FUNDAÇÃO GETULIO VARGAS

ESCOLA DE ADMINISTRAÇÃO DE EMPRESAS DE SÃO PAULO

SIMON DÖRPINGHAUS

ARTIFICIAL INTELLIGENCE IN THE CYBERSECURITY OF GERMAN SMALL AND MEDIUM SIZED ENTERPRISES

SÃO PAULO

2019

SIMON DÖRPINGHAUS

ARTIFICIAL INTELLIGENCE IN THE CYBERSECURITY OF GERMAN SMALL AND MEDIUM SIZED ENTERPRISES

Thesis presented to Escola de Administração de Empresas de São Paulo of Fundação Getulio Vargas, as a requirement to obtain the title of Master in International Management (MPGI).

Knowledge Field: Gestão e Competitividade em Empresas Globais

Adviser: Prof. Dr. Jaci Corrêa Leite

SÃO PAULO

2019

Dörpinghaus, Simon.

Artificial intelligence in the cybersecurity of German Small and Medium Sized Enterprises / Simon Dörpinghaus. - 2019.

97 f.

Orientador: Jaci Corrêa Leite.

Dissertação (mestrado profissional MPGI) – Fundação Getulio Vargas, Escola de Administração de Empresas de São Paulo.

1. Inteligência artificial. 2. Computadores - Medidas de segurança. 3. Redes de computadores - Medidas de segurança. 4. Aprendizado do computador. 5. Pequenas e médias empresas - Alemanha. I. Leite, Jaci Corrêa. II. Dissertação (mestrado profissional MPGI) – Escola de Administração de Empresas de São Paulo. III. Fundação Getulio Vargas. IV. Título.

CDU 007.52(43)

Ficha Catalográfica elaborada por: Isabele Oliveira dos Santos Garcia CRB SP-010191/O
Biblioteca Karl A. Boedecker da Fundação Getulio Vargas - SP

Simon Dörpinghaus

Artificial intelligence in the cybersecurity of German small and medium sized Enterprises

Thesis presented to Escola de Administração de Empresas de São Paulo of Fundação Getulio Vargas, as a requirement to obtain the title of Master in International Management (MPGI).

Knowledge Field: Gestão e Competitividade em Empresas Globais

Approval Date

12/09/2019

Committee members:

_____

Prof. Dr. Jaci Corrêa Leite

_____

Prof. Dr. Julia Von Maltzan Pacheco

_____

Prof. Dr. Ricardo Ratner Rochman

INSPIRATION

"A word 'unprecedented' seems too weak to convey just how much the dimensionless operational space of digital (r)evolution requires instantaneous reaction."

Ludmila Morozova-Buss

ACKNOWLEDGEMENTS

I would like to thank my family, previous friends, and new friends I made along the journey, for all the support throughout the two years around the globe. I would also like to express my sincerest gratitude having these amazing mother, father, and sister, as well as godfather and godmother. You enabled me these amazing experiences during my master. Thank you!

I would like to express my sincere gratitude to Jaci Correa Leite, who not only inspired me during negotiation classes, but also provided me valuable guidance during the dissertation. Thank you!

Lastly, I am very grateful to all contributors during my master dissertation. Thank you!

ABSTRACT

With the recent boom in big data and the continuous need for innovation, artificial intelligence is carving out a bigger place in our society. Through its cognitive capabilities, it brings new possibilities to tackle many issues within organizations. In cybersecurity, artificial intelligent algorithms can over time autonomously mature with exposure to threats. Intelligent algorithms also raise new challenges about its use and limits. This dissertation aims to provide a better understanding of the role of artificial intelligence plays in cybersecurity for small and medium sized enterprises in Germany. The main research question that guides this study is: How can AI-enabled cybersecurity solutions, like machine and deep learning, help German SMEs fighting the increasing threat and past incidence of security breaches?

Therefore, dissertation highlights how a deep understanding of artificial intelligence and its integration in the cybersecurity process of organizations can protect companies from the increasing threat of cyber criminality. Artificial intelligence is an efficient tool to deal with complex cyber-attacks, whereas classical, linear protection methods offer limited protection. Finally, it appears that artificial intelligence in cybersecurity also has certain limitations and needs to cater to the specificities of small and medium sized enterprises.

KEYWORDS:

Artificial intelligence, cybersecurity, machine learning, deep learning, SME, Germany

RESUMO

Com o recente boom do big data e a contínua necessidade de inovação, a inteligência artificial está conquistando um lugar de maior importância em nossa sociedade. Através de suas capacidades cognitivas, traz novas possibilidades para lidar com muitos problemas dentro das organizações. Na segurança cibernética, os algoritmos inteligentes artificiais podem, com o tempo, amadurecer autonomamente com a exposição a ameaças. Algoritmos inteligentes também levantam novos desafios sobre seu uso e limites. Esta dissertação visa fornecer uma melhor compreensão do papel da inteligência artificial na segurança cibernética para pequenas e médias empresas na Alemanha. A principal questão de pesquisa que orienta este estudo é: como as soluções de segurança cibernética habilitadas por IA, como *machine* e *deep learning*, ajudam as PMEs alemãs a combater a crescente ameaça e a incidência passada de violações de segurança?

Portanto, demonstra-se como uma profunda compreensão da inteligência artificial e sua integração no processo de segurança cibernética das organizações podem proteger as empresas da crescente ameaça da criminalidade cibernética. A inteligência artificial é uma ferramenta eficiente para lidar com ataques cibernéticos complexos, enquanto os métodos clássicos de proteção linear oferecem proteção limitada. Finalmente, parece que a inteligência artificial na segurança cibernética também tem certas limitações e necessidades para atender às especificidades das pequenas e médias empresas.

PALAVRAS-CHAVE:

Inteligência artificial, segurança cibernética, *machine learning*, *deep learning*, PME, Alemanha

TABLE OF CONTENTS

Inspiration 4
Acknowledgements 6
Abstract 7
Keywords: 7
Resumo 8
Palavras-chave: 8
Table of contents 9
List of Figures 12
List of Tables 13
List of Abbreviations 14
1. Introduction 15
1.1 Subject choice 15
1.2 Background 16
1.2.1 Background in artificial intelligence 17
1.2.2 Background in cybersecurity 17
1.3 Importance and recent development 18
1.3.1 German SMEs as a target 19
1.3.2 Cyberattacks and how AI can prevent this 19
1.4 Research gap and delimitations 20
1.5 Research question and objectives 21
1.6 Outline 22
2. Literature review 24
2.1 Artificial intelligence 24
2.1.1 History of artificial intelligence 27
2.1.2 Subcategorization of artificial intelligence 29
2.1.3 Machine learning 31
2.1.4 Deep learning 32
2.2 Cybersecurity 33
3. Research methodology 35
3.1 Research approach 35

3.1.1 Background of the research approach 35
3.1.2 Shortcoming of other research methods 36
3.2 Data collection procedure 37
3.2.1 Interview guideline creation 37
3.2.2 Contributor selection 38
3.2.3 Data collection environment and timing 40
3.3 Validity and reliability 40
3.3.1 Background of the researcher 41
3.3.2 Access to interview participants 41
3.4 Data exploitation 42
3.4.1 Data recording procedures 42
3.4.2 Confidentiality issues 42
3.4.3 Data analysis and interpretation 43
4. Findings and analysis 45
4.1 Theoretical perspective 46
4.1.1 Intrusion detection systems 46
4.1.2 Response systems 50
4.2 Supply perspective 51
4.2.1 Darktrace 51
4.2.2 Finally Safe 55
4.3 Demand perspective 56
4.3.1 The increasing global threat in cyberspace 57
4.3.2 Cyberattacks on German SMEs 58
4.3.3 Specific limitations of SMEs in cybersecurity 59
4.3.4 Current status of cybersecurity at SMEs 62
4.3.5 Description of desired AI-enabled cybersecurity system 63
4.3.6 Adaption of AI-enabled cybersecurity solutions 67
5. Final evaluation 69
5.1 Summary of findings 69
5.1.1 Theoretical perspective 69
5.1.2 Supply perspective 69
5.1.3 Demand perspective 70
5.2 Comparison 71
5.2.1 Comparison between theoretical perspective and supply perspective 71
5.2.2 Comparison between supply and demand perspective 73

6. Conclusion 75
7. Contribution to research 78
8. Limitations and future research 79
9. References 81
10. Appendix 89

LIST OF FIGURES

FIGURE 1: ALPHAGO AI MADE A HIGHLY “CREATIVE” MOVE (TELEMARK, 2017, P. 88) 16
FIGURE 2: SUMMARY OF LITERATURE REVIEW (SELF-PROVIDED)..... 24
FIGURE 3: THE SKILL LEVEL OF AI IN DIFFERENT APPLICATIONS (TELEMARK, 2017, P.50) . 26
FIGURE 4: AI APPLICATIONS AND TECHNIQUES (DEJOUX & LÉON, 2018, P. 188) 29
FIGURE 5: AI SUBCATEGORIES OVER THE YEARS (NORMSHIELD, 2019)..... 31
FIGURE 6: NEURAL NETWORK (DORMEHL, 2019)..... 32
FIGURE 7: SUMMARY OF RESEARCH METHODOLOGY (SELF-PROVIDED)..... 44
FIGURE 8: VALUATION DEVELOPMENT OF DARKTRACE 52
FIGURE 9: DARKTRACE’S APPLICATION DASHBOARD (DARKTRACE, 2019)..... 53
FIGURE 10: DARKTRACE'S "ANTIGENA"(DARKTRACE, 2019) 54
FIGURE 11: AVERAGE COST OF EACH CYBERCRIME PER COUNTRY (ACCENTURE, 2018) .. 58
FIGURE 12: SUMMARY OF CONCLUSION (SELF-PROVIDED) 80

LIST OF TABLES

TABLE 1: CONTRIBUTORS SELECTION..... 39

LIST OF ABBREVIATIONS

AI	Artificial intelligence
ML	Machine learning
DL	Deep learning
MRI	Magnetic resonance imaging
IT	Information technology
SME	Small and medium sized enterprises
NLP	Natural language processing
MV	Machine vision
IoT	Internet of things

1. INTRODUCTION

The purpose of this chapter is to present the research topic to the reader by giving a short introduction to the studied subject in the light of current events, identifying research gaps in the literature, introducing the research questions considering such identified gaps, and finally providing an outline. Moreover, this passage also elaborates on the relation of different concepts under study. The introduction, more detailed than usual, is justified because artificial intelligence (AI) and cybersecurity need more development regarding their sometimes-misleading interpretation in the media, and also because of their technical aspects that tend to withdraw the reader.

1.1 SUBJECT CHOICE

The decision was to investigate a buzzing topic, that is believed to reach new heights in the coming years. Indeed, AI is considered as a disruptive technology by many stakeholders, which tends to validate the topic decision and suggests fertile ground for future research. The author is a management student about to finish his master's double degree at the Fundação Getúlio Vargas (São Paulo) in Management (MPGI) and CEMS International Management. After two exchange semesters, in Singapore and St. Gallen, and courses in data analytics as well as advanced programming languages, the author became very interested in new technologies, especially in AI. This is one of the main reasons to write the master dissertation about the use of AI, joint by the belief that it will play a significant role in the upcoming years for the whole economy in various application settings.

Considered the most impactful evolution of our age brought by the internet and technological advancement, AI is the next revolution (Brynjolfsson & McAfee, 2014). In the "Second machine age", these authors explained how an applicable and powerful AI has developed nowadays, and how AI has the potential to change the economy, the work and the everyday life in the years to come. Though personally, the victory of AlphaGo, an AI developed by Google, over the current world champion in the game "Go" let me realized that we entered a new era of AI (Google, 2016). Remarkably, the game "Go" has been considered the most challenging game ever invented, and out of reach for computer programs since it requires intuition, and substantial experience in playing (Tegmark, 2017). In other words, the computer program needed traits we thought only the human brain is capable (Figure 1). Alpha Go not

only managed to develop human traits but also won against a player with decades of training on foreign turf.

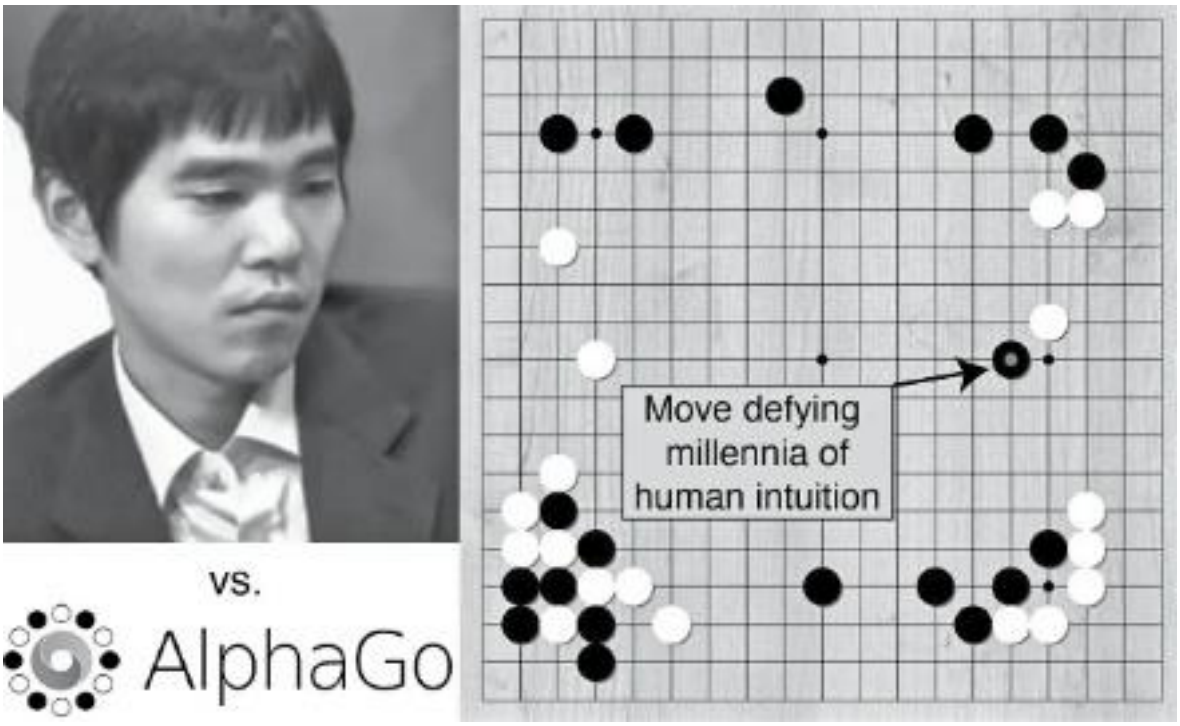

Figure 1: AlphaGo AI made a highly "creative" move (Tegmark, 2017, p. 88)

Joining the personal interest in AI, stemming from previous classes, with a specific set of companies (small and medium-sized enterprises) in a philanthropic application setting (cybersecurity), the author wants to demonstrate in this dissertation how artificial intelligence can be used for our security.

1.2 BACKGROUND

The background section provides the reader with an overview of the two main pillars of this dissertation, namely, artificial intelligence and cybersecurity. Furthermore, this section demonstrates the increasing importance to study these fields, referring to industry experts and openly available data.

1.2.1 BACKGROUND IN ARTIFICIAL INTELLIGENCE

Although AI is not new, its advancement has reached new heights for the last 15 years (Pan, 2016). Until the 2000s, the work on AI had been constrained by the limited amount of available data and the lack of noticeable practical applications. Nevertheless, today, the rise of the internet and the increase in the machine power, together with the emergence of new societal needs, have allowed a renewed interest in AI, that is sometimes called AI 2.0 (Pan, 2016), or the next industrial revolution (Dirican, 2015). Accordingly, one of the future management challenges will be to adapt organizational structures to handle change and transformation in this new digital age. That is why the author, along with most AI researchers believes that the 4th industrial revolution will be leveraged by AI. Businesses already identified the new challenge and intensify investments: the worldwide spending on AI systems is forecast to reach $35.8 billion in 2019, and it is expected to more than double to 79.2 billion in 2022 (IDC, 2019).

According to a survey by Deloitte (Loucks, Davenport, & Schatsky, 2018), 23% of the 1100 respondents ranked cybersecurity vulnerabilities as their main AI concern and investment need for the future. So, why do not we use the threat as part of the solution? Hence, using AI for our cybersecurity. Before answering this paradoxical question, the next section introduces the reader to the recent status of cybersecurity.

1.2.2 BACKGROUND IN CYBERSECURITY

During the last years, the field of security studies experienced a substantial transition from traditional security concerns to new focal points, among which cybersecurity is one of the most eminent. These new crimes in cyberspace are difficult to manage, since they represent not necessarily new types of crimes, but are happening via information technology (IT). For instance, common crimes such as theft and fraud attained a new form of cybercrimes through information technology (Yar & Steinmetz, 2019). Therefore, as technology evolves, criminal cases change correspondingly (Interpol, 2019). Consequently, cybersecurity needs to develop in the course of growing interdependence between society and cyberspace.

Alongside with the enormous advantages of digital innovations, the technological revolution of the 21st century similarly allowed for new criminal opportunities, as information technology facilitates globalization of these crimes by erasing country borders and making it much harder to monitor, detect, prevent or capture cybercriminals (Ben Naseir, Dogan, Apeh,

Richardson, & Ali, 2019). Every day we are faced with an increasing number and variety of cybercrimes, since this technology presents an easy way for criminals to achieve their goals. Therefore, the economic cost of cybercrime is high. In 2016, the cost of cybercrime for the global economy was $335 billion, and is predicted to reach $3 trillion by 2020 (World Economic Forum, 2019).

To add to the fact that cyber-attacks are alarmingly growing in amount and complexity, one of the scariest truths about cybersecurity for companies and organizations is the lack of readiness (Interpol, 2019). The issue is wider than the technical gap. Management often lacks awareness and understanding of the threat, therefore not providing the necessary support for cybersecurity. This lack of support in senior positions causes many companies the subsequent lack of drive, attention, and willingness to commit funding and resources to cybersecurity. Along those lines, it is essential to mention the lack of professionals to fill all future needs for cybersecurity positions, when companies transition and shift their focus on cybersecurity. If the current trend continues until 2021, there are approximately 3.5 million more positions needed in cybersecurity than there is available workforce (Morgan, 2017).

With the pace and amount of cyber-attacks, cybersecurity professionals are not only not available, but also simply not enough for timely attack analysis and appropriate response. The fact is that the most network-centric cyber-attacks are carried out by intelligent programs. Hence, combating them with intelligent semi-autonomous agents that can detect, evaluate, and respond to cyber-attacks will become a requirement. These so-called computer-generated forces must manage the entire process of attack response promptly and will prioritize and prevent secondary attacks in the future (Nogueira, 2011).

1.3 IMPORTANCE AND RECENT DEVELOPMENT

In this section, the dissertation covers cybersecurity and describes its recent issues in Germany, especially for SMEs (small and medium-sized enterprises), which are the backbone of the German economy. As many international successful SME are based in Germany and the researcher speaks the national language, it appeared natural to focus on Europe’s largest economy for this study.

Subsequently, scholars, new to the field of cybersecurity and the application of AI, are invited to read a short introduction on how AI can prevent successful cyberattacks.

1.3.1 GERMAN SMES AS A TARGET

In December 2018, Germany faced a severe cyber-attack, personal data relating to thousands of Germany's most influential people were published on social media by a hacker called "G0d". After a month puzzling about a potential attack sponsored by a rogue state, it turned out that a 20-year-old, working alone, was responsible for the data breach where even Angela Merkel's (Germany's chancellor) data got published. According to newspapers, the culprit was working alone and found his way by merely guessing passwords (Deutsche Welle, 2019).

However, this major scandal in Germany's national cybersecurity is just exemplary for the country's vulnerability. According to a survey of the German IT- association (Bitkom, 2018), two-thirds of Germany's manufacturers have been hit by cyber-crime attacks costing the industry about 50 billion Euros. Additionally, a study by insurance company Hiscox (2019) reveals that the companies of Europe's major economy got hit the hardest, in comparison to other developed countries. German companies were reporting more than twice the average cost per cyber-attack. The experts further specify that Germany's small and medium-sized enterprises (SMEs), the economy's backbone, were particularly vulnerable to the increasing amount of attacks. According to the latest report by the "Deutschland sicher im Netz" (2016) association, many SMEs in the Eurozone's largest economy still do not take any organizational precautions to defend against cyber-crime.

Moreover, the German middle class is particularly interesting for hackers. German SMEs are the most affected by attacks since they are worldwide market leaders, concludes the Bitkom (2018) head, Achim Berg. For example, German SMEs have many innovations in artificial intelligence (AI) and industry 4.0 (Bitkom, 2018), which makes them attractive targets for attacks, trying to steal confidential company information. Now the question arises: How can these companies use their innovativeness, for example, in AI, to strengthen their cybersecurity?

1.3.2 CYBERATTACKS AND HOW AI CAN PREVENT THIS

There were times when only trained specialist could commit cybercrimes. But today, with the expansion of the internet, almost anyone has access to the databases and tools for committing these crimes. Conventional, linear algorithms (hard-wired decision-making level) have become ineffective against combating evolving and dynamic cyber-attacks. Therefore, we need innovative approaches such as Artificial Intelligence (AI), that provide flexibility and

learning capability to software, which will assist humans in fighting cybercrimes (Nogueira, 2011; Tyugu, 2011). "*The key differentiator of this technology is that both old, previously known attacks, as well as new, previously unknown attacks, including those not yet written or conceived, are detectable. This is the power of predictive machine-learning technologies to predict the future*" (Winder, 2016).

To make this concept more vivid, the following section elucidates the differences between AI-enabled security and traditional security systems with a simplified example.

Most of the current security systems consist of rule-based systems. A rule-based system is a software that holds a list of rules, which are applied when security violations are manifesting. These rules can be updated and enriched via security updates. During a security attack, if the security system has no provisions for handling the attack, then the computer user or administrator must shut the computer down and restart it in a safe mode and find a security update to solve the issue. This situation slows down the productivity of the organization or the individual that uses the computer or the network of computers; even confidential data could be compromised already. Security attacks are also evolving at a faster rate as mentioned before, increasing the problems companies face. This situation complicates ensuring security, since most of the built-in rule-based security systems lack adaptivity to new attacks.

Now, is it possible to create a security system that is capable of learning by itself to create new security rules without waiting for security updates? This dissertation investigates the rise of cybersecurity systems based on AI methods as a possible way to provide a better level of adaptivity against the increasing threat of cyberattacks.

1.4 RESEARCH GAP AND DELIMITATIONS

As mentioned before, AI as a field of knowledge is not new, but experienced new heights in research the recent years. Articles about AI experienced a winter in the 1990s and the first decade of 2000 due to the limited storage, and power of computer, together with a lack of data (Brynjolfsson & McAfee, 2014). But, after the victory of IBM's Watson in "Jeopardy!" in 2011, and the triumph of Google's AlphaGo, our society is witnessing the emergence of useful AI, increasing the interest of the public (Tegmark, 2017). However, few researchers have focused on AI and cybersecurity. Furthermore, this research could not identify any study, focusing on the application of AI in cybersecurity for German SMEs. As found in the present

research, literature has mainly focused on the application of AI in specific industries or functions of the enterprise, until now. A growing amount of scholars conducted comprehensive research about the use of AI within a particular function of the enterprise, as in marketing (Martínez-López & Casillas, 2013), or sales (Syam & Sharma, 2018). Another group of researchers focused on a particular application of AI within the enterprise: Wang & Wang (2018) studied the contribution of AI within predictive maintenance, and Robertson, Azizpour, Smith, & Hartman (2018), who studied digital image analysis with AI. However, little interest has been granted to the way AI can impact the cybersecurity of SMEs, especially focusing in Germany. This study aims to contribute to this lack of research within the field of AI and cybersecurity. The goal is to develop a better understanding of the differences between the current state of research and the applications in business.

However, the application fields of AI in cybersecurity are vast. So, the scope of this dissertation is narrowed to enable a more in-depth analysis. According to previous research and preliminary interviews with experts, the researcher decided to focus on intrusion detection systems and autonomous response systems, whose applications are promising in cybersecurity studies. Lastly, the researcher reminds the reader that this dissertation is conducted to obtain a picture from a business perspective and accordingly elaborates on technical terms in broad strokes to enable quick understanding from a management perspective.

1.5 RESEARCH QUESTION AND OBJECTIVES

This dissertation aims to illustrate how artificial intelligence techniques can be used in cybersecurity for SMEs in Germany. The main goal is to evaluate AI-enabled systems that are capable of automatically defend computer and network systems against attacks. Not all the areas of artificial intelligence are discussed in this research. As previously presented, the subject of artificial intelligence is vast, and studying how to employ all the areas of artificial intelligence in cybersecurity cannot fit in one dissertation. Therefore, this study focuses on machine learning and deep learning, since both algorithms are the most relevant in cybersecurity. For the same reason, not all possible types of cybersecurity measures can be analysed in this dissertation. Therefore, this study focuses on intrusion detection systems and automated response systems. By evaluating cybersecurity systems that can learn how to defend companies' infrastructures autonomously, this research provides an understanding about the

new automatic and adaptive security system. This dissertation also studies the specifications of small and medium sized companies regarding AI.

The need to develop new cybersecurity solutions, joint with the versatile application and growing technical abilities of artificial intelligence, display the potential of AI-enabled cybersecurity solutions. Moreover, the emerging difficulties of SMEs in the realm of cybersecurity further stresses the need and scopes the study. As mentioned previously, research does not provide an answer to the question, how AI can support SMEs in their cybersecurity.

To fulfil the purpose of the study and to add to the current body of research, the author formulated the following research question:

> How can AI-enabled cybersecurity solutions, like machine and deep learning, help German SMEs fighting the increasing threat and past incidences of security breaches?

Furthermore, research sub-questions are developed to break down the research question:

1. What are the main challenges SMEs face when adopting AI for cybersecurity?
2. How may AI be advantageous, compared to traditional cybersecurity, fighting cyber-attacks?
3. What are commercialised and available AI-enabled cybersecurity solutions offer to SMEs?

1.6 OUTLINE

This dissertation tries to address SME's current difficulties in cyberspace, as mentioned in the introduction. The content is structured as follows: After the first introduction, the theoretical foundations are laid, using a general literature review on artificial intelligence and cybersecurity. The following chapter explains the methodological approach of this research, and further describes the research approach as best fit to answer the research question. After, this study provides the reader with the results, a summary of the findings, and a comparison

of different perspectives. This analysis is summarized in the conclusion, which also provides the reader with the contribution to the current body of research, as well as this dissertation's limitations.

2. LITERATURE REVIEW

Generally, there is extensive academic research both on artificial intelligence and on cybersecurity. Especially looking at subcategories of AI, there are many studies in the field. Therefore, in order to establish the literature review, this study narrows down the horizon on two subcategories of AI which have robust applications on cybersecurity according to literature, namely, machine learning and deep learning.

First, the literature review examines how AI is defined by the pioneering scholars. Subsequently, literature is reviewed on how the definition and application of AI developed over time from the perspective of advanced technologies and subcategories. Furthermore, as stated above, AI algorithms are examined to narrow down the broad application field. Finally, this study examines the vast literature on cybersecurity and breaks down the definition to foster understanding.

Figure 2 gives the reader a high-level chapter overview for the following literature review.

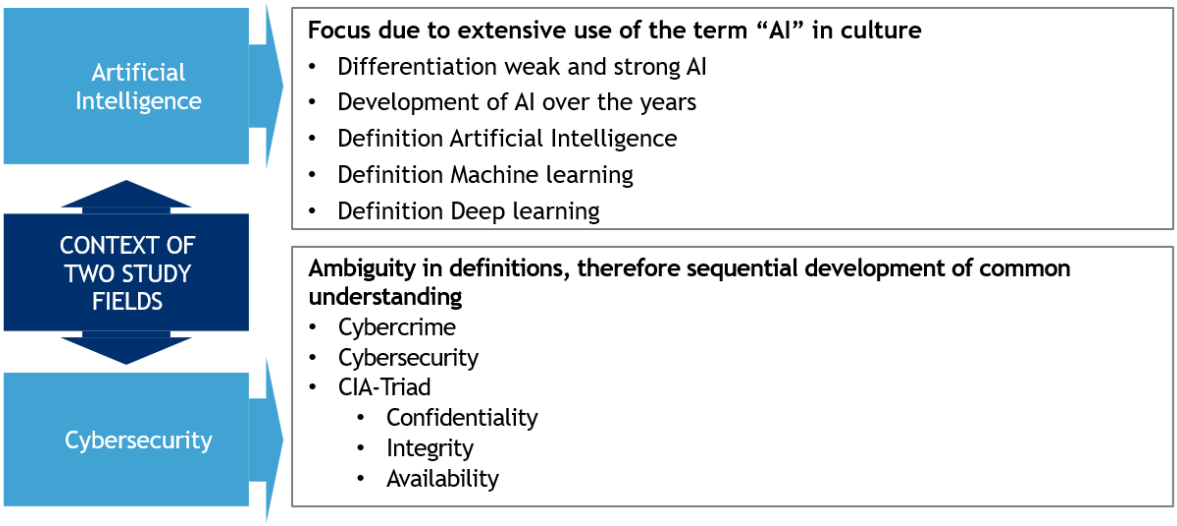

Figure 2: Summary of literature review (Self-provided)

2.1 ARTIFICIAL INTELLIGENCE

The father of AI, John McCarthy, defined the challenge of AI as "*that of making a machine behave in ways that could be called intelligent like if a human were so behaving*" (McCarthy, Minsky, Rochester, & Shannon, 2006, p. 11). In other words, AI is a machine able to think

and learn like a human being and able to perform cognitive humans tasks (Brynjolfsson & Mcafee, 2014, p. 91; Jarrahi, 2018, p. 577). Therefore, AI is a wide field of study that has evolved over time. Nevertheless, a distinction has to be made, because AI can be classified in strong and weak AI (Colby, Weber, & Hilf, 1971; Susskind & Susskind, 2015, p. 272). This typology of AI, weak and strong, has been established by the society, scientists and philosophers. Most of the time, people are afraid of the strong AI, an AI with a conscious, and tend to confuse the term with the weak AI, that exists currently.

The weak AI is present in the everyday life of people, and it includes autocorrection, chatbots, and product suggestions on Amazon. It can emulate human logic through the analysis of vast amounts of data (Jarrahi, 2018, p. 3). Thanks to sophisticated algorithms, weak AI can make precise decisions when the process of decision making is rational and can be automated, as in the sector of high-frequency trading (Brogaard, 2010). Furthermore, it can be a support to the rational decision and propose different scenarios to the decision-maker (Jarrahi, 2018, p. 3). Nowadays, most people use AI synonymous for a smarter algorithm. For instance, Amazon's (2019) Alexa, thanks to its AI algorithm, can talk with us, but in a very limited way. Sometimes Alexa is bugging or does not know what to answer to an unclear, ambiguous or complicated question. Thus, according to experts, there might be a long way to go to have a powerful and strong AI, which can interact with us like another human being (Tegmark, 2017).

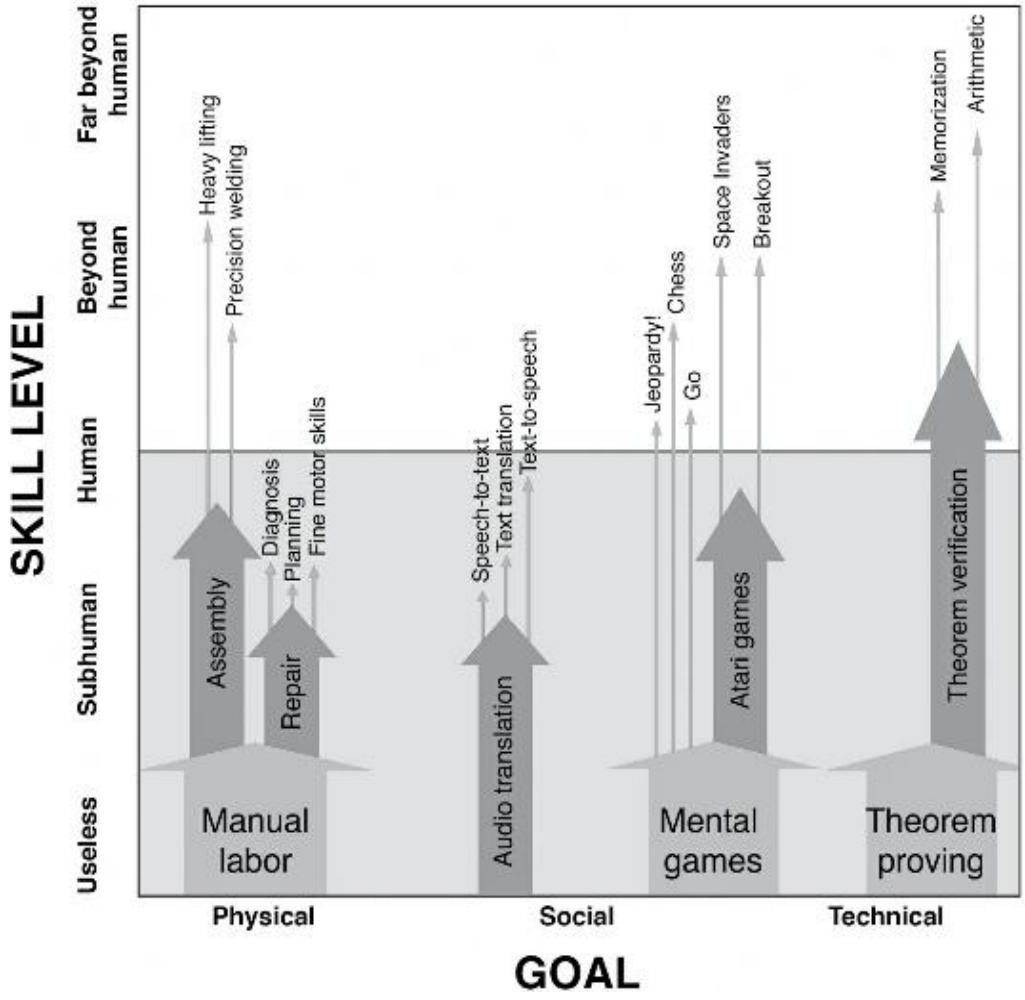

Figure 3: The skill level of AI in different applications (Tegmark, 2017, p.50)

The second type of AI, the strong AI, is defined as having consciousness and ability emulate the primary function of the human brain (Colby et al., 1971). Although this type of AI does not exist yet, the author has chosen to clarify that the AI that exists today is not close to the AI that people fear. Nevertheless, the accomplishment in specific cases is substantial, as seen in Figure 3. Strong AI divides public opinion into three central schools of thoughts. The first group sees strong AI as a non-dangerous technology that could make human beings augmented in their decision making (Stacey, Clarkson, & Eckert, 1999). Thus, firms as Amazon and Apple have already integrated AI in their structure and praise a partnership between human beings and machines with assistant systems like Alexa and Siri (López, Quesada, & Guerrero, 2017). The second school of thoughts considers a merge, an hybridization of humans, and a strong AI; the transhumanism philosophy (Dewdney, 1998). Lastly, the third school includes Stephen Hawking and warns strong AI could end humanity and take over human jobs, or

automated human tasks (Cellan-Jones, 2014). This group tackles ethical and societal debates that a strong AI raises. They further view strong AI as an enabler of an unprecedented wave of automation, and a threat for humanity as a whole. However, weak AI already has much potential for the future of work, as AI can support humans in their tasks and replace humans in routine tasks (Jarrahi, 2018, p. 2).

The distinction between weak AI and strong AI is eminent in the way machines interact with rules. In his research, Wolfe (1991, p. 1091) distinguishes rule-based decisions in which machines strictly respect the rules set by developers, from rule-following decisions in which machines follow rules that have not been explicitly stated. Conversely, rule-based decisions match weak AI, while rule-following decisions characterize the strong AI. Fully developed strong AI would be machines making their own rules and then follow them, which is not possible as of right now (Wolfe, 1991, p. 1091).

After describing the main schools and definitions of AI, a brief excursion reciting the history and development of AI over the years follows, to illustrate the recent improvements of AI. This paragraph might motivate the reader to study this emerging field in more detail because of its implication and application in various study fields and industries.

2.1.1 HISTORY OF ARTIFICIAL INTELLIGENCE

Besides the recent surge of interest for AI, the concept and technology are not new. The White House's National Science and Technology Council (2016) traces the roots of AI back to the 1940s. However, the idea of artificial intelligence was crystallized by Alan Turing (1950), in his famous paper "Computing Machinery and Intelligence". The central question posed in this paper was: Can machines think?, Turing wanted to answer using what came to be known as the Turing Test (Luger & Chakrabarti, 2017):

- It provides an objective notion of intelligence.
- It enables unidimensional focus by containing a single standard of measurement. This avoids side-tracking with questions such as whether the machine knows that it is thinking.
- It eliminates bias by centring the focus of a neutral third-party on the output.

Nevertheless, the term artificial intelligence itself was not coined until 1956, during which time three crucial meetings took place: A 1955 session on learning machines held in

conjunction with the 1955 Western Joint Computer Conference in Los Angeles, a 1956 summer research project on artificial intelligence convened at Dartmouth College, and a 1958 symposium on the mechanization of thought processes sponsored by the National Physical Laboratory (Anand, Sinha, Tiwari, & Ray, 2019).

In the beginning, the development of AI was used to solve mathematical problems, puzzles, or games. In the 1960s, however, programs were required to perform more intellectual tasks like storing information, answering questions, and creating semantic networks (Matthias, 2004).

Natural Language Processing (NLP), a fundamental prerequisite for AI-development, emerged in the 1950s and 60s mainly due to increased government funding (Morel, 2011). Natural languages were understood by the machine and translated into a language that could be used by the computer. Additionally, the 1960s also saw computer chess programs progressing slowly from beginner-level play to mid-level play.

While AI research dealt with "game" problems until the early 1970s, the focus gradually shifted to real-world issues, leading to the creation of expert systems and computer vision (Anand et al., 2019).

Described as the AI boom, the sudden increase in popularity was bolstered by Japan's Fifth Generation Computer Systems project in 1982 and Europe's ESPRIT program in 1983 (Kurzweil, Richter, & Schneider, 1990). The 1980s also saw an increasing amount of attention being paid to machine learning, which has come to be one of the most prominent branches of AI until now (Morik, 1989). During the 1980s, AI sustained as a separate industry, so that most major corporations in the US had separate groups working on AI. This can also be the reason that the AI industry had grown from being valued at a few million dollars in 1980 to a billion-dollar industry in 1988. This era was immediately followed by the AI winter, where a multitude of AI companies was unable to deliver on their earlier grand promises (Anand et al., 2019).

In recent years, a powerful and useful AI has emerged thanks to the increase of big data and technological progress in computing (Brynjolfsson & Mcafee, 2014, p. 90). AI can perform cognitive tasks that used to be human attributes, such as language processing and image recognition (Brynjolfsson & Mcafee, 2014, p. 91). Nowadays, AI applications are able to

reproduce human reasoning in a faster way and further cover vast domains such as health, finance, law, journalism, art, transport, and language (Oke, 2008).

2.1.2 SUBCATEGORIZATION OF ARTIFICIAL INTELLIGENCE

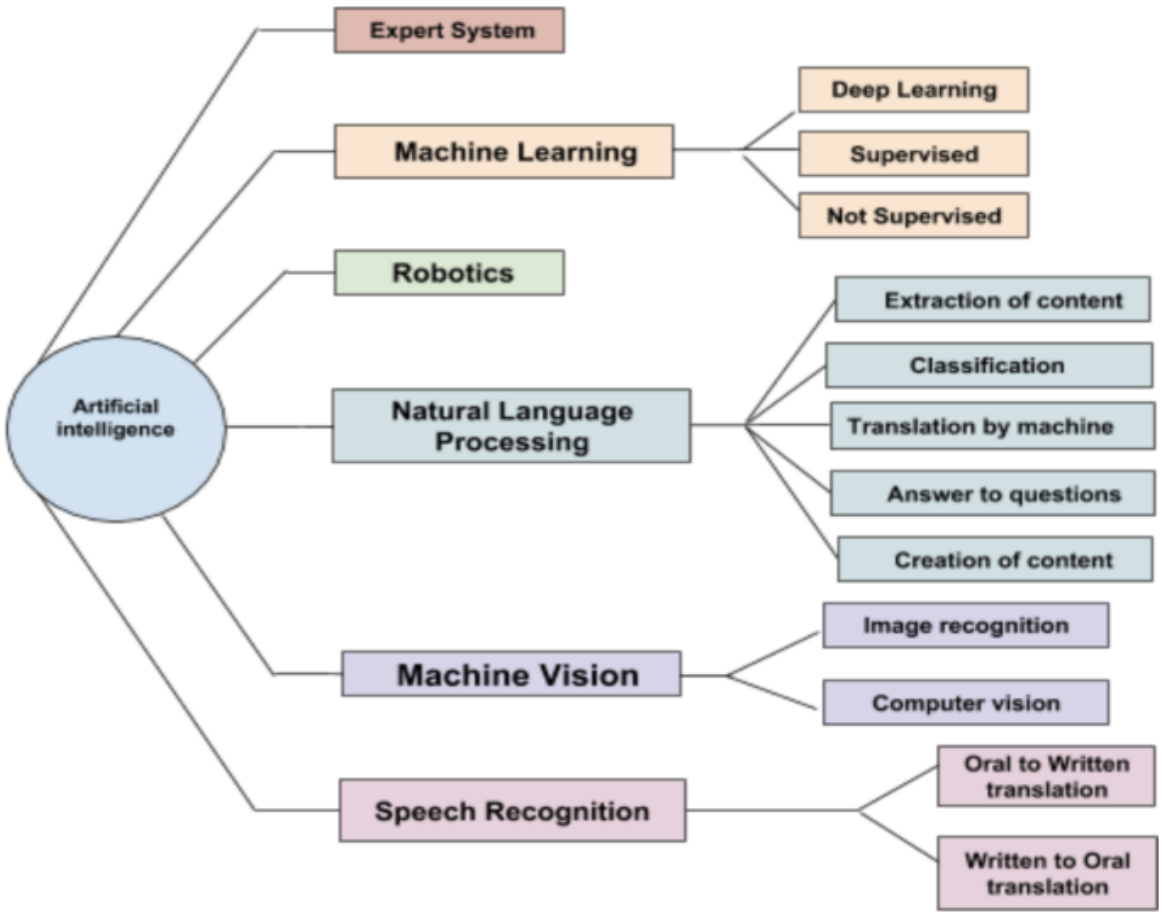

Figure 4: AI applications and techniques (Dejoux & Léon, 2018, p. 2018)

The following subcategories, structured analogously to figure 4, will give the reader a short definition of particular subcategories to provide an overview of the potential applications of AI. One of the first AI application fields in enterprises are expert systems, "*a computer system designed to simulate the problem-solving behaviour of a human who is expert in a narrow domain*" (Denning, 1986, p. 1). ML is "*the ability of a computer to automatically refine its methods and improve its results as it gets more data*" (Brynjolfsson & Mcafee, 2014, p. 91). Robotics connotes, "*a mechanical creature which can function autonomously*" (Murphy & Murphy, 2000, p. 3). NLP is defined as "*the process through which machines can understand and analyse language as used by humans*" (Jarrahi, 2018, p. 2). Machine vision (MV) has no satisfactory definition of it yet produced (Davies, 2004, p. 757), but can be described as

"*algorithmic inspection and analysis of image*" (Jarrahi, 2018, p. 2). Lastly, speech recognition technology is based by definition on NLP techniques. Figure 4 provides an overview of the main subcategories of AI.

Taking the example of IBM's Watson, AI can also combine NLP, ML, and MV techniques (Jarrahi, 2018, p. 2). Watson is an AI platform and has been developed by IBM since 2006. Watson can analyse vast amounts of data and communicate in natural language. Most remarkably NLP enabled IBM's Watson in 2011 to play and win the TV game show "Jeopardy!".

During this game, Watson did not only understand a wide range of questions and culture, but also developed an understanding of "*nuanced human-composed sentences and assign multiple meaning to terms and concepts*" (Brynjolfsson & McAfee, 2014, p. 20, 24; Jarrahi, 2018, p. 2). Moreover, in the medical field ML has allowed Watson to make decisions regarding the diagnosis of cancer, based on the analysis of previous research articles, and electronic medical records (Jarrahi, 2018, p. 2). Machine Vision has enabled Watson to analyse MRI (Magnetic resonance imaging) scans of the human brain and to detect tiny haemorrhages in the image for doctors (Jarrahi, 2018, p. 2).

As we can see in the example of Watson's application of ML on MRI scans, ML developed as a powerful tool. ML is extensively used not only for diagnostic but also in the field of cybersecurity.

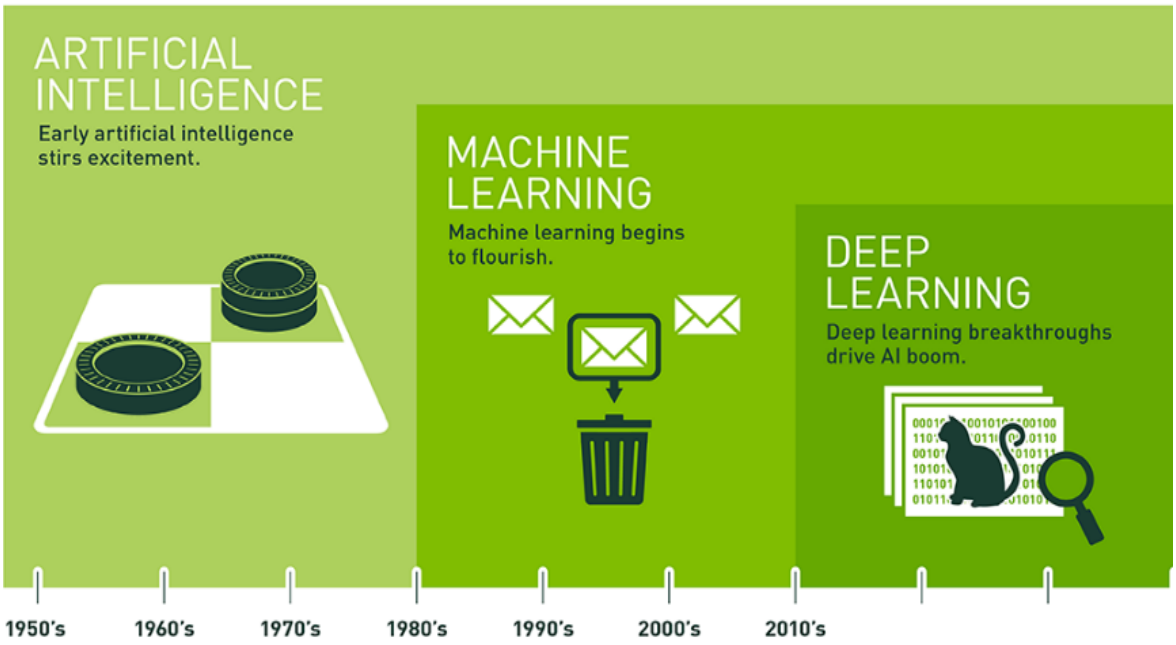

Figure 5: AI subcategories over the years (Normshield, 2019)

Within the field of ML emerged deep learning (DL), which in recent years caused enormous disruption (Xin et al., 2018). Figure 5 serves as an overview of the emergence of ML and DL. Stressing ML's and DL's importance to the application of cybersecurity, the following paragraph will elaborate on those topics in more detail.

2.1.3 MACHINE LEARNING

As stated above, ML is a subset of AI. Following the logic, all ML counts as AI, but not all AI counts as ML. For example, expert systems are described as AI, but cannot be connotated as ML. One crucial differentiation that separates ML from expert systems is its ability to modify itself when exposed to more data (Raina, Battle, Lee, Packer, & Ng, 2007, p. 1). Thus, ML is dynamic and does not necessarily require human intervention to make specific changes and is less reliant on human experts. Arthur Samuel (1988), one of the pioneers of ML, used ML to improve a computer playing checkers. The computer improved to a level which was better than its creator, so ML can learn something without being explicitly programmed. Likewise, the author defines ML as a program that adjusts itself in response to the data it is exposed to.

After its inception, ML has dramatically changed people's lives and reshaped traditional AI technology. ML can be applied in facial recognition, speech recognition, and robotics, but its application scope goes far beyond the three aspects. In cybersecurity, for example, the technology offers the potential to improve malware monitoring and intrusion detection (Li,

2018, p. 1463). Intrusion detection systems are software that monitors the system or network for malicious activity. Although ML is considered powerful, it depends heavily on feature extraction. This flaw is particularly evident in the field of cybersecurity since the input must be compiled manually, separating various features associated with malware. This is due to ML algorithms, which work according to the pre-defined specific feature set, which means that features which are not pre-defined cannot be detected by the algorithm (Li, 2018, p. 1463). This certainly limits the efficiency and accuracy of threat detection.

In the light of practical difficulties, researchers began to study deep learning (DL), also known as a deep neural network (DNN), as sub-domain of ML.

2.1.4 DEEP LEARNING

Deep learning (DL) is a subset of machine learning (ML). In research, people use the term deep learning interchangeably to deep neural networks (DNN). In order to understand deep neural networks, this paper first introduces the concept of neural networks. Neural networks consist of input and output layers, as well as a hidden layer transforming the input into something that the output layer can use (Figure 6) (Jain, Mao, & Mohiuddin, 1996). Artificial neural networks are one of the main tools used in machine learning. As the word “neural” suggests, the concept is inspired by the human brain and intents to replicate the way human learn (Dormehl, 2019).

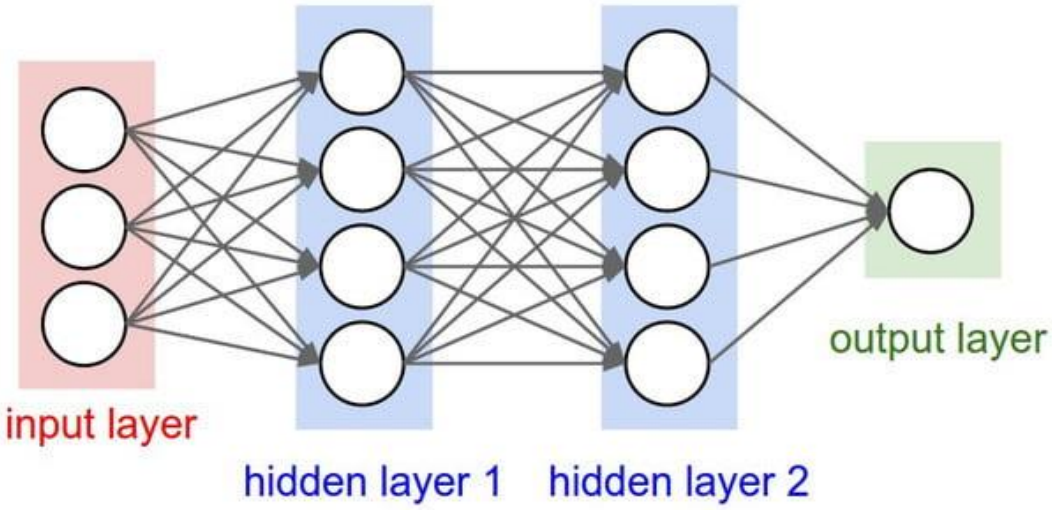

Figure 6: Neural network (Dormehl, 2019)

Regarding deep neural networks or deep learning, deep is used as a technical term. It refers to the number of layers in a neural network. A shallow or usual network has one hidden layer, but a deep network has more than one. Multiple hidden layers allow deep learning to extract features of the data in a so-called feature hierarchy. As an illustration, DL can recombine simple features (e.g., two pixels) from one layer to the next, to form more complex features (e.g., a line). DL solves the issue of manual feature extraction as identified in the previous passage and inputs can be directly used to train the original data without extracting its features (Deng & Yu, 2014).

2.2 CYBERSECURITY

Although it is theoretically possible for organizations to manage their affairs without the use of modern technology, few managers choose to do so. Given the availability and low cost of IT to collect, manage, and share data, modern companies leverage IT to remain competitive within their industry. The degree to which information technology and cyberspace brought freedom, it similarly gave rise to security threats that can be used against the very same user. Some of the risks are demonstrated in the form of data breaches and the leakage of sensitive information, as mentioned in the introduction (Topic 1.2.2). Given that computer threats may cause widespread disruption to enterprise stability, cybersecurity or computer security (interchangeable use in this dissertation) has evolved to a pressing need for organizations (Acuña, 2016, p. 38). Cybersecurity is a nascent field with a growing body of research (Lingenheld, 2015). It is rooted in traditional computer science but has recently gained prevalence in other fields such as law and business management, as well as areas of technology that did not initially operate with the internet.

Due to the broad scope of cybersecurity, it is also "*a broadly used term, whose definitions are highly variable, often subjective, and at times, uninformative.*" (Craigen, Diakun-Thibault, & Purse, 2014, p. 1). Thus, we first introduce the definition of cybercrime, which has descriptions more agreed upon, and subsequently develop a shared understanding and definition for cybersecurity.

Gordon and Ford (2006, p. 14) defined cybercrime as "*any crime that is facilitated or committed using a computer, network, or hardware device*" where "*computer or device may be the agent of the crime, the facilitator of the crime, or the target of the crime*". However, not

all offenses committed in cyberspace are covered by the term cybercrime, as among the most prominent are cyber-warfare and cyber-terrorism. Thus, this dissertation further refines the definition to ensure clarity. Since this academic study uses the angle of a business perspective, this dissertation solely covers the term cybercrime from a financial perspective, which refers to cases where technology is used in the commission of crime which is often financially motivated and encompasses different concepts of varying levels of specificity (Jahankhani, Al-Nemrat, & Hosseinian-Far, 2014).

Coming from the definition of cybercrime to the definition of cybersecurity. In their paper, Schatz, Bashroush, and Wall (2017, p. 53) already acknowledged the little understanding in the current literature on what the term "cybersecurity" really entails. Their final definition of cybersecurity, joining multiple definitions in current literature, is: "*The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity, and availability of data and assets used in cyberspace*" (Schatz et al., 2017, p. 66).

This definition is further explained with the following definitions and is widely known as the CIA-Triad (Randrianasolo, 2012).

- Confidentiality: Confidentiality means preventing unauthorized parties from knowing and accessing information in the computer system (Medvidovic & Taylor, 2010). The term secrecy is used interchangeably with confidentiality (Randrianasolo, 2012).
- Integrity: Preserving integrity means only authorized parties can access information (Medvidovic & Taylor, 2010). This imposes creating user identifications which will be checked at different levels before granting access authorizations.
- Availability: A requirement intended to assure that systems work promptly, and service is not denied to authorized users (Guttman & Roback, 1995).

3. RESEARCH METHODOLOGY

The purpose of this chapter is to present how the research is conducted. First, it is necessary to explain the overarching research approach and why this dissertation uses a qualitative approach through interviews. Second, to ensure a seamless and objective research paper, clear study design and data collection procedure are established and explained. Third, the validity and the reliability of the research are reviewed. Last, this chapter reflects on the data gathered during the study and how it is exploited.

3.1 RESEARCH APPROACH

This paper hypothesizes that it is difficult to obtain reliable insider knowledge on cybersecurity issues of SMEs in Germany, because these market participants do not want to share the information which can put the organization's security at risk. It is further hypothesized that the knowledge is retained inside the company to vail potential vulnerabilities for attackers. Consequently, there is no numerical data openly available, which can be analysed to answer the research question posed in this dissertation. According to this hypothesis, this Master dissertation uses a more qualitative approach, leveraging interviews.

Since this study is qualitative, it presents the core characteristics of qualitative studies as presented by (Creswell, 2013). The researcher collected field data from multiple interviews in a natural setting as well as documentary research, outside sources, and documents to support the argument of this dissertation.

3.1.1 BACKGROUND OF THE RESEARCH APPROACH

Following the hypothesis mentioned above, the most direct way to obtain reliable information is to ask relevant market participants. This qualitative study, therefore, emphasizes on the data that is obtained through interviews and develops on the literature review of chapter two. Considering that the subject of cybersecurity for SMEs in Germany is not covered academically to the authors best knowledge, there is no available dataset or other external quantitative sources that can be used to study the topic further. Consequently, conducting interviews seems the most fitting choice.

Interviews can be conducted face-to-face, by telephone, in focus groups, or via e-mail (internet interview). As the author writes the dissertation in Brazil, interviews need to be conducted remotely, since relevant participants reside in Germany. Before the interviews, the connection over the telephone line was tested, because of the long distance between Brazil and Germany. Subjectively, the acoustic quality and the understanding suffered using standard telephone lines. After multiple testing calls, voice over IP offered better acoustic quality and hence understanding over the long distance. More specifically, most research participants suggested interviewing via Skype (2019), mostly because of no additional cost. Finally, the researcher tries to engage the interviewee in a conversation, learn as much as possible from the contributors, and attempts to guide the conversation into the area the interviewee is most comfortable sharing information.

In summary, a qualitative research approach using interviews represents the most solid methodology for this study and is used because of multiple reasons. For a better understanding, this paper subsequently describes why other research forms are not adding more insights than the chosen approach described above.

3.1.2 SHORTCOMING OF OTHER RESEARCH METHODS

As stated above, other research methods prove not to be appropriate for this dissertation. Indeed, a quantitative approach could benefit this study, which might compare AI cybersecurity measures (implemented or not) with the number of data breaches, costs incurred as a result of cyber-attacks, or the number of cybersecurity experts needed. Two obstacles prohibited the author from finding publicly available data concerning cybersecurity of German SMEs. First and most important, companies do not share their security measures and do not want to share their cybersecurity strategies, thus becoming an easy target for hackers. Second, the author considered to use financial statements and other information, SMEs are obliged to report to the public. However, the German commercial code requires firms based in Germany to make information available progressing with size (Ebenroth, Boujong, Joost, & Strohn, 2014). Therefore, larger companies need to make more information publicly available measured by their revenues, balance sheet total, and the number of employees. As the term small and medium-sized companies indicates, the size of the research subject is by definition the smaller companies, and therefore has few public information available. So, this source of information can be discarded, because a comparison does not yield representativeness when there is not the same amount of data available.

Therefore, a quantitative analysis is not feasible in this research context, and a qualitative analysis is preferred.

3.2 DATA COLLECTION PROCEDURE

For this dissertation, the data collection procedure design ensures the integrity of the study to add to the academic knowledge on the topic. In other words, a framework was developed to collect data as objectively as possible. Therefore, the author developed a questionnaire (Appendix) to collect the field data scientifically.

3.2.1 INTERVIEW GUIDELINE CREATION

As previously stated, this qualitative study identifies interviews as a method for collecting data. In that case, multiple questions must be created. These questions, included in the interview guideline, were developed before the data collection started, which ensures that the questions remain the same throughout the whole process to guarantee comparable data collection across all interviewees.

During the interview guideline creation process, two significant specificities were addressed to create an academically sound, but also useful data collection procedure in practice.

One specificity is that people in the study do not share the same profiles. As this dissertations hypothesis is that most SMEs in Germany do not use artificial intelligence yet, but need to develop their cybersecurity infrastructure, most knowledge about the use-cases cannot be generated by solely interviewing SMEs. Therefore, this study touches multiple players within the ecosystem (more information is provided in “selection of contributors” the following topic). In this case, it is challenging to develop a questionnaire which fits all participants. Hence, a more adaptable solution with a standardized part, asked to all participants, was created to ensure reliability and a customized part, asked specific participants with specialized knowledge, was developed to get specific insights for this academic paper.

Most interviews were conducted during office hours in a limited time frame. In consequence, the questions had to be as concise as possible and kept to a minimum. Especially regarding the safety requirements in the cybersecurity industry, participants had the liberty to answer or refuse questions. Moreover, participants were encouraged to follow their thoughts, as these

experts have most insights on the subject matter. One drawback of this method is that some interviews could not touch all questions, but deeper insights obtained in other questions offset this drawback.

Thus, these interviews were semi-structured, since they rely on an interview protocol (Appendix) prepared previously (Creswell, 2013), and the main research question and sub-questions (Section 1.5). The interviews were conducted, as preferred by the participants, in German to foster a natural environment for the German study participants.

3.2.2 CONTRIBUTOR SELECTION

As stated in the title of this dissertation, the main research subjects in this dissertation are SMEs. Therefore, this dissertation is meant to gain the most insights directly from the research subject. However, during preliminary discussions and research, it became apparent that SMEs represent the "demand-side" or final user of the AI-enabled cybersecurity solutions in the cybersecurity ecosystem. Hence, other participants in the ecosystem have a significant influence on the cybersecurity options available and consequently on the SMEs. As a result, this dissertation broadened its horizon to enable a comprehensive overview of AI-enabled cybersecurity for SMEs. Within the ecosystem, this dissertation includes interviews from the supply perspective of AI-enabled cybersecurity (software providers), the demand perspective (SMEs), and support function (business associations of official institutions which support SMEs' in cybersecurity). The author finally wants to highlight that SMEs remain the foremost focus, which can be seen in the relative share in the list of contributors (4/6 interviews). It needs to be further noted, that most official governmental institutions and software providers refused to give interviews. Regarding governmental institutions, the researcher received often the answer, that the information which can be shared is available online, and that further information cannot be provided. Therefore, the researcher is happy to conduct one interview and gathered the remaining information from the, indeed, vast information pool on official governmental websites. Regarding software providers, the main problem is that there are a few, offering their services in this still young industry. Therefore, the researcher is pleased to conduct an interview with the only German corporation, providing AI-enabled cybersecurity. Since this corporation represented the only German company in this niche, the data is representative for Germany.

Each study participant was previously researched and gathered in an Excel sheet, containing the date, the last contact, as well as the function within the ecosystem. During the identification of contributors, it was imperative to get participants with different positions in the ecosystem (i.e., Supply, demand, or support side).

From the point of reaching out to potential participants to conducting the interview, the most crucial part lies in convincing professionals to incorporate a timeslot for an interview in their tight schedule. Understandably, some potential participants refused because of their full calendars. Furthermore, the cybersecurity industry is notorious for withholding information, because of security reasons. Sharing information about the security systems can make companies vulnerable to hackers, who can use this information to exploit vulnerabilities in the security systems. Therefore, the researcher is happy to have interviewed four SMEs, which shared their view on the subject.

Refer-ence in text	**Staff number**	**Industry**	**Yearly Reven-ues in Million**	**Official position**	**Years of expe-rience**	**Part of eco-system**	**Inter-view date in 2019**	**Length of interview (H:M:S)**
1_SME	100-250	Industrial goods	50-200	Head of IT	10	SME	24.07	1:16:10
2_SME	50-100	Consumer goods	25-50	CEO	36	SME	25.07	1:03:02
1_Softw are	5-10	Cyber-security	0,5-50	Head of advanced threat protection	14	Software provider	29.07	0:57:29
3_SME	20-40	Advisory	10-100	CEO	33	SME	31.07	0:34:52
4_SME	5-10	Advisory	0,5-50	Cyber-security consultant	28	SME	01.08	1:13:08
1_Asso ciation	100-200	Industry Association	ND	Head of security politics and defence	16	Digital association	02.08	0:43:13

Table 1: Contributors selection

Creswell (2013) set the sample size for a phenomenological qualitative study from three to ten interviews, with different individuals. This study conducted six interviews and is in the middle of the scale. Another guideline of Charmaz (2006) indicating the right amount of interviews specifies that the study does not need to collect more data when a topic has been saturated. Accordingly, this study contains six interviews, while the researcher has been attentive that each new contribution adds value to the overall study.

The interviews were conducted in German to foster open conversation with the study participants who are based in Germany. This enabled longer and more in-depth conversation, as it can be seen in table one, lasting on average far longer than the intended 30 minutes.

In summary, the contributor selection in this study has been laid out. Additionally, to be comprehensive, the next topic explains how the data has been collected in terms of data collection environment and timing.

3.2.3 DATA COLLECTION ENVIRONMENT AND TIMING

As already mentioned, the professionals contributing to the study are generally quite busy. Hence, all interviews were conducted via voice over IP, since this method provides more leeway to reschedule and most importantly enabled conversations over a long distance. The fact that the interviews were conducted remotely does not seem to affect the insights gained in the study, it instead enabled more flexibility, which was also appreciated by the participants and reduced the barriers for participation. All participants were alone, undisturbed when attending the conversation. Therefore, the environment was the same for each participant.

Regarding the time of the year, the interviews took place in July and August of 2019. Moreover, most interviews were conducted in the afternoon in the participants' time-zone.

Finally, this dissertation aims to create an objective data collection procedure to ensure academic standards for this research.

3.3 VALIDITY AND RELIABILITY

As stated above, the research approach consists of interviews with professionals working with the cybersecurity of SMEs. For a scientific paper, it is therefore imperative to guarantee

objectivity and consistency during the data collection. So, this section describes the methods used to ensure validity and reliability in this study.

3.3.1 BACKGROUND OF THE RESEARCHER

Before writing this dissertation, the researcher had no professional experience in cybersecurity. Most of the knowledge and previous exposure in this realm is limited to academic papers and books. Therefore, the researcher is not biased in terms of previous industry knowledge.

However, the researcher worked three years during an apprenticeship as an industrial management assistant in an SME, which is a “hidden champion” (relatively small but highly successful companies) in the paper industry in Germany. In the course of the apprenticeship, the researcher went through each function within the company and learned about the pain points of smaller enterprises. This knowledge allowed a better understanding of the processes in smaller corporations and facilitated a seamless flow in the interviews, and, moreover, gave certain credibility around the project. Furthermore, participants felt that the researcher knows the pain points of SMEs and shared more insights during the interview process. Therefore, the background of the researcher shows no potential for biases, but rather enabled access to valuable insights and enhanced communication.

3.3.2 ACCESS TO INTERVIEW PARTICIPANTS

This dissertation had no real gatekeepers that enabled access to multiple interview partners. Most participants were contacted via cold calling or e-mail, which were stated on the company’s website. Some contributors were accessed by referral or previous contact. To facilitate the process, since some German companies were suspicious about a request from a foreign country regarding cybersecurity, the researcher made use of his work and academic credentials to convey professionalism and gain the trust of potential contributors. The researcher, therefore, ensured an unbiased research procedure during the contact and the access process of interview participants.

3.4 DATA EXPLOITATION

It is imperative to document the most relevant insights of the data collected during the interviews and to obtain this, the methodology is described in this section.

3.4.1 DATA RECORDING PROCEDURES

The most comprehensive way to enable further studies and provide a detailed view of the gathered data is to include the transcribed interviews in the appendix. Nevertheless, the interviewers would remain anonymous with all names censored. However, the contributions were very rich and reached very far in internal data. This knowledge can be exploited by hackers. Therefore, no transcriptions are published alongside this dissertation.

The interviews were mostly audio recorded to facilitate more straightforward data analysis and interpretation. Therefore, interviewees were asked before the interview to give their consent, that the interview is recorded. Fortunately, most participants agreed to audiotape the interview. To further reinforce the non-disclosure of the contributor's company insights, the author will delete the recordings after finishing the dissertation or latest, the last day of the year 2019.

Moreover, live notes were taken to highlight the most critical data points accurately during the conversation. These notes were recorded on a computer and will be discarded alongside the records, at the end of the dissertation or latest, the last day of the year 2019.

These measures are necessary when it comes to information safety in cybersecurity. Most interview participants, who studied and learned about cybersecurity are trained to leave few data trails and minimize available information about their security systems.

3.4.2 CONFIDENTIALITY ISSUES

At the beginning of the interviews, the researcher presents his work by explaining the research question and the current status from previous interviews. The background of the study was already laid out in a previous email, which contained the research background, the interview guideline and the consent for recording. Nevertheless, the researcher reinforces the written information orally when starting the interview to give more context.

In the course of the conversation, some participants mentioned information they might share in a conversation, but do not want to make public. When an interviewee mentioned that the respective information should be “off the record”, the researcher reinsured which part should not be published and excluded this part from the study. As already mentioned, cybersecurity experts are generally aware of the information that can be used to exploit cybersecurity vulnerabilities. The researcher understands this confidentiality issue and does not share information when explicitly asked to refrain from publishing it.

3.4.3 DATA ANALYSIS AND INTERPRETATION

As above mentioned, during the interviews, the discussions were recorded, but in order to make sense of the data, notes were taken to be able to highlight the most critical data points accurately. As mentioned in the contributor selection (Topic 3.2.2), every interview enhanced the final results. It was possible to touch the most relevant themes during the data collection. When all interviews were conducted, the final data analysis consisted of going through the notes again and complete them by using the recordings.

Across interviews, the emergence of similar topics was observed. The emergence of topics in common during the interviews, joint with the literature review enabled a structured and detailed analysis under common topics. After the clustering, it is feasible to work with the data and interpret it more analytically. This interpretation and analysis (Chapter 4) can go beyond pure paraphrasing interview passages to a more liberal, high-level analysis finding overarching relations of the topics. However, the researcher wants to provide the reader with primary data. Therefore, excerpts from the interview are inserted in the text. It is further noted that interviews were conducted in German and that the quotes are translated from German to English.

This chapter laid out the guiding principles to ensure a scientific processes and replicable results as summarized in figure 7. The next chapter provides the reader with the actual findings.

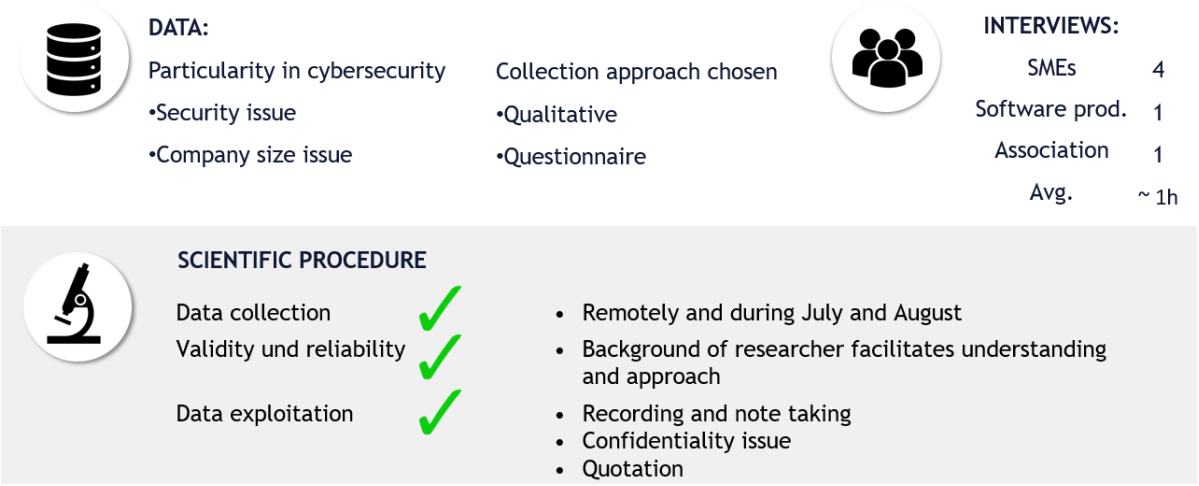

Figure 7: Summary of research methodology (Self-provided)

4. FINDINGS AND ANALYSIS

The interviews were conducted according to the methodology presented before. As stated in the introduction and literature review, the application of AI in cybersecurity is still mostly unexplored. Therefore, it is necessary to start from the very beginning and elaborate on the potential applications of AI for SMEs. As stated in the literature review (Section 2.1), AI enables us to design autonomous computing solutions, capable of adapting to the context of use, leveraging methods of self-management, self-tuning, self-configuration and self-diagnosis. When it comes to the future of cybersecurity, AI techniques seem an up-and-coming area of research, that focuses on improving the security measures for cyberspace (Dasgupta, 2006; X. Wang, Yang, Li, & Liu, 2008). In times when hackers are growing in numbers and abilities, traditional approaches of cybersecurity seem to start hitting their limits. Now, most of the machinery evolves and is connected to the internet (Industry 4.0), which increases the potential cyber vulnerabilities or as one of the interviewees put it well:

> If I can control my machines and equipment remotely, hackers have, in theory, the ability to do the same [4_Software].

Thus, there is a need to test new approaches, which might increase the cybersecurity of corporations. Therefore, the ambition of this dissertation is to provide an answer to the research question (Section 1.5): How can AI-enabled cybersecurity solutions, like machine and deep learning, help German SMEs fighting the increasing threat and past incidences of security breaches? This section creates a foundation for answering this question and is split into three parts.

First, this paper gathers information on potential applications of AI in cybersecurity according to research and experts (Section 4.1), elaborating on the research sub-question: How may AI be advantageous, compared to traditional cybersecurity fighting cyber-attacks?

Second, already commercialized AI-enabled cybersecurity solutions in the software market are analysed. Hence, two products that are currently offered, commercialized, and available for SMEs are studied (Section 4.2). The second part of the results, therefore, elaborates on the research sub-question: What are commercialized, and available AI-enabled cybersecurity solutions offer to SMEs?

Last, SMEs' competences and experiences in AI-enabled cybersecurity solutions are studied during the interviews, and specific requirements of AI-enabled cybersecurity solutions are

extracted (Section 5.3). This part, thus, elaborates on the research sub-question: What are the main challenges SMEs face when adopting AI for cybersecurity?

4.1 THEORETICAL PERSPECTIVE

As mentioned above, this section studies the potential applications of AI in cybersecurity according to research and experts. Within the subject, this part focuses specifically on the intrusion detection systems (IDS) and response systems, as one interviewee supported the claim that AI has strong potential in these two areas.

> AI has strong potential when it comes to intrusion detection and the response to cyber-attacks [1_Software].

4.1.1 INTRUSION DETECTION SYSTEMS

As mentioned in the literature review (Section 2.2), an intrusion detection system is a software that monitors the system or network for malicious activity. Security breaches include external intrusions and internal intrusions. If malicious activity is registered, it will be reported to the administrator. As of now, detection techniques fall into two categories, signature-based and anomaly-based systems. These two techniques provide the current base for cyber-defence in all companies interviewed. However, they fall short of detecting complicated or sophisticated new attacks, which have not been seen before. In order to remain comprehensive, there are also hybrid detections systems, which are, as it can be inferred from the name, only hybrids of both basic detection techniques (signature- and anomaly-based) and are thus not part of the further analysis. The following part, therefore, studies the signature-based, anomaly-based, and AI-enabled IDS.

Signature-based detection systems rely on existing databases of known threats to detect invasion. For example, traditional security solutions such as firewalls and virus scanners mostly use a signature-based approach. These systems examine incoming data and retrieve the signatures. Subsequently, the system compares the signature of the incoming data with a database of previously identified malicious signatures. If the data package matches with a signature, the system assumes that an intrusion has been detected. Hence, these systems are used for known types of attacks and are an effective method to detect intrusions that have been

previously detected, without generating many false alarms (false-positives). These signature-based detection systems require frequent manual updates of the rule and signature database to obtain comprehensive security. However, the most critical vulnerability of these systems is the detection of novel (zero-days) attacks, or a variant of an existing attack, also known as a mimicry attack. Therefore, they are not a sufficient guard against skilled attackers who use the latest attack methods and exploits (Buczak & Guven, 2015).

Other detection systems are grounded on **anomaly-based** detection. Unlike signature-based detection systems, anomaly-based detection systems indicate intrusions or intrusion-attempts by assessing the behaviour in a network. This technique observes the normal network behaviour and the actual system behaviour and identifies anomalies as deviations from normal behaviour. In order to detect new threats, the administrators need to create protocols as validators to detect anomalies. Those protocols determine what normal or legitimate network traffic resembles. Therefore, the anomaly-based systems rely on the administrator to create new rules and cannot find an intrusion if the rule that could detect it is not established. The main disadvantage of anomaly-based techniques are high false alarm rates, because previously unseen, but legitimate, system behaviour can be categorized as anomaly. However, one advantage of anomaly-based detection systems is attributed to their capacity to detect novel (zero-day) attacks. Another advantage is that the rules for normal or abnormal activities can be customized for every system, application, or network, therefore making it difficult for attackers to know which activities remain undetected (Jose, Malathi, Reddy, & Jayaseeli, 2018).

When it comes to automated cybersecurity, products which solely scan signatures are not **AI,** but mere patching. Similarly, anomaly detection which is solely based on rules is not intelligent, but rather rule execution. However, it is recommended to be cautious, especially when vendors try to oversell their tools with the term AI. Thus, it is essential to delineate between products that have rules-based detection engines and ones that leverage true AI, since some vendors with thousands of rules feel they have accomplished a version which is almost AI. Real AI algorithms nonetheless enable some fundamental shifts from signature-based detection to a flexible method that understands standard, or normal network activities. Like anomaly-based detection, AI algorithms can detect abnormal behaviour, but without requiring previous rule definition. In general, these AI algorithms require extensive training sets and improve over years of deployment.

As mentioned in the literature review (Topics 2.1.3 and 2.1.4), ML focuses on classification and prediction, based on features and properties learned from the training data. DL is a new field, where neural networks simulate the human brain for analytic learning. Additionally, DL methods are based on the characterization of the learned data, where each layer in the network abstracts the input even more.

In cybersecurity, **ML** learns from previous experience and detects threats when it observes deviations from the past. So, every ML algorithm uses previous patterns to make decisions on new emerging patterns (pattern recognition). Applying this method to ML-based intrusion detection systems, researchers can increase detection rates for new intrusions that did not happen before (Jean-Philippe, 2018). To give an example, if a new malware manages to enter the system penetrating the firewall and intends to spread and encrypt files, the ML-based IDS can detect and prevent the process on devices across the network.

In cybersecurity, **DL**, including artificial neural networks, is capable of recognizing patterns that are too complex for humans to recognize. Moreover, DL can process a large amount of data, which makes it useful for intrusion detection systems, since these systems skim through vast amounts of data. Even unclassified datasets, without previous feature extraction, can be used to perform calculations and determine a threat. Before determining if the data belongs to a threat, the DL-enabled intrusion detection system calculates the errors in addition to the results it expects (Qu, Zhang, Shao, & Qi, 2017). For instance, some intruders use botnets, that launch Distributed Denial of Service (DDoS) attacks. Since many bots are attacking the network, the traditional intrusion detection system can generate large numbers of false alarms, which distract cybersecurity experts from finding real threats. DL-enabled cybersecurity is the network administrator's help to filter out false alarms and increase real detections rates.

As stated above, AI-enabled intrusion detection systems offer several advantages to traditional cybersecurity systems, like signature and anomaly-based detection methods. At the same time, it is essential to distinguish between ML and DL. As already mentioned in the literature review (Topic 2.1.2), DL and ML are preferred on different learning techniques and datasets. Correspondingly, the following section creates a more in-depth understanding of the learning methods regarding cybersecurity.

There are three main types of deep and machine learning techniques: Unsupervised, semi-supervised, and supervised. **Unsupervised learning** is used when a labelled dataset is not available. Clustering can represent one kind of result from unlabelled data, where the

algorithm is grouping similar instances in clusters. Clustering is used to discover patterns in data. In summary, the primary task of unsupervised learning is to find patterns or structures in unlabelled data. When a portion of the whole dataset is labelled during the data acquisition or by human experts, the problem is called **semi-supervised** learning. The portion of the labelled data can significantly help to solve the problem. If the dataset is entirely labelled, the problem is called **supervised learning**. Supervised learning is leveraged to solve classification problems. The objective of supervised learning is to train the algorithm to classify an input accurately (Buczak & Guven, 2015).

ML mostly requires labelled data for classification problems. For example, malware detection can be seen as binary classification scenario, malicious or not malicious (Goodfellow et al., 2014). Classification problems request the algorithm to identify the input data as the member of a class, or group. Supervised learning, consequently, works better in problem statements where there is a set of available reference points to train the algorithm. Still, those are not always available, especially when it comes to companies which are trying to detect malicious activities in their networks.

Similar to ML methods, DL methods can be used for supervised learning, but are also powerful in unsupervised learning. The benefit of DL is the use of unsupervised or semi-supervised learning and hierarchical feature extraction to efficiently replace features manually (Deng & Yu, 2014). For now, supervised learning has probably delivered the best results, but it is essential to mention that when it comes to cybersecurity, research seems to be shifting towards unsupervised learning (Veiga, 2018). Since clean and correctly labelled datasets are tedious and expensive to generate, unsupervised learning seems promising. In cybersecurity, the unsupervised learning model can organize the data in clusters or can single out anomalies. Some banks, for example, already use AI for pattern recognition to identify fraudulent transactions, by looking for unusual patterns in customer's purchasing behaviour. If the same credit card is used in Brazil and Germany within the same day, the credit card is likely compromised. Nevertheless, unlabelled data is unlikely to provide certainty in terms of prediction quality since there is no label feedback. However, there are some areas where labelled data is indefinable or too expensive to obtain. In these cases, using the deep learning model to find patterns of its own can produce high-quality results.

4.1.2 RESPONSE SYSTEMS

Detection is a very crucial part of cybersecurity and this dissertation already illustrated how AI could improve safety in this regard (Topic 4.1.1). However, cybersecurity processes do not stop when the algorithm detects a system intrusion. Malicious code can cause significant damage to the system and forward classified data to the intruder's servers over time. Therefore, the present topic focuses on AI applications handling and responding to an attack once it was detected.

If hacker intrudes the system, the most effective way to not leak any data is to pull the electricity plug, and no confidential information will leak the system. As most readers already realized by now, this response is not preferred, because almost no business can continue operations nowadays without their information systems. Therefore, a more reasonable response, enabling the system to operate, is preferred. Besides the response choice, time is also a critical component when responding to threats. The time between intrusion occurrence and intrusion elimination determines how much valuable data the hacker can extract. For this reason, cybersecurity staff must be quick identifying the part of the system that is under attack and respond timely to reduce the data, leaked. However, it might prove advantageous to leverage an algorithm, which knows the right actions to take, without disrupting the organization, in almost no time.

According to the Boston consulting group (2018), AI can facilitate intelligent responses to attacks based on shared knowledge and learning. Based on prior knowledge and changes in network usage, the automated response system can segregate networks and isolate valuable assets and information in non-intruded environments. Alternatively, the system might encrypt organizational data automatically or block outgoing command and control connection to stop outgoing malware communication. The intelligent algorithm can perform these actions autonomously, and almost instantly (IBM, 2018). If the protocol nevertheless requires a human decision, the AI algorithm could prioritize the areas for attention and redirect cybersecurity analysts to focus on higher-value activities.

Today's cybersecurity also offers a more active approach when securing the organization's systems (Heinl, 2014). Semiautonomous lures duplicate environments the hacker tries to infiltrate and identifies the attacker who believes he is on the intended path to valuable data. While creating traps using deception techniques and tracking the attacker's activities does not seem illegal, clear international law is absent for some actions, particular remote information

gathering, which requires close observations from the organization employing these techniques (Heinl, 2014).

For now, the researcher could not find any academic article, which solely focuses on AI-enabled automated response to cyberattacks. Nonetheless, some innovative cybersecurity providers already leverage AI for automated responses and claim:

> *"You can't be everywhere. Autonomous response is there to stop threats spreading – giving you time to catch up. Hundreds of business leaders sleep better at night knowing AI has got their back."* (Darktrace, 2019)

This quote from one cybersecurity software provider leads to the next section, which describes the available and commercial AI-enabled cybersecurity solutions for SMEs.

4.2 SUPPLY PERSPECTIVE

It takes much trust for a company to allow a cybersecurity provider to install its software into the system to monitor all activities. It is analogous to contract a security guard who sits in the living room of the house and watches that nobody breaks in. However, many customers trust the AI-enabled cybersecurity solutions, because of its superiority to traditional methods as can be seen by the suppliers of software in the market. Although there are just a few successful players in the market, this section elaborates on two AI-enabled cybersecurity providers. In the pool of players, Darktrace represents the leader in the industry measured by valuation, valued over one billion USD (Financial times, 2018). Furthermore, finally safe (note: the name of this company, finally safe, is written without capital letters), for now, the only German cybersecurity provider which leverages AI in their software solution, is analysed. Therefore, studying the current market leader and the only German player provides a sufficient base, evaluating the cybersecurity options for German SMEs.

4.2.1 DARKTRACE

Darktrace was founded in 2013 by students of the University of Cambridge and has its headquarters in Cambridge (UK) and San Francisco (US) (Hall, 2017). Since 2013, the start-up received multiple investments, which increased the company value exponentially (Figure

8). Now, the company is worth more than $1.65 Billion and is according to experts, one of the most promising innovators in the application of AI in cybersecurity. Darktrace was one of the first movers in the AI space for cybersecurity and delivered a robust solution early on. Therefore, the company obtained more than 7,000 deployments since its inception (Browne, 2018). Darktrace uses ML to scan and identify security weaknesses and malicious traffic inside a company's network (Section 4.1) and responds automatically (Section 4.2).

> A system, integrating IDS and autonomous response systems is necessary to capture the full potential of the software [4_SME].

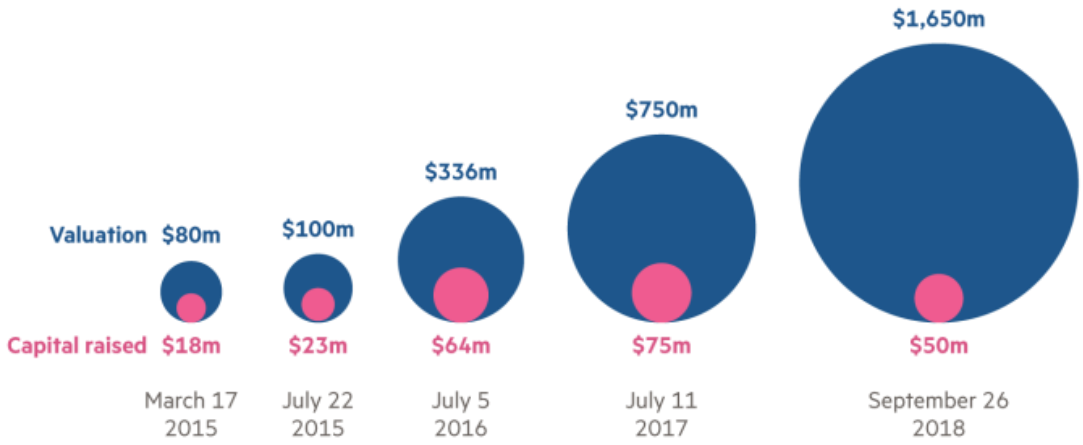

Figure 8: Valuation development of Darktrace (Financial times, 2018)

Darktrace advertises its cybersecurity solution as an **enterprise immune system,** comparable to the human immune system. The algorithm is explained briefly, using the immune system analogy: The ML algorithm is installed in the "heart" of the company's network and analyses 400 data features for every user and device. By tracking the data features regularly, the algorithm builds a "normal pattern" or "pattern of life." Therefore, when some data feature does not meet the normal pattern, the algorithm or immune system gets suspicious.

After the high-level illustration, a more detailed explanation of the intrusion detection system (IDS) is provided. Traditional network monitoring uses signature-based intrusion detection, comparing the signature with activities in the network (Topic 4.1.1). However, Darktrace establishes a profile of the network to understand normal, baseline behaviour, for every user and devise within the network of the organization. Subsequently, it leverages correlation techniques to classify and cross-reference these profiles to understand how normal activities look like (Hall, 2017). If an activity in the network deviates from this "normal pattern", the

system detects a potential threat and displays on the application dashboard where the threat has been identified (Figure 9).

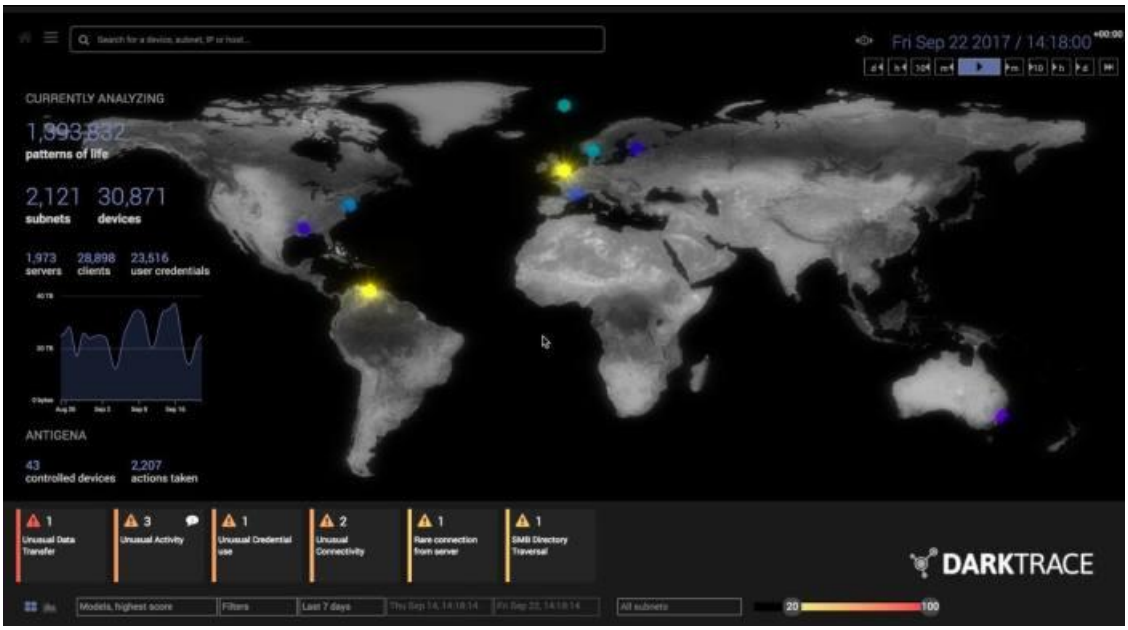

Figure 9: Darktrace's application dashboard (Darktrace, 2019)

The enterprise immune system of Darktrace further uses an autonomous response technology called "Antigena". This technology enables the network to take autonomous actions against emerging cyber-attacks. "Antigena", for example, slows or stops the connection of a compromised device. This technique advertises itself as neutralizing threats without impacting normal business operations (Darktrace, 2019). Thus, the system can stop never-before-seen attacks shortly after inception. As illustration, Figure 10 shows the compromised devise in the company network in yellow and "Antigena" automatically stops the connection of the device.

> I have heard that the big American software providers are using and trying to improve the use of deep learning algorithms [1_Software].

As seen in Figure 9 and 10, visualization plays a key-role in these cybersecurity systems. The threat visualizer makes the detected anomalies searchable and provides a comprehensive overview of the current network status. Furthermore, the implementation process does not seem overly complicated. The algorithm is implemented in the customer's system and placed in the heart of the network system. After inception, the algorithm works independently by monitoring and learning from network activity.

Figure 10: Darktrace's "Antigena"(Darktrace, 2019)

Darktrace's clients range from global banks to the City of Las Vegas and National Hockey League Players' Association. In one interview, Darktrace's CEO, Nicole Eagan, illustrates how the company's software is superior to traditional cybersecurity, by showing examples from the field (Vieira, 2017). One example is given to the reader to enhance understanding.

A casino was hacked through an internet-enabled fish tank. The large fish tank had an IoT-connected (internet of things) thermostat to measure the water temperature. The IT department of the casino was not informed about the installation and that the new device was also connected to the company's networks. Attackers exploited this loophole and broke through the thermostat into the company's network. With network access, the attackers further searched for a specific database which was valuable to them and tried to pull data out of the network and upload it into their cloud. Darktrace was able to spot this behaviour as unusual activity in the network. When the IDS identified the threat, they stopped the network communication, so that no data was compromised (Vieira, 2017).

Besides the example mentioned above, which illustrates how the AI-enabled cybersecurity system can spot unprecedented threats, some clients also raised their concerns. One engineer, who asked to remain anonymous, states that the system sends too many false alerts. After some time, these false alerts become a routine for the IT staff, which starts ignoring them. Others mentioned that the system is very pricey, but has an appealing and easy to use interface, which is highly valued by cybersecurity experts (Financial times, 2018).

4.2.2 FINALLY SAFE

Finally safe is a German-based company and offers clients an AI-enabled cybersecurity software. The company started in 2005 from a research project of the German federal office for information security and the institute for internet security. Together with Securinet Security networks AG, a major shareholder in finally safe, they are a partner of the federal republic of Germany in matters of IT-security. The proprietary "Advanced security analytics platform" (ASAP), as it is called by the company, has the purpose of visualizing network communication to achieve higher network resistance and faster recognition of emerging cyber-attacks (Finally safe, 2019b). Finally safe uses mostly ML-enabled cybersecurity solutions, because they, for now, yield the best results.

> Over the years, finally safe tried multiple applications of DL in cybersecurity. The advantages of these solutions are the lower false-positive rate. Nevertheless, ML-enabled solutions, for now, offer better performance [1_Software].
>
> For AI-enabled cybersecurity solutions, I see major improvements in the future. With better processing powers, DL solutions will enable a deeper understanding of the data and traffic in the future [1_Software].

Finally safe's software has six main pillars, namely: Advanced threat detection, real-time monitoring, compliance reporting, anomaly detection, analysis and forensic, and service monitoring (Finally safe, 2019a).

- Threat detection is the "*automated detection and reporting of advanced and hidden attacks*" (Finally safe, 2019a). Any previously classified data traffic to train the algorithm is used to detect hidden control attempts, data theft, or manipulations. This seems similar to Darktrace's "Antigena" (Topic 4.2.1), and ML-enabled IDS mentioned in the theoretical perspective (Topic 4.1.1)

  > The usage of ML algorithms in cybersecurity depends on the application, but in IDS, it is a classic and often used [1_Software].

- Realtime monitoring and security operation center (SOC) make use of visualizing the traffic and deviations from the norm. Large amounts of data are gathered and visualized on a dashboard for a quick understanding of the current network status.

- The compliance reporting offers a customized management report of network compliance rules. An updated assessment system identifies vulnerabilities and misconfigurations.

- Anomaly detection tracks deviations from regular traffic (Topic 4.1.1) to uncover innovative attacks, which are not detected via signatures.

- The analysis and forensic enables access to data for forensic analysis. Data is recorded and permanently stored, so analysis and optimization for forensic purposes can be performed.

  Depending on the client's specifications, finally safe offers a variety of direct response options to a threat. The cybersecurity software can put the attacked network in quarantine, trigger a ticket for IT, or prompts the firewall. It is though imperative to know which networks are crucial for essential business activities, to not shut down essential processes for the staff [1_Software].

- Service monitoring continuously observes critical applications and IT infrastructure. Complex supplier and customer networks increase the amount of data. Therefore, it is imperative to ensure overview functionalities to enable reliable operations.

With these key-features, finally safe offers a holistic approach to the cybersecurity system of corporations and provides customers with tools to solve issues in their IT department. However, the AI-based algorithms still require signature-based systems as a fundament for the cybersecurity.

> Sometimes, past attacks, like the "WanaCry" virus, are not detected by the AI. So, if one adds the signature-based detection method, with an AI-enabled one, you will have better protection [1_Software].

4.3 DEMAND PERSPECTIVE

This section provides the reader with a view on cybersecurity from the SMEs' perspective, the actual victims of cyberattacks and potential user of AI-enabled cybersecurity solutions.

Starting with the global threats in cyberspace, the results try to narrow down the specific issues SMEs in Germany face, and their limitations compared to larger enterprises. It is essential to first understand the research subject and the individual issues they face before probing a solution. Therefore, this section also elaborates on the status-quo of the SMEs' cybersecurity. The researcher, one more time, wants to highlight that the research subject itself first must be studied. The situation can be compared to a doctor, who first need to see his patient before suggesting a treatment.

> Smaller enterprises are different in their disposition and readiness to fight cyberattacks [4_SME].

Subsequently, this section provides insights about the benefits, short-comings and key-features of AI-enabled cybersecurity solutions and concludes with the willingness of SMEs to adapt AI in cybersecurity.

4.3.1 THE INCREASING GLOBAL THREAT IN CYBERSPACE

As stated in the introduction (Topic 1.2.2), the field of security studies experienced a substantial shift and focuses more on cybersecurity. Corporate security often comprises the classic fields, like physical security, fire protection, protecting against burglary theft, and sabotage. However, with the increasing use of information technology in companies, enterprises need to adapt their security measures when growing interdependence between their daily activities and cyberspace develops. Businesses face, not only an increasing number, but also a variety of cyberattacks, which costs are predicted to reach $3 trillion by 2020 (World Economic Forum, 2019). Moreover, annual cost of cybercrime increases in every developing country over the recent years as can be seen in figure 11.

> The last years a major paradigm shift happened for us. We still need to ensure the security of our physical property, but it became increasingly important to secure our information systems. First, they become more important for our daily business and second, the threat of attacks is increasing [2_SME].

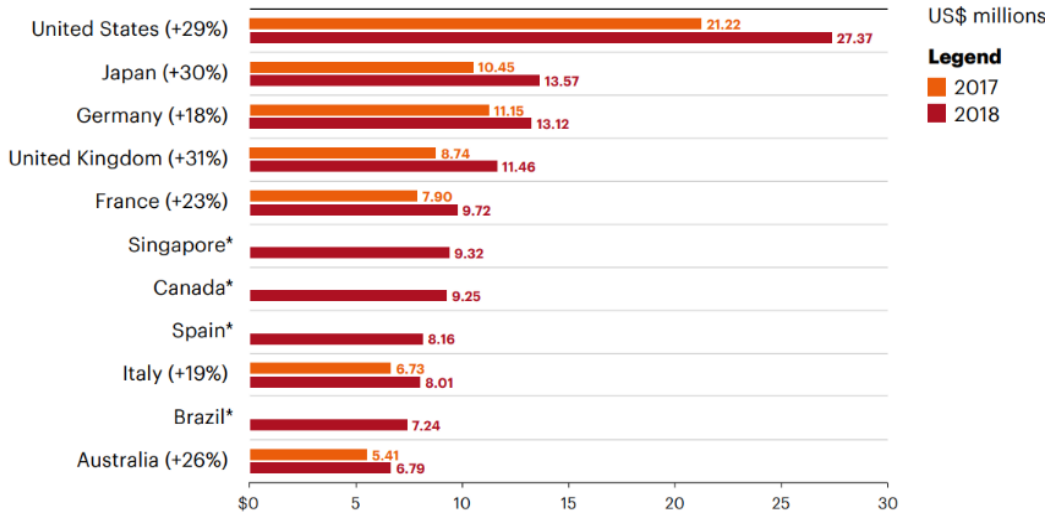

Figure 11: Average cost of each cybercrime per country (Accenture, 2018)

The author believes that a better understanding of the cost of cyber-crime might nudge companies to allocate the appropriate amount of investment to cybersecurity to mitigate the costly consequences of the attacks. Nevertheless, new technologies, which might mitigate growing attacks, also develop in parallel to the increasing amount of cybercrime. Deloitte (Loucks et al., 2018) surveyed more than two hundred executives on AI and found that investment in AI is ramping up. With these improved investments and abilities, they further concluded that companies can improve their risk and change management, especially in terms of reducing cybersecurity vulnerabilities with AI (Sections 4.1 and 4.2).

> Besides a lot of hype around AI, I believe that the increased attention and investment will more and more increase the capabilities of these algorithms [2_SME].
>
> AI in cybersecurity is very interesting, because it is forward looking and not past oriented. That is what is needed [3_SME].

4.3.2 CYBERATTACKS ON GERMAN SMES

The global threat of cyberattacks is rising, as seen above, but the German “Mittelstand” is particularly interesting for hackers (Topic 1.3.1). German SMEs are the most affected by attacks since most of them represent market leaders in a specific segment, so called hidden champions. Especially, German SMEs have many innovations in artificial intelligence (AI) and industry 4.0 (Bitkom, 2018), which makes them interesting targets also for industry espionage.

> Our study showed that SMEs were particularly under attack [1_Association].

Almost every SME in Germany has experienced recent cyber-attacks. More than 39 percent of all German companies were affected in 2012 alone. Nowadays, 96 percent of all German SMEs have already had unpleasant experiences involving cyber-attacks (German Federal Ministry of education and research, 2019). These incidents usually involve the violation of company secrets, the theft of data, computer fraud, data espionage and interception, damage to systems, and computer sabotage (Bitkom, 2018).

> A lot of similar businesses face severe problems with cybersecurity. One of our competitors went bankrupt, since data security is one of the most important requirements from our clients [3_SME].

> One client needed to invest in a completely new IT system since they could not track the intrusion and needed to continue their regular business [4_SME].

After all, successful cyber-attacks reduce productivity, violate corporate secrets and ultimately threaten the existence of the entire organization. Corresponding investments in cybersecurity are a necessary condition for maintaining the image, market position and competitiveness of the company. Most managers of SMEs already realize the increasing importance.

> As IT-specialist, it is my duty to address the importance of proper cybersecurity. Sometimes I convey this by telling the worst-case examples of the industry [4_SME].

4.3.3 SPECIFIC LIMITATIONS OF SMES IN CYBERSECURITY

As cyber-attacks are becoming an increasing threat to businesses, the first companies who raised their cyber defence systems were the large and more well-known businesses. Some leading German corporations including Allianz, BASF, Bayer and Volkswagen jointly launched an innovative competence center and platform for cybersecurity in Germany called the “DCSO - Deutsche Cyber Sicherheitsorganisation” (DCSO, 2019). This organization joints the scientific knowledge of large German corporations to develop a sound European cybersecurity strategy for the investors.

Taking this example, large corporations have the resources and manpower to fund and initiate these joint organizations, trying to secure their corporations from the increasing threat of cybercrime. However, as cybercrimes evolved the threat has also reached smaller players as

their importance in the world-wide intertwined value chain grows and they also become a part of the digital economy (Pankit, 2018). Hackers assume that SMEs do not make the necessary investment in cybersecurity and that the techniques that the criminals used years ago on large enterprises will work even today on smaller enterprises. This was supported by one of the interviewees.

> Smaller players are currently under attack as well. The "Emotet" virus, which infected Heise in 2019, showed that attacks use ransomware and put the price of ransom at a level where smaller corporations do not get bankrupt. They gathered the company's data over time and therefore know what a smaller corporation can pay without defaulting [1_SME].

Therefore, it seems that a lack of financial means is a limitation for SMEs in improving their cyber-defence and that hackers particularly exploit these vulnerabilities.

As mentioned in the introduction chapter (Topic 1.2.2), cyber-attacks are growing in amount and complexity, but alarming is the companies and organizations is the lack of readiness (Hiscox, 2019). The issue is wider than the technical gap. Management often lack awareness and understanding of the threat, therefore not providing the required support for cybersecurity. This lack of support in senior positions causes for many companies the subsequent lack of drive, attention, and willingness to commit funding to cybersecurity.

> For me, as head of IT, cybersecurity has maximum priority. In the past, I needed to fight with the management for more budget. In the last years this changed since cybersecurity also received more media attention, which nudged the management to prioritize cybersecurity [1_SME].

Therefore, it can be inferred that a major paradigm shift took place and management is aware of the problem, at least in some companies.

According to Winter (2016), the German manufacturing sector is very different to the United States or the United Kingdom. German enterprises are very hierarchical, steep in tradition, and increasing sceptical in new digital technologies, also when it comes to cybersecurity.

> If the management does not have a background in IT or is interested in this topic, it is difficult to convince them for new cybersecurity solutions. From the management

> perspective, you do not sell more products with new cybersecurity solutions. What management sees instantly is that it costs money [1_SME].

Further, Winter (2016) mentioned that it is quite difficult to integrate cybersecurity awareness and training in the rigid structure of German SMEs. However, in this study it is observed that two CEOs cover responsibilities in their IT-departments and closely supervise their cybersecurity.

> I am the responsible person in the company for cybersecurity. We have an external expert who helps us with issues we face, but the responsible person within the company is me [2_SME].

> As the CEO and owner, I am the one in charge and liable for any leakage of our clients' data. Of course, I grew into this position, but seeing the importance for our clients, cybersecurity must have a significant importance for us [3_SME].

On this ground, cybersecurity developed to a matter with importance for the CEOs, as learned during the interviews. According to this study, the lack of support of the management in cybersecurity does not seem to be a limitation for some companies.

Along those lines, it is important to mention the lack of professionals to fill all future needs for cybersecurity positions, when companies transition and focus on cybersecurity (Topic 1.2.2). Even when corporations try to contract cybersecurity experts, there is a lack of professionals in this field in Germany. With the pace and amount of cyber-attacks, cybersecurity professionals are not only not available but also simply not enough for timely attack analysis and appropriate response.

> For sure, there is no employee available which can be paid by an SME. SMEs are too small to hire one person with the sole purpose of monitoring the system, especially with the current wages paid. However, AI can be advantageous here and enable the IT department to focus on more strategic issues. If an AI-based cybersecurity software can work more autonomously, I can focus on tasks which can secure the whole network [1_SME].

> SMEs do not have cybersecurity experts like large enterprises. Usually, the IT staff ensures a functioning company network and does not have the capacity to work fulltime on cybersecurity [1_Software].

> A cybersecurity expert is not feasible for the size of SMEs. The IT staff must consist of allrounders. However, I see that the current education is focusing more and more on cybersecurity [4_SME].

In some cases, the management of small enterprises is responsible for the IT network and cybersecurity within the company. These mangers usually do not have a background in IT, but enlarged their knowledge as the company evolved over time. For them, one employee with the sole purpose of ensuring cybersecurity would be too expensive.

> I am basically responsible for the network and technology. When we were starting the company, we had less than a handful of people. Therefore, it was not feasible for us to contract an IT specialist. Furthermore, twenty-five years ago we had no IT infrastructure we had to take care of [2_SME].

Therefore, the lack of cybersecurity professionals available in the market illustrates the third limitation of SMEs when it comes to cybersecurity. After describing potential limitations, the next topic reports on the current cybersecurity systems of SMEs.

4.3.4 CURRENT STATUS OF CYBERSECURITY AT SMES

As mentioned above, most SMEs are aware of the increasing threat when it comes to cyberspace. Therefore, this dissertation tests, what cybersecurity measures are already implemented by SMEs? This helps to determine the “status-quo” and current actions taken, in order to evaluate, how AI-enabled systems can build on the current cybersecurity foundation? All companies in this study employ traditional cybersecurity software like anti-virus programs or a firewall, which protects the company networks from less complex attacks.

> Nowadays, a company cannot survive without the classic cybersecurity systems, like a firewall and an antivirus software. These programs are preinstalled on each company laptop or computer [2_SME].

While tools like antivirus programs or basic firewalls may offer security on paper, SMEs still need to customise security controls and re-assess those on an ongoing basis. For example, cybersecurity measures that worked for SMEs a year ago may no longer be even the minimum requirement nowadays, given the scale of growth. Therefore, regular patching and reviewing of the software in use is imperative.

> For now, the IT department focuses on regular patching of our software and anti-virus programs, hence, updating our software. On another level, we look if the software is state-of-the-art to ensure that we also use software providers which develop their software on a continuous basis [1_SME].

Besides classic cybersecurity software and regular updates, interviewees stress the importance of regular trainings for their staff. These trainings empower the employee to recognize common cyber-threats and further reinforce awareness of vulnerabilities when using the company's information technology. These trainings strengthen, according to the interviewees, the most vulnerable part (the employee) in the cybersecurity chain.

> Half of my work I spend training our employees in terms of dos and don'ts when interacting with the computer. When your employees do not adhere to the most basic rules, like using external USB sticks on company computers, then the most advanced cybersecurity software cannot protect you [1_SME].

Although it does not count as cybersecurity measure by definition, the author does not want to withhold from the reader that some corporations recently signed a cybersecurity insurance, which insures costs incurring during a cyberattack. These costs include potential ransom, cost of loss of business, cost for legal processes, and hardware replacement.

> We recently signed a contract insuring potential cyber-attacks. In order to receive the money in case of an attack, we must prove that we adhered to certain cybersecurity standards. These standards were also tested before we signed the insurance contract [2_SME].

In summary, all SMEs in this study are aiming to improve their cybersecurity. As of the time of the interviews, the companies had traditional cybersecurity software installed, updated their programs regularly, provided training to the staff, and some even signed an insurance in case of an attack.

4.3.5 DESCRIPTION OF DESIRED AI-ENABLED CYBERSECURITY SYSTEM

During the interviews, participants were asked about features and standards AI-based cybersecurity solutions should provide. When questioned about the requirements and benefits

of AI-enabled cybersecurity solutions, answers can be clustered in four different categories: Seamless implementation in current IT-system, enhanced IDS, autonomous response systems, and superior usability for the IT staff.

The first process step when acquiring new software is the **implementation process**, including distribution of the new software over the company network. Two study participants raised the concern that the implementation process takes time and thus adds to the total cost of the software.

> We needed ¾ of a year to roll out a new anti-virus software. These processes take a lot of manpower and increase the total cost of the new software [1_SME].

> The implementation of new infrastructure and software takes a lot of time, because in almost all the cases the corporation needs to continue with the daily business during the implementation. Therefore, the implementation process mostly takes place after the office hours or in the night [4_SME].

Therefore, an AI-enabled cybersecurity solution should be easy and quick to implement.

Secondly, **AI-enabled IDS** is considered a significant advantage compared to traditional IDS. The ability to detect zero-day attacks is one of the most significant advantages (Topic 4.1.1), reported the company representatives.

> If the system can detect attacks, which did not occur before. That would be a huge improvement. For the moment, there is no other software available which can provide protection against zero-day attacks [1_SME].

> It is imperative to have software which anticipates the future. I would compare it to an autonomously driving car, which hit a deer by accident. If you tell the system not to do this again, but the next time a boar is on the street, the situation changed. The system must be, as the term AI indicates, intelligent [3_SME].

However, multiple study participants also mentioned concerns regarding the reliability of the predictions of the AI-enabled IDS. One interviewee referred to an online review, in which the AI algorithm was tricked by simple code alterations (Schmidt, 2019).

> By simply adding some characters to a malware program, the AI-based system was tricked and did not identify the malicious code [1_SME].

Additional requirements for the IDS are a low false-positive rate. If the software produces a substantial number of false-positives alerts, which need to be manually checked by cybersecurity specialists, these systems cost the IT department time. Hence, an AI-enabled cybersecurity solution is only valuable to the SMEs when the false-positive rate is low.

> False-alarms are another significant problem of some AI-enabled solutions. I could not follow my other daily tasks, if I must check the alarm from the system regularly and investigate the problem further. I would need another employee for checking these alarms during the day and these cybersecurity exerts are expensive [1_SME].

> A common problem of the AI-enabled IDS is the high false-positive rate. If most of the activities in the system create an alarm, this requires manual check-ups by the IT department. This costs time and money [3_SME].

In conclusion, AI-enabled IDS show potential for advanced cybersecurity, since it can detect zero-day attacks. Nevertheless, some caveats identified by the SMEs are easy deception of the AI algorithm and high false-positive rates.

Thirdly, most SMEs viewed the **automated response** as the main advantage of AI-enabled cybersecurity software. The interview participants desired a timely response to cyber-attacks, as mentioned in topic 4.1.2.

> Relocating the malicious code in a quarantine network would be a substantial improvement. This would be a killer feature. If the program can perform this task autonomously, this is even better, since on the weekend there is no staff at the office which can perform such actions [1_SME].

> Autonomous evaluation of the importance of the network and direct response by the systems are how future cybersecurity should work. As I mentioned, time is one of the most critical factors when responding to cyberattacks [4_SME].

Nevertheless, some interview participants also raised their concerns about automated response performed by an AI algorithm. If the AI algorithm responds to cyber-attacks by slowing down

or stopping traffic in the company network, this can affect the daily business of the company. For example, when employees try to use the part of the network, which is slowed or even shut down, the staff is unable to continue their daily work.

> It is though imperative to know which networks are crucial for important business activities, to not shut down essential processes for the staff [1_Software].

> If some networks are autonomously shut down or not usable anymore, we also incur costs [3_SME].

Furthermore, the linkage between false-positives in IDS and automated response systems can result in an unnecessary slowdown of the network.

> It is a similar issue. If there are a lot of false-positives in the IDS, there will be autonomous responses from the system, although there is no real threat. In my opinion that is definitely an important point to raise and to solve [4_SME].

Finally, few interview participants require the new AI-enabled cybersecurity systems to be **user-friendly**. In the category of user-friendliness, comprehensive and concise visualization, as well as ease of use, were stated as vital criteria.

> I want to have an immediate overview of my network security. Since I am not a cybersecurity expert, an interface with too much information or even code is not feasible for us. [2_SME].

In general, IT specialists prefer to spend the least time necessary on cybersecurity operation. Hence, concise visualization can reduce the time for IT specialists to understand the current status, as well as potential issues in the network.

> Visualization is very important. I want to get an overview of the status of my network systems quickly [3_SME].

Moreover, the ease of use and intuitive handling also represented a critical feature for the SMEs. Since most of the IT staff has no particular background in cybersecurity, the system needs to be navigable by novices.

> If I cannot use the system on my own, because it is too complicated and I need to call an expert every time, this new solution is not feasible for us. Its intrusion detection capabilities might be superior, but if I cannot use it, these systems won't be of any help to us [2_SME].

4.3.6 ADAPTION OF AI-ENABLED CYBERSECURITY SOLUTIONS

Finally, the actual willingness of the interview participants to adapt the previously described algorithms was studied. In general, German SMEs view AI as potential aid fighting cyber-attacks and acknowledge the benefits in theory.

> If the AI-enabled solution delivers on its promises, it is certainly something we will consider in our next update of our cybersecurity systems [1_SME].

> For me, AI is the most promising field of study in cybersecurity [4_SME].

A few participants requested further information about artificial intelligence in cybersecurity and specfically asked for the most advanced AI-enabled cybersecurity solutions, offered in the market. This interest demonstrates that some SMEs seriously consider the use of AI-enabled cybersecurity.

> If you know any company which is leading in the market, let me know [1_SME].

> This area seems very promising. Please send me your findings and the thesis after you finish [1_Association].

Nevertheless, some interview participants also raised doubts about the actual benefits of the systems in practice.

> I am tracking the development in AI-enabled systems. However, before I invest, I really want something for my money [2_SME].

> A distinction between marketing effort of the software providers and the actual value-added of the systems needs to be made. For this reason, I mostly trust big German cybersecurity providers, which already built a reputation in the market [4_SME].

The gap between the interest in AI-enabled cybersecurity solutions and the actual investment is further supported by Bitkom's business study (2018, p. 39). In this survey, 503 executives were asked, if they have AI-enabled cybersecurity solutions in use, or if they intent to use them in the future. Ninety percent of smaller and medium-sized corporations answered that they do not plan to use AI for now. However, half of the participants view AI in cybersecurity as a very important tool.

> There is a gap between the interest of SMEs and the actual drive to implement it. Smaller enterprises are usually more careful when trying new things. One malinvestment might be costly for SMEs [1_Association].

> I think we will not invest in this AI-enabled software soon. First, we wait and see how this technology is developing. I am not an expert and cannot assess if the systems for now are good or not. However, we will closely observe the future development [2_SME].

Therefore, most of the interview participants do not intent to invest into AI-enabled security systems soon. For the moment, the interviewees prefer to allocate more resources to basic protection of their systems than to advanced cybersecurity solutions like AI.

> For now, the employee represents our main vulnerability in terms of cybersecurity. Before we invest in AI, we anticipate more benefit by conducting cybersecurity trainings with our staff [2_SME].

> First, we must improve the basic security, after we can talk and think about AI [3_SME].

> We see basic protection as main opportunity, for now, to increase cybersecurity. However, AI can be a very important technology in the years to come [1_Association].

In summary, SMEs view AI in cybersecurity as beneficial and track the development of these software solutions. However, these companies are also cautious and prefer to wait for more mature software solutions available in the market, before undertaking an investment in AI. Lastly, basic security and staff trainings have higher priority for the experts than advanced cybersecurity.

5. FINAL EVALUATION

This chapter provides the reader with the relation and analysis of the study results from the previous chapter. Therefore, the results are clustered analogously by the same structure, in the theoretical, supply, and demand perspective. Insights from the previous chapter are compiled and a summary is provided to refresh the insights. Subsequently, these chapters are compared to each other to find commonalities and differences.

5.1 SUMMARY OF FINDINGS

This section provides short summaries of the insights gathered. Subsequently, these insights are used for comparison and further analysis (Section 5.2).

5.1.1 THEORETICAL PERSPECTIVE

The theoretical section investigates how the AI-enabled algorithms work and compares these intelligent algorithms to traditional methods. As has been noted, intelligent algorithms, like deep learning or machine learning, are forward-looking and can detect zero-day attacks, which traditional methods like signature-based IDS cannot. Moreover, machine learning and deep learning are compared regarding their learning methods. The results acknowledged that deep learning methods should be preferred over other machine learning methods, since deep learning performs feature extraction autonomously, and therefore is very powerful working with unlabelled data. The theoretical perspective on AI-enabled response systems shows that algorithms can respond quickly to emerging threats. However, academic journals lack scientific studies on AI-enabled response systems.

5.1.2 SUPPLY PERSPECTIVE

The section on the software providers delivers an overview on the AI-enabled applications, offered in the market and accessible for SMEs. Darktrace and finally safe, both, offer IDS, which track the “normal pattern” of the network and compares it to actual system behaviour. According to the publicly available information, the software providers claim the superiority of their AI-enabled IDS compared to traditional IDS. Regarding the response systems, the companies’ algorithms appear very sophisticated and show advanced autonomous behaviour.

As illustrated with screenshots from the software, both companies emphasize the visualization of their applications. Threats and software responses are presented, visually appealing, and easy to navigate by experts. However, some users criticize a high false-alarm rate and the price of the systems.

5.1.3 DEMAND PERSPECTIVE

Globally, corporations face an ever-increasing threat of cyber-attacks; growing by cost per attack and number of attacks. Notably, German SMEs seem to be most affected, as was confirmed by the study participants. It can be inferred from the study that the lack of investment in cyber-defence, compared to larger organizations, is one of the reasons hackers specifically target SMEs. Adding to the issue, cybersecurity experts are first, not available and second, not affordable for smaller enterprises.

Additionally, this study examined if the lack of management awareness in cybersecurity is resulting in a slower drive as proposed by Winder (2016). Contrary, every study participant, including managers of SMEs, stated that cybersecurity has developed to a topic of significant importance for their enterprises. The increasing importance is indicated by the current status of cybersecurity solutions within the company. Traditional IDS, firewalls, and anti-virus protection are implemented in each of the SMEs. Furthermore, regular patching and updates are performed to ensure comprehensive security. Besides cybersecurity systems, SMEs emphasise on regular trainings of the staff, since human represent the highest vulnerability for the network. If all the previously mentioned systems cannot protect the IT systems, some SMEs even purchase a cybersecurity insurance for the worst-case scenario, when the system is actually compromised.

This dissertation also informs the reader about SMEs' specifications for AI-enabled cybersecurity solutions. Before the system is used, some participants require a short implementation process of the new software. When the system is in use, AI-enabled IDS are identified as a significant improvement to traditional IDS. However, some participants raised their concerns about the readiness of the current software, since some studies stated a high percentage of false-positive rates, and simple tweaks, which can trick the AI-enabled systems easily. Additional to stronger IDS, participants view autonomous response systems as the most significant advantage of AI. However, again, some participants doubt the readiness of the software and fear that the system might shut down critical company processes, because of

false-positive alerts. Lastly, the study participants prefer systems with high user-friendliness, mainly because most SMEs do not have specialized staff, who has expertise in reviewing complex computer interfaces.

Concluding, it critical to examine the actual willingness to use AI-enabled cybersecurity systems. Most of the surveyed companies acknowledge the benefits of AI in cybersecurity in theory. However, this dissertation shows a clear preference towards implementing basic cybersecurity measures and subsequently investing in more advanced solutions, when these systems are more sophisticated.

5.2 COMPARISON

This section compares the three perspectives summarized above. Therefore, this section provides the reader with similarities and gaps of the different perspectives. Since the software providers are the sole source for SMEs to obtain AI-enabled cybersecurity systems, comparing theory to the SMEs' specification directly adds not much value from a practical perspective. Therefore, the researcher undertakes additional effort and compares the research perspective with the products on the market and the products on the market with the specifications from SMEs.

5.2.1 COMPARISON BETWEEN THEORETICAL PERSPECTIVE AND SUPPLY PERSPECTIVE

In general, business and research sectors should join their efforts to provide comprehensive cybersecurity solutions. With this effort emerges a need for better collaboration between research and industry fields. Despite the collaboration effort, this dissertation identified some gaps between research and actual business practice.

On the first view, the commercialized intrusion detection systems appear similar to the AI-enabled cybersecurity systems, described and developed by researchers. Whether they are called "enterprise immune system" or "threat detection system", both solutions in this dissertation offer an intrusion detection system based on AI. The software packages compare the "normal" system pattern with the current performance of the network and thereby enable the detection of zero-day attacks. However, most commercialized software solutions make use of machine learning and not deep learning. The theoretical perspective, nevertheless, identified

deep learning as a superior algorithm, which leverages feature extraction, and thus is more potent in unsupervised learning with unlabelled data. This represents a significant gap between theory and actual implementation in practice. Furthermore, it seems that software providers cannot reduce the false-positive rate of their algorithms to the level of research studies. Since most theoretical articles yield low false-positive rates, the researcher suggests that academia needs to work closer with software providers to provide solutions that also have practical validity and better performance in real-world settings.

When it comes to AI-enabled response systems, the author could not identify one academic article, which describes how such systems work. Per contra, software providers offer very advanced solutions for automated response systems. Cybersecurity companies developed algorithms, which autonomously respond to intruders and thus perform timely answers to attacks. Companies seem to be far more advanced than academia in creating algorithms, which perform autonomous actions when attacked. Therefore, the author identified a significant gap in research and calls for closer collaboration in automated response systems to develop these algorithms further.

Regarding the ease of use and visualization techniques of AI-enabled software, there are also no scientific articles available. Indeed, multiple academic articles describe visualization techniques for cybersecurity in general, but it appears that software providers in the field of AI-enabled cybersecurity focus on robust visualization techniques, especially for AI. Since AI algorithms can work autonomously, it seems crucial to provide the user with superior visualization, because users want to understand what the system is doing. Hence, the author concludes that future research should study the visualization of AI-enabled cybersecurity solutions specifically.

Similarities of research and supply perspective identified:

- IDS usage of ML algorithms
- IDS compare “normal” network pattern with actual behaviour
- IDS potential to identify zero-day attacks

Gaps between research and supply perspective identified:

- DL algorithms in IDS are not widely used in practice
- IDS in practice show high false-positive rates
- Research lacks articles in AI-enabled response systems

Research lacks articles which focus on the visualization of AI-enabled cybersecurity systems.

5.2.2 COMPARISON BETWEEN SUPPLY AND DEMAND PERSPECTIVE

German SMEs are facing more cyberattacks than ever before. Consequently, these companies are searching for products which increase the protection against these threats. With growing investment in AI, the application fields of this new algorithms extended also into cybersecurity. Therefore, this study elaborates on AI-enabled cybersecurity systems for SMEs. Some surveys already identified that the current adoption rates of this emerging technology are low. Therefore, it is critical to compare the available options on the market with the specification of the SMEs and determine what features are needed for future adoption.

First, SMEs require new IT systems to be as cost-effective as possible. Indeed, smaller companies have a lower budget than larger enterprises, which adds to the importance of cost-effective solutions. Therefore, acquisition and implementation costs should be reduced to a minimum to cater the smaller budget of SMEs. Although the system prices are not officially stated, online reviews stated that AI-enabled software is quite pricy. Adding to the fact, IT implementation processes, in general, can last very long and represent another major cost driver. Regarding the implementation process, Darktrace offers seamless integration of its software in the computer systems of its clients, because the algorithms need only one installation in the heart of the network. Hence, it is inferred that a seamless implementation process can be provided by the software suppliers, which is desired by SMEs.

Regarding IDS, SMEs seem to prefer future-oriented cybersecurity solutions over past-oriented algorithms. Consequently, an IDS identifying zero-day attacks is regarded as the future of cybersecurity. Besides the benefit of anticipating future attacks, current AI-enabled IDS also show high false-positive rates, which interviewees view as a significant disadvantage of these systems. Furthermore, some online reviews, quoted by the interview participants, describe how simple alterations of the malware code deceived AI-enabled IDS. Hence, the

interview participants require more rigorous detection abilities before implementing these systems. In summary, current IDS need further improvement regarding false-positive rates and rigorous detection, before SMEs are willing to adapt these systems. This represents a significant gap between supply and demand.

AI-enabled response systems are considered the main advantage of cybersecurity systems leveraging AI. In general, the response time to cyber-attacks should be as short as possible. Since autonomous response systems can react in real-time, they have the potential to reduce reaction time to a minimum, which makes them a powerful tool fighting cyber-attacks. However, high false-positive rates of AI-enabled IDS can trigger a response, slowing or shutting down the network, although the system has not been compromised. Therefore, the interviewees require more sophisticated algorithms with low false-positive rates, representing a gap between the current supply and demand.

Finally, the software providers show robust visualization and intuitive handling of their services. This enhanced user-friendliness is one of the SMEs' specifications and considered to be met by the software providers.

Concluding, SMEs are very particular in their specifications, which are not entirely met by the software currently on the market. Therefore, SMEs prefer to wait for more sophisticated software solutions in the market, before undertaking an investment in AI.

Similarities of supply and demand perspective identified:

- Seamless integration in the network
- IDS zero-day attack prevention
- Automated and timely response
- User-friendliness and strong visualization

Gaps between supply and demand perspectives identified:

- Pricy software
- False-positive rate might prove impractical

6. CONCLUSION

The introduction of this dissertation stressed how the threat of cyber-attacks is increasing in number and severity over the last years. Therefore, did society make a mistake when incorporating the internet in our everyday life, where users are so exposed and vulnerable? If following this logic, it is like saying, I am afraid of catching the flu and will not go outside of my house. This person could not go to work, travel, or expose himself to the outside world. Contrary, the power of human civilization is making progress by experimenting with new things. For the author, the internet is just another manifestation of the obstacles humanity faces during a continuous development process. Now, society adjusts to cyberspace, because it must. Therefore, it is imperative to develop cybersecurity solutions, which make the internet a safer medium to use. This dissertation tries to contribute to this development in one specific area, by answering the research question, how can AI-enabled cybersecurity solutions, like machine and deep learning, help German SMEs fighting the increasing threat and past incidences of security breaches?

This dissertation finds that some cybersecurity-related challenges of SMEs can be solved by applying artificial intelligence. Particularly in times when the number and the complexity of malware are evolving at a fast rate, intelligent solutions can assist in fighting these threats. Especially, AI-enabled IDS and automated response systems can enhance network security when fighting new evolving threats quickly. For the moment, cybersecurity providers mostly leverage machine learning algorithms for their solutions, but research is driving and supporting deep learning methods for even better analysis. Therefore, intelligent systems underpin solutions for future challenges in cyberspace. Although there are many benefits of deploying AI for cybersecurity, the limitations of AI are obstructing the mainstream adoption of the technology. Hence, these solutions might need some adjustment, not only in their underlying algorithm, but also to cater to the needs of the potential users, the SMEs. According to this study, the foremost necessity of AI-enabled cybersecurity is to decrease the false-positive rate. With this improvement, IDS require less human interaction, and automated response systems do not slow, or shut down critical company processes. As additional areas for improvement, the paper further identified a more rigorous intrusion detection and user-friendliness. After all, cybersecurity developed into a central function for the management. Therefore, it is imperative to continuously improve on the visualization of data to improve the ability of security specialist to understand a broader range of threats, with less time and effort. Consequently,

adaptation rates of SMEs are projected to increase when future AI-enabled cybersecurity software meets the specifications of SMEs. For now, SMEs do not intent to adopt these solutions over the short-term horizon.

However, the author suggests that software producers of AI-enabled cybersecurity might provide a service to monitor and track the cybersecurity for SMEs. Software providers employ cybersecurity experts, which have the expertise to monitor and analyse alerts made by the system. A monitoring service can help SMEs, which are currently not using AI-enabled cybersecurity software, because of the high false-positive rates and the lack of cybersecurity experts within the company. Furthermore, this additional service can have the potential to bridge the gap between current detection accuracy and the more accurate detection with more advanced and autonomous algorithms in the future.

We can conclude that artificial intelligence can provide enhanced security for SMEs. Especially automated response systems and intrusion detection systems show great potential. With increasing data which can be leveraged to train the software, algorithms will become even stronger over the years. It remains to be seen if AI-enabled systems become the new cybersecurity standard. In the spam detection of e-mails, ML is already becoming the standard. Similar to ML-enabled spam filters, AI in cybersecurity needs to develop into a commercially viable product. Analogously, AI-enabled systems can only help SMEs fighting the increasing threat of cyber-attacks when the final product is tailored towards the end-user, the SMEs. Therefore, research and cybersecurity provider need to fill the gaps and cater to the requirements of SMEs. This might spread AI-enabled cybersecurity solutions and represents the next step to form strong cyber-defence in cyberspace.

Concluding, AI is not being used nowadays as it is expected, but a more customer centred solution might increase the adoption rate. From a technical point of view, this dissertation identified ML as the main algorithm applied in cybersecurity, until now. Despite the caveats, mentioned in this thesis, supervised ML is the field of AI which delivered, for now, the best results in cybersecurity, as confirmed by the interview participants. The author believes that in the future immense malware databases and increasing computational power will upsurge the detection accuracy and reduce the false-positives rate. Moreover, growing technological advancement will also reduce the cost for software providers, which in turn might reduce the price of the software. Therefore, DL algorithms, which have superior performance on

unlabelled data than other ML algorithms and are available for a lower price will play a more prominent role in cybersecurity in the future.

7. CONTRIBUTION TO RESEARCH

This dissertation contributes and fills a gap of the existing literature as mentioned in the research gaps (Section 1.4).

As AI in cybersecurity is a relatively new topic, specific application cases are not studied, yet. To provide a better overview of the ecosystem parts in this new study area, the focus of this research changed during the writing process and now relates the current research, the actual cybersecurity solutions, and the final consumer with each other. This approach adds substantial value to the current body of research since it offers multiple perspectives.

Furthermore, this dissertation compares the specifications for AI-enabled cybersecurity systems for German SMEs specifically, because these companies are increasingly targeted by cyber-attacks, as mentioned in the introduction

8. LIMITATIONS AND FUTURE RESEARCH

In terms of limitations, it was already discussed that the qualitative research method fosters a rather descriptive study of the subject matter. Therefore, some observations from the interview might not be exclusively applicable to the target group, but also for other corporations. Moreover, selecting a sample that is representative of the target group, these observations are few in numbers compared to quantitative studies. In addition, the findings are solely based on interviews and do not have statistical methods implemented, measuring the accuracy of data. Lastly, AI-enabled software providers are quite a few. Nevertheless, two software companies provided additional insights and understanding of the commercialized products, which improves the readers understanding. Initially, the researcher intended to compare the current research status with SMEs' specifications of the software. However, the researcher desires to provide additional insights in the form of software providers, which were not mandatory to answer the research question, but helped to enhance understanding.

One method that could strengthen the study is an additional survey. After this dissertation provided more descriptive results, a larger data set can provide a more detailed vision of AI-enabled cybersecurity solutions for SMEs. Furthermore, a comparative study with other countries or business sizes can improve the current body of research and build on this dissertation.

Finally the dissertation's conclusion, contribution, limitations, and outlook are summarized in the figure 12 to offer a quick overview to the reader.

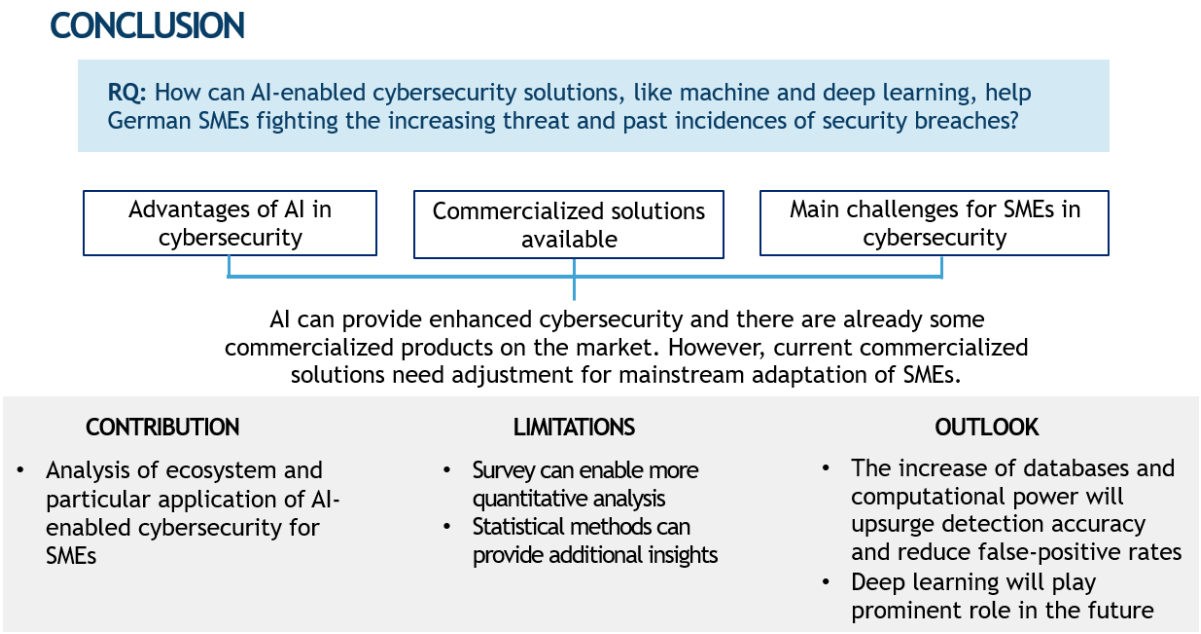

Figure 12: Summary of conclusion (Self-provided)

9. REFERENCES

Accenture. (2018). *The cost of cybercrime*. Retrieved from https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf

Acuña, D. C. (2016). Enterprise computer security: A literature review. *Journal of the Midwest Association for Information Systems*, *1*, 37–53.

Amazon. (2019). Amazon Echo & Alexa Devices: Amazon Devices & Accessories. Retrieved June 28, 2019, from https://www.amazon.com/Amazon-Echo-And-Alexa-Devices/b?ie=UTF8&node=9818047011

Anand, S., Sinha, A., Tiwari, U., & Ray, S. (2019). *Artificial Intelligence-Literature Review*. Retrieved from https://cis-india.org/internet-governance/files/artificial-intelligence-literature-review

Ben Naseir, M. A., Dogan, H., Apeh, E., Richardson, C., & Ali, R. (2019). Contextualising the National Cyber Security Capacity in an Unstable Environment: A Spring Land Case Study. *Advances in Intelligent Systems and Computing*. https://doi.org/10.1007/978-3-030-16181-1_35

Bitkom. (2018). *Wirtschaftsschutzstudie 2018*. Retrieved from https://www.bitkom.org/Bitkom/Publikationen/Wirtschaftsschutzstudie-2018.html

Boston Consulting Group. (2018). Artificial Intelligence Is a Threat to Cybersecurity. It's Also a Solution. Retrieved July 12, 2019, from https://www.bcg.com/publications/2018/artificial-intelligence-threat-cybersecurity-solution.aspx

Brogaard, J. (2010). High frequency trading and its impact on market quality. *Northwestern University Kellogg School of Management Working Paper*, *66*.

Browne, R. (2018). Cybersecurity startup Darktrace raises $50 million in Series E funding. Retrieved July 22, 2019, from https://www.cnbc.com/2018/09/26/cybersecurity-startup-darktrace-raises-50-million-in-series-e-funding.html

Brynjolfsson, E., & Mcafee, A. (2014). The digitization of just about everything. *The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies*.

Brynjolfsson, E., & McAfee, A. (2014). *The second machine age : work, progress, and prosperity in a time of brilliant technologies*.

Buczak, A. L., & Guven, E. (2015). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials*, *18*(2), 1153–1176.

Cellan-Jones, R. (2014). Stephen Hawking warns artificial intelligence could end mankind. *BBC News*, *2*, 2014.

Charmaz, K. (2006). Constructing Grounded Theory (Kathy Charmaz, 2006). *Slideshare*.

Colby, K. M., Weber, S., & Hilf, F. D. (1971). Artificial paranoia. *Artificial Intelligence*, *2*(1), 1–25.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10).

Creswell, J. W. (2013). Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research. In *Journal of Chemical Information and Modeling*. https://doi.org/10.1017/CBO9781107415324.004

Darktrace. (2019). Darktrace | Technology. Retrieved June 24, 2019, from https://www.darktrace.com/en/technology/

Dasgupta, D. (2006). Computational intelligence in cyber security. *2006 IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety*, 2–3. IEEE.

Davies, E. R. (2004). *Machine vision: theory, algorithms, practicalities*. Elsevier.

DCSO. (2019). DCSO – Engineering Security. Retrieved July 20, 2019, from https://dcso.de/

Dejoux, C., & Léon, E. (2018). *Métamorphose des managers...: à l'ère du numérique et de l'intelligence artificielle*. Pearson.

Deng, L., & Yu, D. (2014). Deep learning: methods and applications. *Foundations and Trends® in Signal Processing*, *7*(3–4), 197–387.

Denning, P. J. (1986). The science of computing: Expert systems. *American Scientist*, *74*(1), 18–20.

Deutsche Welle. (2019). Angela Merkel and hundreds of German politicians hacked | News | DW | 04.01.2019. Retrieved June 27, 2019, from https://www.dw.com/en/angela-merkel-and-hundreds-of-german-politicians-hacked/a-46955419

Deutschland Sicher im Netz. (2016). SicherheitsMonitor 2016. Retrieved June 27, 2019, from https://www.sicher-im-netz.de/node/1675

Dewdney, C. (1998). *Last flesh: Life in the transhuman era*. Harper San Francisco.

Dirican, C. (2015). The Impacts of Robotics, Artificial Intelligence On Business and Economics. *Procedia - Social and Behavioral Sciences*. https://doi.org/10.1016/j.sbspro.2015.06.134

Dormehl, L. (2019). What is an artificial neural network? Here's everything you need to know | Digital Trends. Retrieved June 29, 2019, from https://www.digitaltrends.com/cool-tech/what-is-an-artificial-neural-network/

Ebenroth, C. T., Boujong, K., Joost, D., & Strohn, L. (2014). Handelsgesetzbuch: HGB, Band 1 (§§ 1–342e), 3. *Auflage, München*.

Finally safe. (2019a). Advanced Security Analytics Platform - finally safe (en). Retrieved July 23, 2019, from https://www.finally-safe.com/product/

Finally safe. (2019b). The company - finally safe (en). Retrieved July 23, 2019, from https://www.finally-safe.com/company/

Financial times. (2018). Inside Darktrace, the UK's $1.65bn cyber security start-up. Retrieved July 29, 2019, from https://www.ft.com/content/2fa5bade-cb09-11e8-9fe5-24ad351828ab

German Federal Ministry of education and research. (2019). Cybersecurity research to boost Germany's competitiveness - BMBF. Retrieved July 20, 2019, from https://www.bmbf.de/en/cybersecurity-research-to-boost-germany-s-competitiveness-1418.html

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., … Bengio, Y. (2014). Generative adversarial nets. *Advances in Neural Information Processing Systems*, 2672–2680.

Google. (2016). AlphaGo Korea | DeepMind. Retrieved June 24, 2019, from

https://deepmind.com/research/alphago/alphago-korea/

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, *2*(1), 13–20.

Guttman, B., & Roback, E. A. (1995). *An introduction to computer security: the NIST handbook*. DIANE Publishing.

Hall, S. (2017). Darktrace Automates Network Security Through Machine Learning - The New Stack. Retrieved July 22, 2019, from https://thenewstack.io/darktrace-applies-math-unsupervised-machine-learning-automate-network-security/

Heinl, C. H. (2014). Artificial (intelligent) agents and active cyber defence: Policy implications. *2014 6th International Conference On Cyber Conflict (CyCon 2014)*, 53–66. IEEE.

Hiscox. (2019). *Cyber Readiness Report 2019*. Retrieved from www.hiscoxgroup.com.

IBM. (2018). Understanding the Relationship Between AI and Cybersecurity. Retrieved July 12, 2019, from https://securityintelligence.com/understanding-the-relationship-between-ai-and-cybersecurity/

IDC. (2019). Worldwide Spending on Artificial Intelligence Systems Will Grow to Nearly $35.8 Billion in 2019, According to New IDC Spending Guide. Retrieved June 25, 2019, from https://www.idc.com/getdoc.jsp?containerId=prUS44911419

Interpol. (2019). Cybercrime. Retrieved June 25, 2019, from https://www.interpol.int/en/Crimes/Cybercrime

Jahankhani, H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. In *Cyber Crime and Cyber Terrorism Investigator's Handbook* (pp. 149–164). Elsevier.

Jain, A. K., Mao, J., & Mohiuddin, K. M. (1996). Artificial neural networks: A tutorial. *Computer*, (3), 31–44.

Jarrahi, M. H. (2018). Artificial intelligence and the future of work: human-AI symbiosis in organizational decision making. *Business Horizons*, *61*(4), 577–586.

Jean-Philippe, R. (2018). *Enhancing Computer Network Defense Technologies with Machine Learning and Artificial Intelligence*. Utica College.

Jose, S., Malathi, D., Reddy, B., & Jayaseeli, D. (2018). A survey on anomaly based host intrusion detection system. *Journal of Physics: Conference Series*, *1000*(1), 12049. IOP Publishing.

Kurzweil, R., Richter, R., & Schneider, M. L. (1990). *The age of intelligent machines* (Vol. 579). MIT press Cambridge, MA.

Li, J. (2018). Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, *19*(12), 1462–1474.

Lingenheld, M. (2015). The Unfortunate Growth Sector: Cybersecurity. Retrieved July 1, 2019, from https://www.forbes.com/sites/michaellingenheld/2015/04/27/the-unfortunate-growth-sector-cybersecurity/#743a6f2f7574

López, G., Quesada, L., & Guerrero, L. A. (2017). Alexa vs. Siri vs. Cortana vs. Google assistant: a comparison of speech-based natural user interfaces. *International Conference on Applied Human Factors and Ergonomics*, 241–250. Springer.

Loucks, J., Davenport, T., & Schatsky, D. (2018). *State of AI in the Enterprise, 2nd Edition*. 26.

Luger, G. F., & Chakrabarti, C. (2017). From Alan Turing to modern AI: practical solutions and an implicit epistemic stance. *AI & SOCIETY*, *32*(3), 321–338.

Martínez-López, F. J., & Casillas, J. (2013). Artificial intelligence-based systems applied in industrial marketing: An historical overview, current and future insights. *Industrial Marketing Management*. https://doi.org/10.1016/j.indmarman.2013.03.001

Matthias, A. (2004). The responsibility gap: Ascribing responsibility for the actions of learning automata. *Ethics and Information Technology*, *6*(3), 175–183.

McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A proposal for the dartmouth summer research project on artificial intelligence, august 31, 1955. *AI Magazine*, *27*(4), 12.

Medvidovic, N., & Taylor, R. N. (2010). Software architecture: foundations, theory, and practice. *Proceedings of the 32nd ACM/IEEE International Conference on Software Engineering-Volume 2*, 471–472. ACM.

Morel, B. (2011). Artificial intelligence and the future of cybersecurity. *Proceedings of the*

4th ACM Workshop on Security and Artificial Intelligence, 93–98. ACM.

Morgan, S. (2017). Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021 | CSO Online. Retrieved June 25, 2019, from https://www.csoonline.com/article/3200024/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html

Morik, K. (1989). *Knowledge representation and organization in machine learning*. Springer.

Murphy, R., & Murphy, R. R. (2000). *Introduction to AI robotics*. MIT press.

Nogueira, J. (2011). Mobile Intelligent Agents to Fight Cyber Intrusions. *The International Journal of Forensic Computer Science*. https://doi.org/10.5769/j200601003

Normshield. (2019). Cyber Security with Artificial Intelligence in 10 Question | NormShield Cyber Risk Scorecard. Retrieved June 23, 2019, from https://www.normshield.com/cyber-security-with-artificial-intelligence-in-10-question/

Oke, S. A. (2008). A literature review on artificial intelligence. *International Journal of Information and Management Sciences*, *19*(4), 535–570.

Pan, Y. (2016). Heading toward Artificial Intelligence 2.0. *Engineering*. https://doi.org/10.1016/J.ENG.2016.04.018

Pankit, D. (2018). Is Cybersecurity Required For SMEs? Retrieved July 20, 2019, from https://www.entrepreneur.com/article/323943

Qu, F., Zhang, J., Shao, Z., & Qi, S. (2017). An intrusion detection model based on deep belief network. *Proceedings of the 2017 VI International Conference on Network, Communication and Computing*, 97–101. ACM.

Raina, R., Battle, A., Lee, H., Packer, B., & Ng, A. Y. (2007). Self-taught learning: transfer learning from unlabeled data. *Proceedings of the 24th International Conference on Machine Learning*, 759–766. ACM.

Randrianasolo, A. (2012). *Artificial intelligence in computer security: Detection, temporary repair and defense*.

Robertson, S., Azizpour, H., Smith, K., & Hartman, J. (2018). Digital image analysis in breast pathology—from image processing techniques to artificial intelligence.

Translational Research. https://doi.org/10.1016/j.trsl.2017.10.010

Samuel, A. L. (1988). Some Studies in Machine Learning Using the Game of Checkers. II—Recent Progress. In *Computer Games I* (pp. 366–400). Springer.

Schatz, D., Bashroush, R., & Wall, J. (2017). Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law*, *12*(2), 8.

Schmidt, J. (2019). Antivirus: Cylance-KI böse ausgetrickst | heise online. Retrieved July 30, 2019, from https://www.heise.de/security/meldung/Antivirus-Cylance-KI-boese-ausgetrickst-4477463.html

Skype. (2019). Skype | Communication tool for free calls and chat. Retrieved July 12, 2019, from https://www.skype.com/en/

Stacey, M., Clarkson, P. J., & Eckert, C. (1999). *Signposting: an AI approach to supporting human decision making in design*. Citeseer.

Susskind, R. E., & Susskind, D. (2015). *The future of the professions: How technology will transform the work of human experts*. Oxford University Press, USA.

Syam, N., & Sharma, A. (2018). Waiting for a sales renaissance in the fourth industrial revolution: Machine learning and artificial intelligence in sales research and practice. *Industrial Marketing Management*. https://doi.org/10.1016/j.indmarman.2017.12.019

Tegmark, M. (2017). *Life 3.0: Being human in the age of artificial intelligence*. Knopf.

Turing, A. (1950). Computing machinery and intelligence-AM Turing. *Mind and Quarterly Review of Psychology and Philosophy*.

Tyugu, E. (2011). Artificial intelligence in cyber defense. *Cyber Conflict (ICCC), 2011 3rd International Conference On*. https://doi.org/CFP1126N-PRT

Veiga, A. P. (2018). Applications of artificial intelligence to network security. *ArXiv Preprint ArXiv:1803.09992*.

Vieira, H. (2017). Nicole Eagan:“Cybersecurity is very fast becoming an all-out arms race.” *LSE Business Review*.

Wang, K., & Wang, Y. (2018). How AI Affects the Future Predictive Maintenance: A Primer of Deep Learning. *Lecture Notes in Electrical Engineering*.

https://doi.org/10.1007/978-981-10-5768-7_1

Wang, X., Yang, G., Li, Y., & Liu, D. (2008). Review on the application of artificial intelligence in antivirus detection system i. *2008 IEEE Conference on Cybernetics and Intelligent Systems*, 506–509. IEEE.

White House's National Science and Technology Council. (2016). *Preparing for the future of artificial intelligence. Executive Office of the President National Science and Technology Council. Committee on Technology*.

Winder, D. (2016). AI could rescue failing cyber security sector - Raconteur. Retrieved June 23, 2019, from https://www.raconteur.net/technology/ai-could-rescue-failing-cyber-security-sector

Wolfe, A. (1991). Mind, self, society, and computer: Artificial intelligence and the sociology of mind. *American Journal of Sociology*, *96*(5), 1073–1096.

World Economic Forum. (2019). Centre for Cybersecurity. Retrieved July 3, 2019, from https://www.weforum.org/centre-for-cybersecurity

Xin, Y., Kong, L., Liu, Z., Chen, Y., Li, Y., Zhu, H., … Wang, C. (2018). Machine learning and deep learning methods for cybersecurity. *IEEE Access*, *6*, 35365–35381.

Yar, M., & Steinmetz, K. (2019). Cybercrime and society. In *SAGE Publications Limited.*

10. APPENDIX

Appendix 1: Introduction and approach for interviews - original

Interview Fragebogen

FUNDAÇÃO GETULIO VARGAS

- ⇨ *Begrüßung und persönliche Vorstellung*
- ⇨ *Informationen welche den Projektrahmen umschreiben*

Lieber Interviewteilnehmer,

vielen Dank für Ihre Teilnahme und der Unterstützung meiner Masterthesis. Das Interview kann zwischen 20-60 Minuten dauern. Mit meiner Masterarbeit untersuche ich die Cybersecurity Industrie und spezialisiere mich in diesem Bereich auf die Anwendung von künstlicher Intelligenz für kleine und mittelständige Unternehmen in Deutschland. Selbstverständliche teile ich nach der Fertigstellung meine Thesis mit Ihnen. Für eine bessere Analyse meiner Ergebnisse frage ich Sie höflichst, ob ich das Interview für eine spätere Analyse aufzeichnen kann. Die Aufnahmen werden NUR für das verschriftlichen der Ergebnisse in meiner Masterthesis verwendet und nach der Fertigstellung unverzüglich gelöscht (bis spätestens 31.12.2019). Aufgrund der sehr vertraulichen Informationen werde ich meine Ergebnisse anonymisiert veröffentlichen.

Falls Sie weitere Fragen hinsichtlich meiner Thesis haben, kontaktieren Sie mich gerne unter der E-Mail-Adresse simon.doerpinghaus@gmail.com

Abschließend bedanke ich mich bei Ihnen nochmals herzlichst,

Simon Dörpinghaus

Appendix 2: Introduction and approach for interviews - translated

Interview questionnaire

- ⇨ Welcome and introduction
- ⇨ Information describing the project scope

Dear study participant,

Thank you for your participation and the support of my master thesis. The interview can take between 20 and 60 minutes. My Master's dissertation examines the cybersecurity industry and specializes in the application of artificial intelligence for small and medium-sized enterprises in Germany. Certainly, I can share my results with you after completion. For a better analysis of my results, I politely ask you for permission to record the interview for later analysis. The recordings are used solely for the writing process of my master thesis and are deleted immediately after completion (until 31.12.2019 at the latest). To tackle confidentiality issues, I will publish the results anonymously.

If you have further questions regarding my thesis, feel free to contact me via this email address simon.doerpinghaus@gmail.com

Warm regards,

Simon Dörpinghaus

Appendix 3: Questions regarding the participant's background - original

Fragen zum Hintergrund der befragten Person

Sie sind: **männlich/weiblich/divers**

Wie lange arbeiten Sie schon in der Organisation? _____Jahre

Welche Position bekleiden Sie momentan? _____

Wie lange halten Sie schon diese Position? _____Jahre

Bitte wählen Sie eine Beschreibung welche am besten auf Ihre Arbeit zutrifft:

□ Management □ IT Abteilung □ Software Provider

□ Industrieverband

Appendix 4: Questions regarding the participant's background - translated

Questions regarding the participant's background

You are: **male / female / divers**

How long have you been working in the organization? _____years

Which position do you currently hold? _____

How long have you been working at this position? _____years

Please select a description that best suits your work:

□ Management □ IT Department □ Software Provider

□ Industry Association

Appendix 5: Questions to SMEs - original

Fragebogen KMUs:

A) Fragen zu der Entwicklung von Cybersecurity im Unternehmen:

1. Wie sehen Sie persönlich den Stellenwert von Cybersecurity?
2. Wie wichtig ist in Ihrem Unternehmen Cybersecurity, wie hoch ist der Stellenwert für das Management?
3. Wie hat sich der Stellenwert von Cybersecurity für das Management über die letzten Jahre entwickelt?
4. Wurde in den letzten Jahren das Computersystem/Netzwerk des Unternehmens gezielt angegriffen und ist ein Schaden entstanden?
5. Was wurde die letzten Jahre unternommen, um die Sicherheit im Bereich Cybersecurity zu erhöhen?
6. Welche Anforderungen haben Sie an Cybersecurity Systeme, welche Kriterien würden Ihnen einfallen?

B) Fragen zu Einfluss von Größe des Unternehmens auf Cybersecurity:

1. Welche Probleme im Bereich Cybersecurity haben andere Unternehmen ähnlich zu Ihrer Größe?
2. Welchen Einfluss hat der Fachkräftemangel im Bereich Cybersecurity, insbesondere für KMUs?
3. Welche Unterschiede bestehen zwischen der Cybersecurity von KMUs und größeren Unternehmen?

C) Fragen zu KI basierten Cybersecurity Lösungen:

1. Haben Sie schon von KI basierten Cybersecurity Lösungen gehört?
2. Wie würden Sie die KI basierten Cybersecurity Systeme definieren?
3. Wie helfen diese Algorithmen das Unternehmen vor Cyberangriffen zu schützen?
4. Wie schätzen Sie die KI basierten Systeme im Hinblick auf „Intrusion detection systems“ (IDS) ein?
5. Wie schätzen Sie die KI basierten Systeme im Hinblick auf das Störungsmanagement ein? (Antwort des Unternehmens, wenn das System angegriffen wird)
6. Wie schätzen Sie die KI basierten Systeme hinsichtlich der „Usability“ für IT Experten im Unternehmen ein?
7. Welche der drei Kategorien (Intrusion Detection, Störungsmanagement, Usability) in der Cybersecurity Software hat für Sie den höchsten Stellenwert und warum?
8. Würden Sie ein KI basiertes Cybersecurity System kaufen?
9. In welchem Cybersecurity Bereich würden Sie eine KI basierte Lösung kaufen?
10. Was müsste sich verändern, damit Sie eine solches System kaufen würden?
11. Was ist Ihre persönliche Meinung, wie sich KI und Cybersecurity entwickeln werden?

Appendix 6: Questions to SMEs - translated

Questionnaire SMEs:

A) Questions about the development of cybersecurity in the enterprise:

1. How do you view the significance of cybersecurity?
2. How important is cybersecurity in your company, how important is it for the management?
3. How has the importance of cybersecurity for management evolved over the last few years?
4. Have the computer systems / networks of the company been targeted in recent years and has damage incurred?
5. What has been done the last years to increase cybersecurity?
6. What requirements do you have for cyber security systems, which criteria would you consider?

B) Questions about the influence of the size of the company on cybersecurity:

1. What problems in cybersecurity do other companies have, similar to your size?
2. What impact does the skill shortage in cybersecurity have, especially for SMEs?
3. What differences exist between cybersecurity of SMEs and larger companies?

C) Questions about AI-based cybersecurity solutions:

1. Have you heard about AI-based cybersecurity solutions?
2. How would you define the AI-based cybersecurity systems?
3. How do these algorithms help to protect the company from cyber-attacks?
4. How do you assess the AI-based systems regarding intrusion detection systems (IDS)?
5. How do you assess the AI-based systems in terms of response systems? (Company's response when the system is attacked)
6. How do you assess the AI-based systems in terms of usability for the IT department?
7. Which of the three categories (Intrusion Detection, response systems, Usability) in the cybersecurity software has the highest importance to you and why?
8. Would you buy an AI-based cybersecurity system?
9. In which of the before mentioned categories would you buy an AI-based solution?
10. What would have to change for you to buy such a system?
11. What is your opinion on how AI and cybersecurity will evolve in the future?

Appendix 7: Questions to business associations - original

Fragebogen öffentliche Organisationen:

A) Fragen zu der Entwicklung von Cybersecurity in Unternehmen:

1. Wie sehen Sie persönlich den Stellenwert von Cybersecurity?
2. Wie hoch ist der Stellenwert von Cybersecurity für Management von Unternehmen?
3. Wie hat sich der Stellenwert von Cybersecurity für das Management über die letzten Jahre entwickelt?
4. Welche Cybersecurity Lösungen haben das Umfeld die letzten Jahre stark geprägt?
5. Nach welchen Kriterien werden Cybersecurity Systeme ausgewählt?

B) Fragen zu Einfluss von Größe des Unternehmens auf Cybersecurity:

1. Welche Probleme im Bereich Cybersecurity haben KMUs?
2. Welchen Einfluss hat der Fachkräftemangel im Bereich Cybersecurity insbesondere für KMUs?
3. Welche Unterschiede bestehen zwischen der Cybersecurity von KMUs und größeren Unternehmen?

C) Fragen zu KI basierten Cybersecurity Lösungen:

1. Haben Sie schon von KI basierten Cybersecurity Lösungen gehört?
2. Wie würden Sie die KI basierten Cybersecurity Systeme definieren?
3. Wie helfen diese Algorithmen das Unternehmen vor Cyberangriffen zu schützen?
4. Wie schätzen Sie die KI basierten Systeme im Hinblick auf „Intrusion detecion systems“ (IDS) ein?
5. Wie schätzen Sie die KI basierten Systeme im Hinblick auf das Störungsmanagement ein? (Antwort des Unternehmens, wenn das System angegriffen wird)
6. Wie schätzen Sie die KI basierten Systeme hinsichtlich der „Usablity“ für IT Experten im Unternehmen ein?

Appendix 8: Questions to business associations – translated

Questionnaire business associations:

A) Questions about the development of cybersecurity in the enterprise:

1. How do you view the significance of cybersecurity?
2. How important is cybersecurity in companies, how important is it for the management?
3. How has the importance of cybersecurity for management evolved over the last few years?
4. Which cybersecurity solutions have significantly shaped the ecosystem in recent years?
5. According to which criteria are cybersecurity systems selected?

B) Questions about the influence of the size of the company on cybersecurity:

1. What problems in cybersecurity do SMEs face?
2. What impact does the skill shortage in cybersecurity have, especially for SMEs?
3. What differences exist between cybersecurity of SMEs and larger companies?

C) Questions about AI-based cybersecurity solutions:

1. Have you heard about AI-based cybersecurity solutions?
2. How would you define the AI-based cybersecurity systems?
3. How do these algorithms help to protect the company from cyber-attacks?
4. How do you assess the AI-based systems regarding intrusion detection systems (IDS)?
5. How do you assess the AI-based systems in terms of response systems? (Company's response when the system is attacked)
6. How do you assess the AI-based systems in terms of usability for the IT department?

Appendix 9: Question to cybersecurity providers - original

Fragebogen Cybersecurity Provider:

A) Fragen zu der Entwicklung von Cybersecurity in Unternehmen:

1. Wie sehen Sie persönlich den Stellenwert von Cybersecurity?
2. Wie hat sich der Stellenwert von Cybersecurity für das Management von Unternehmen über die letzten Jahre entwickelt?
3. Welche Cybersecurity Lösungen haben das Umfeld die letzten Jahre stark geprägt?
4. Nach welchen Kriterien werden Cybersecurity Systeme ausgewählt?

B) Fragen zu Einfluss von Größe des Unternehmens auf Cybersecurity:

1. Welche Probleme im Bereich Cybersecurity haben KMUs?
2. Welchen Einfluss hat der Fachkräftemangel im Bereich Cybersecurity insbesondere für KMUs?
3. Welche Unterschiede bestehen zwischen der Cybersecurity von KMUs und größeren Unternehmen?

C) Fragen zu KI basierten Cybersecurity Lösungen:

1. Wie würden Sie KI-basierte Cybersecurity Lösungen definieren?
2. Wie würden Sie Ihre angebotenen Produkte definieren?
3. Benutzt Ihre Software „machinen learning“ oder „deep learning“ Algorithmen?
4. Wie helfen diese Algorithmen das Unternehmen vor Cyberangriffen zu schützen?
5. Wie schätzen Sie die KI basierten Systeme im Hinblick auf „Intrusion detecion systems“ (IDS) ein?
6. Wie schätzen Sie die KI basierten Systeme im Hinblick auf das Störungsmanagement ein? (Antwort des Unternehmens, wenn das System angegriffen wird)
7. Wie schätzen Sie die KI basierten Systeme hinsichtlich der „Usability“ für IT Experten im Unternehmen ein?

Appendix 10: Question to cybersecurity providers - translated

Questionnaire to cybersecurity provider:

A) Questions about the development of cybersecurity in the enterprise:

1. How do you view the significance of cybersecurity?
2. How has the importance of cybersecurity for management evolved over the last few years?
3. Which cybersecurity solutions have significantly shaped the ecosystem in recent years?
4. According to which criteria are cybersecurity systems chosen nowadays?

B) Questions about the influence of the size of the company on cybersecurity:

1. What problems in cybersecurity do SMEs face?
2. What impact does the skill shortage in cybersecurity have, especially for SMEs?
3. What differences exist between cybersecurity of SMEs and larger companies?

C) Questions about AI-based cybersecurity solutions:

1. How would you define the AI-based cybersecurity systems?
2. How would you define your cybersecurity solution?
3. Does your software use machine learning or deep learning algorithms?
4. How do these algorithms help to protect the company from cyber-attacks?
5. How do you assess the AI-based systems regarding intrusion detection systems (IDS)?
6. How do you assess the AI-based systems in terms of response systems? (Company's reponse when the system is attacked)
7. How do you assess the AI-based systems in terms of usability for the IT department?