřebují něco, s čím by mohli začít. Z tohoto důvodu práce hledá jak podobnosti, tak specifika v souvislosti s jinými doménami. Nalezením společných charakteristik v rámci propojeného světa je pak čtenář schopen zařadit téma kybernetické bezpečnosti v automobilovém průmyslu. Hlavním cílem je však najít specifika. Po úvodu a vysvětlení obecných pojmů jsou zvýrazněny parametry a jevy specifické pro automobilový průmysl. Hlavními parametry, na kterých se ukazují podobnosti a specifika, je problematika dat a spolupráce mezi veřejnými a soukromými aktéry. Měřítkem úspěšnosti této práce bude schopnost čtenáře po přečtení celého práce popsat, jaké jsou současné výzvy v automobilové kybernetické bezpečnosti a porozumět jejímu významu pro její zabezpečení do budoucna.

Klíčová slova:

Zabezpečení automobilů, Kybernetická bezpečnost, Nová mobilita