LUND UNIVERSITY
School of Economics and Management

Department of Informatics

Addressing Cyberthreats:

Exploring the Intersection of AI and Cybersecurity Frameworks in the EU

Master thesis 15 HEC, course INFM10 in Information Systems

Authors: Mumbi Eugene Mwelwa
Christos Kyprianou

Supervisor: Osama Mansour

Grading Teachers: Niki Chatzipanagiotou
Odd Steen

Addressing Cyberthreats:

Exploring the Intersection of AI and Cybersecurity Frameworks in the EU

AUTHORS: Mumbi Eugene Mwelwa and Christos Kyprianou

PUBLISHER: Department of Informatics,
Lund School of Economics and Management, Lund University

PRESENTED: May, 2024

DOCUMENT TYPE: Master Thesis

FORMAL EXAMINER: Osama Mansour, Associate Professor

NUMBER OF PAGES: 75

KEY WORDS: Artificial Intelligence, Cybersecurity, Frameworks, Cyberthreats.

ABSTRACT (MAX. 200 WORDS):
The complexity and frequency of cyberthreats continue to escalate as IT systems become increasingly central to our society. This thesis explores the role of human expertise along with AI technologies in improving cybersecurity frameworks within the EU. By integrating AI, organisations can improve threat detection and response times and navigate the evolving landscape of digital threats more effectively. AI does not only present numerous opportunities, but also challenges and risks. This complexity partly stems from the broad and varied definitions of AI, which encompass a diverse range of technologies, processes, and actors. This research employed a qualitative approach, combining a comprehensive literature review with interviews and insights from industry professionals, EU agents, and Swedish authorities. The findings underscore the critical need for policy frameworks that adapt to technological advancements and highlight the dual-use nature of AI in cybersecurity, which presents both opportunities and challenges. The study offers insights into practical applications of AI in cybersecurity, recommending strategic approaches for EU organisations to harness AI's potential while mitigating associated risks. Future research directions are suggested to address the rapid pace of AI development and its implications for cybersecurity strategies.

Table of Contents

Figures

Tables

List of Abbreviations

Abbreviation	Definition	Abbreviation	Definition
AI	Artificial Intelligence	ISC2	International Information System Security Certification Consortium
AIA	Artificial Intelligence Act	ISACA	Information Systems Audit and Control Association
API	Application Programming Interface	ISO	International Organization for Standardization
APT	Advanced Persistent Threat	IT	Information Technology
AR	Association Rule	ITU	International Telecommunication Union
BEV	Battery Electric Vehicle	JRC	Joint Research Centre
BEC	Business E-mail Compromise	KNN	K-Nearest Neighbour
BGP	Border Gateway Protocol	LLM	Large Language Model
CEN	European Committee for Standardization	ML	Machine Learning
CENELEC	European Committee for Electrotechnical Standardization	MM	Mumbi Mwelwa
CERT	Computer Emergency Response Team	NIS	Network and Information Systems
CISSP	Certified Information Systems Security Professional	NIST	National Institute of Standards and Technology
CK	Christos Kyprianou	NN	Neural Networks
CNN	Convolutional Neural Networks	NSCAI	National Security Commission on Artificial Intelligence
CSA	Cyber Security Act	PCA	Principal Component Analysis
CTO	Chief Technology Officer	P1	Participant 1
DBN	Deep Belief Networks	P2	Participant 2
DDoS	Distributed Denial of Service	P3	Participant 3
DL	Deep Learning	P4	Participant 4
DT	Decision Trees	P5	Participant 5
EDLN	Ensemble of Deep Learning Networks	P6	Participant 6
EL	Ensemble Learning	P7	Participant 7
ENISA	European Network and Information Security Agency	RBM	Restricted Boltzmann Machines
EU	European Union	RDoS	Ransomware Denial of Service
EU-LISA	European Union – Large-scale Information Systems Agent	RF	Random Forest
FFN	Feedforward Neural Networks	RMF	Risk Management Framework
FMV	Försvarets Materielverk	RNN	Recurrent Neural Networks

GAN	Generative Adversarial Networks	SAE	Stacked Autoencoders
GDPR	General Data Protection Regulation	SIM	Subscriber Identity Module
GPT	Generative Pre-Trainer Transformer	SMEs	Small and medium-sized enterprises
GPU	Graphics Processing Unit	SVM	Support Vector Machine
GSM	Graduate School of Management	SWIFT	Society for Worldwide Interbank Financial Telecommunications
HTTPS	Hypertext Transfer Protocol Secure	TLS	Transport Layer Security
IEC	International Electrotechnical Commission	UN	United Nations
ICC	Inspektionen för cyber säkerhets-certifiering	UNIDIR	United Nations Institute for Disarmament Research
ICT	Information and Communication Technologies	URL	Uniform Resource Locator
IoT	Internet-of-Things	USA	United States of America
IS	Information Systems	USD	US Dollars

Table 1: List of Abbreviations

1 Introduction

This chapter will introduce the background, the problem and the purpose of the study. Additionally, the research aims, research questions and the delimitations of the study are presented.

1.1 Background

In recent years, we have been surrounded by IT and its applications, and they have become crucial to our lives. The applications of IT have become very important for our work and lives, and we have become progressively dependent on them (Shoemaker and Conklin, 2011). However, this does not mean that we fully understand our digital world. There is a recognized gap in understanding what cybersecurity is, what it does and what affects it, despite efforts to increase overall security (Frisk et al., 2023). It is extremely important to understand cybersecurity as it is a crucial component in society, its individuals, and organisations (Frisk et al., 2023).

Today, cybersecurity has been considered one of the most highly mentioned topics that is circulated frequently among companies and organisations to protect their data from hacking operations (Mijwil and Aljanabi, 2023). The term cyberspace is explained by Mijwil and Aljanabi, (2023) as the virtual digital space that creates the possibility for computers to connect with each other or with other electronic devices within the IoT environment and utilises AI techniques to protect its data against any wrong operations. As per Patel (2023) with the use of AI, the possibility of a security threat is decreased, and the level of security is increased. Cybercrime has become one of the biggest challenges that companies, organisations, and individuals are facing according to Button et al. (2022). In line with this is Campina and Rodrigues (2022), who have emphasised in their study that cybercrime is one of the hardest crimes to face, mainly due to its international reach. It has been emphasised by Mijwil and Aljanabi (2023), that cybercrime disrupts the digital world through data manipulation, intelligence, threats, and illegal content, affecting both individuals and businesses. Amongst others, this includes hacking, identity theft, and malware.

Similarly, Arpaci and Aslan (2023) have stated that cybercrime affects the performance of computers as well as the psychological state of users. Theft, alteration, or deletion of the data is one of the most dangerous occurrences that companies, organisations, or individuals face. Consequently, seeking the use of modern and advanced technologies in developing the systems and protecting the customers' data is essential (Mijwil and Aljanabi, 2023), although privacy will not be the focus of this research study. As per Campina and Rodrigues (2022), the battle against cybercrime involves different parties using a range of strategies and cutting-edge technologies. These methods and tools are constantly evolving and often remain undetected by even the most advanced security systems (Campina and Rodrigues, 2022).

Since the rise of personal computers in the 1970s and 1980s, cybercrime has continually increased, not only in frequency but also in cost (Lee and Holt, 2020). Initially, cybercrimes targeted businesses and national security, but now they encompass all illegal acts including those against computer data and systems. This includes unauthorised access or modification without geographic limits, leaving only digital traces, as described by Frisk et al. (2023). In recent years, cybercrime has also begun to adopt the use of AI algorithms to initiate untraceable attacks and to create the spread of fake information (Alzboon et al, 2023). Mathew (2021) interestingly introduced a concept of the dual role of AI to both allow for automated detection of cybercrimes whilst also potentially being the source of initiating complex attacks. There is evidently a need then, for more enterprises to find smart ways of protecting themselves from the manipulation of modern day cyber risks that stand the chance of compromising their corporate data integrity.

AI is a trending subject nowadays and is already impacting organisations, societies, and individuals (Dwivedi et al., 2023) playing a key role in digital transformation through its automated capabilities. The benefits of this emerging technology are significant, but so are the challenges. AI could play a crucial role in enhancing cybersecurity by assisting in crime analysis and protection of networks and users, however, its high resource demand and potential misuse by hackers are prominent concerns, as emphasised by Patel (2023). The integration of AI can provide deeper visibility into attack surfaces, enabling rapid response to incidents and improved management of digital risks (Dilek et al., 2015). Cybercriminals are using AI algorithms or changing the behaviour of AI systems to penetrate networks to steal and manipulate data (Dilek et al., 2015). Various incidents have already taken place and demonstrated the complexity and evolving nature of cyberthreats, emphasising the importance of AI in enhancing cybersecurity measures (Dilek et al., 2015).

1.2 Research Problem

According to Jada and Mayayise (2023) in the modern era of digitisation, organisations are recognising the potential and higher risks that come with the adoption of novel technologies, and specifically highlight that there is merit in exploring the use of AI in cybersecurity. In identifying seven trends for proactive cybersecurity in 2024, ISACA listed the rise of AI in cybersecurity as their number one (ISACA, 2024). Whilst AI has the great potential to detect cyberthreats that human beings do not identify as quickly, it also presents some risks including that of systems being taken advantage of by attackers. It is known that the integration of AI in cybersecurity presents significant challenges, primarily due to the inadequacies in the current legal and regulatory frameworks related to data protection, privacy, and security in the EU (Hadzovic et al., 2023). The rapid evolution of AI-driven cyberthreats highlights a critical skills gap in the current workforce, as identified by Thakur (2024). There is a notable deficiency in professionals trained in AI-driven cybersecurity practices, amplifying the challenge of effectively countering emerging cyberthreats (Ghelani, 2023). This shortage of skilled personnel is a significant barrier to leveraging AI's full potential in cybersecurity.

Despite the urgency, an analysis reveals a gap in the literature, particularly in IS research. A keyword search of "artificial intelligence AND cybersecurity" in the major eleven information systems journals yields fewer than forty relevant results, indicating a lack of

focused academic discussion on AI's role in enhancing cybersecurity within the EU. Zeadally et al. (2020, p23832) identified a few areas for future research indicating that "it is imperative to investigate how AI can be employed for human basic needs and for developing cybersecurity controls". They further observed that while AI's role in addressing cybersecurity issues is still being explored, there are fundamental concerns about how it can be regulated. The AI economy is projected to significantly impact the global market, reaching an estimated €13 trillion by 2030 (EU Publications, 2017). With the potential to introduce more complex threats and opportunities, the need for AI integration into cybersecurity frameworks becomes more crucial.

The main research problem being addressed is the need to develop effective AI-inclusive cybersecurity frameworks and strategies within the EU, among evolving AI-driven cyberthreats and a shortage of skilled professionals in AI cybersecurity. This involves exploring existing regulations and identifying gaps in expertise.

1.3 Purpose

The interest of the researchers incorporates the regulatory framework that supports the integration of AI in cybersecurity which now presents an essential moment in technological advancement within the EU. This integration offers major opportunities to enhance cyber defense processes and tools but also introduces complex challenges and limitations that need to be carefully navigated. With the dynamic nature of AI technologies, there is a demanding need to align cybersecurity policies and practices with emerging challenges. The AI technologies must not only be able to protect against evolving threats but also be flexible enough to adapt to technological advancements. The EU, with its unique blend of diverse socio-political landscapes and strict regulations, stands at the forefront of addressing these challenges.

In addition, the purpose of this Master's thesis study was to investigate some of the challenges the cybersecurity landscape in the EU is facing. In particular, this study examines the skills gap, the interplay between human expertise and AI technologies, and the regulatory framework impacting cybersecurity practices. This investigation is driven by the need to understand how these factors collectively influence the effectiveness of cybersecurity measures across the EU. By dissecting the dynamics of human-AI collaboration and the current policy environment, this research clarifies some of the underlying challenges and opportunities that these factors present, assisting in improving and fostering a safer digital environment in the EU.

1.4 Research Aims

This research aims to explore the cybersecurity landscape in the EU, focusing on the existing skills gap, the dynamics of human-AI collaboration, and the impact of current EU cybersecurity policies and frameworks. This Master's thesis study aims to clarify how these factors influence the effectiveness of cybersecurity measures and contribute to the overall security posture of the EU.

1.5 Research Questions

This research question provides a solid foundation for our investigation into the complexities of AI integration in cybersecurity frameworks and the associated skills development challenges and legal implications within the EU context. In the context of this Master's thesis, the research question is formulated as follows:

What are the implications of integrating AI technologies into cybersecurity within EU organisations, and how do current regulations and guidelines facilitate or delay this integration?

1.6 Delimitation

The focus of this study is to investigate how human expertise, coupled with AI technologies, can enhance cybersecurity within EU organisations. Additionally, this research explores the primary challenges and opportunities associated with integrating AI into cybersecurity frameworks specifically in the EU.

The study is based on a small sample size, comprising only seven interviews conducted in Greece and Sweden. This limited sample size and geographical focus restricts the generalisability of the findings, as they might not reflect broader perspectives in the field of AI and cybersecurity. Furthermore, the four-month duration of the study limits the depth of data analysis, potentially leading to a more shallow understanding of the complex issues involved. The qualitative nature of the research also introduces a degree of subjectivity in data interpretation, which could be influenced by personal biases. Additionally, due to the fast-paced nature of technological advancements in AI and cybersecurity, this research may not fully capture the latest developments or emerging trends. These limitations are crucial, as they highlight areas for further investigation. A foundation for future research to build upon, is provided by understanding these constraints.

2 Literature Review

The theoretical basis of this thesis is established through an extensive review of scholarly literature relevant to the research topic. This review is essential for achieving a deep understanding of the subject under investigation. Additionally, this chapter aims to obtain a thorough understanding of the concepts employed throughout the research process.

2.1 Human-Artificial Intelligence Synergy in Cybersecurity

2.1.1 Collaboration between humans and AI

As Patel (2023) suggested, security professionals need significant assistance from intelligent machines and cutting-edge technology such as AI to do their tasks efficiently and safeguard their businesses and organisations from cyber assaults. In line with this is ENISA, where the report "Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity," published on their website emphasises that human skills and knowledge, rather than vulnerabilities, can be made to work in favour of an organisation’s defensive cybersecurity.

The benefits of applying AI in this industry are explored in this literature review. In the increasingly complex domain of cybersecurity, the collaborative interplay between AI and human insight is becoming crucial. Sinclair (2023) underscores that security protocols must evolve continually to counter advanced cyberthreats, necessitating a harmonious integration of AI mechanisms and human supervision. This necessity for a balanced approach is reinforced by various scholars who advocate for the convergence of human-centric AI frameworks with stringent cybersecurity measures (Sinclair, 2023; Nielsen, 2023).

This first part of the literature review discusses the role of collaborative solutions and the importance of human-machine collaboration in developing strong and agile cybersecurity frameworks (Petrović and Jovanović, 2024). In their paper, Petrović and Jovanović (2024), aimed to explore the current challenges, technical foundations, collaborative solutions, and strategic human-machine interaction. The vital synergy between AI capabilities and human expertise is highlighted in the literature (Sinclair, 2023; Nielsen, 2023; Bao et al., 2023) as being essential for devising intelligent and adaptable cybersecurity structures.

The integration of advanced AI technologies, including ML, DL and NLP, is redefining human-machine interactions, steering us towards a new paradigm of human-AI collaboration (Bao et al., 2023). According to Patel (2023), the application of ML is increasingly becoming an essential tool for enhancing the productivity of IT security teams. Given the complex nature of security tasks, it is impractical for an individual to effectively protect all potential vulnerabilities within a modern organisation's entry points. AI meets the high demands placed on security professionals for thorough analysis and timely threat detection. Consequently, the adoption of AI in security protocols substantially reduces the likelihood of breaches and enhances overall security levels (Patel, 2023).

Bao et al. in their paper (2023), aimed to develop a framework that methodically analyses and categorises the nuances of human-AI interactions, with a particular focus on their variations in different decision-making contexts. In the context of decision-making, AI technologies offer enhanced capabilities that significantly strengthen the process, improving decision accuracy and enhancing transparency by clarifying uncertainties and providing explanations. This progression sets the stage for a future where human and AI collaboration is co-operative, with each entity augmenting the other's strengths. The rich body of existing literature on this topic sheds light on the intricate nature of human-AI synergy, offering insights into optimising this partnership for superior outcomes (Lai et al., 2021). Within cybersecurity, this synergy is crucial for enabling individuals to harness technology securely, emphasising the collaborative interplay between humans and machines to imitate vigorous defenses. This partnership aims not to replace human intelligence but to augment it, fostering a cooperative intelligence that leverages the collective strengths of both humans and machines (Petrović and Jovanović, 2024).

Exploring the dynamics of human-AI synergy, (Lai et al., 2021) conceptualised this collaboration as a cohesive team where tasks are shared, and collective efforts aim to achieve a conclusive decision. Their findings suggest that the combination of human and AI capabilities yields superior outcomes compared to individual efforts. The roles within this team-like structure vary, with each entity, human or AI bringing distinct strengths to the table depending on the available technology. This collaborative model has demonstrated potential across various sectors, including healthcare and automotive engineering (Järvelä et al., 2023; Lawrence, 2023). While (Lai et al., 2021) acknowledge that not every decision-making process should be fully automated, Cheng et al. (2019) note that automated systems can substitute human decisions in specific scenarios, although humans often remain the ultimate decision-makers, guided by AI-generated recommendations.

Stevens (2020), highlights that AI systems are increasingly used in cybersecurity to detect cyberthreats and malware due to their effectiveness and the rise in cyber attacks, however, it has limitations and cannot entirely replace humans. According to Stevens (2020), AI may struggle with highly sophisticated or evolving threats, as it operates within predefined tasks and can miss nuances in advanced cyberthreats. Moreover, cybercriminals constantly update their methods, challenging AI's adaptability. Despite AI reducing the workload for security teams, human expertise remains crucial for addressing AI's limitations and ensuring continuous system improvement. Developers must equip AI with diverse capabilities to tackle the dynamic nature of cyberthreats effectively (Stevens, 2020). Patel (2023) highlights in his paper, the critical role of AI in enhancing organisational cybersecurity measures against a broad spectrum of potential attacks. More specifically, he suggests that it is unlikely for any individual to fully distinguish all the risks faced by an organisation, due to the diversity in motivations and methodologies among hackers. Such unidentified threats possess the capacity to cause substantial damage to network infrastructures. In this context, AI demonstrates superior capabilities compared to human efforts in detecting and mitigating novel business threats before they can cause destruction.

In the rapidly evolving field of cybersecurity, the synergy between AI and human expertise is crucial for addressing contemporary cyberthreats effectively. Patel (2023) highlights that while cybersecurity specialists have limitations in evaluating all data for potential threats, AI excels in identifying hidden dangers within the network. However, AI's capacity to interpret data with the depth of human analysis is still developing. Despite advancements towards

more human-like processing, AI capabilities, which would include the application of abstract concepts across various contexts, remain a distant goal (Patel, 2023). AI lacks the creative and critical thinking that human specialists bring to complex decision-making scenarios (Patel, 2023).

Furthermore, while ML-based network security significantly benefits from human oversight in updates and modifications, the scarcity of skilled professionals capable of providing these nuanced responses underscores the ongoing need for human collaboration (Patel, 2023). On the other hand, Trappe and Straub (2021) highlight that AI's efficiency in routine tasks has reduced the demand for traditional cybersecurity roles, as automated systems often outperform humans in maintaining and securing systems.

Kioskli et al. (2023) propose a human-centric approach to cybersecurity, emphasising collaborative intelligence where automated functions do not replace, but rather enhance, human interaction with security technologies. This model not only automates detection and response but also engages end-users actively, fostering an organisational culture that values critical thinking and proactive security practices. The framework suggested, involves assessing information handling, testing employee awareness, reviewing interactions, and promoting critical thinking skills among staff. Petrović and Jovanović (2024) further argue that human analysts are indispensable due to their unique capacity for judgement and detailed response. AI should be viewed as a supportive tool that enhances human capabilities, allowing analysts to shift their focus from routine tasks to strategic decision-making. This synergy enables a more effective response to the millions of threats organisations face daily, which individual researchers might otherwise be too slow to address. The integration of AI not only automates threat detection but also supports comprehensive data analysis, expediting the response time significantly (Prasad et al., 2020).

The collaboration between humans and AI in cybersecurity should prioritise agility, safety, and trust, ensuring human oversight remains central, especially in high-stake decisions (Petrović and Jovanović, 2024). As AI technologies become integral to security frameworks, ethical considerations such as privacy, bias, and potential misuse must be rigorously addressed. Transparent, accountable AI that adheres to ethical standards is essential for maintaining public trust and ensuring the technology's responsible use (Petrović and Jovanović, 2024).

Finally, a holistic view of cyber risk is essential, recognizing the substantial impact of human behaviour on security vulnerabilities. An effective strategy integrates awareness, education, and the promotion of cyber hygiene throughout the organisational structure, addressing the complex interplay of technical, human, and organisational factors in cybersecurity (Petrović and Jovanović, 2024). Adaptive policy frameworks should evolve based on empirical insights, promoting innovation while ensuring safety and resilience in the digital ecosystem. Incorporating these insights into the discourse on human-AI interaction within cybersecurity underscores the importance of a concerted approach across research, education, and policy-making. Such efforts are imperative to harness the full potential of human-AI synergy, setting a strategic course for future endeavours in enhancing the value of cybersecurity measures (Petrović and Jovanović, 2024).

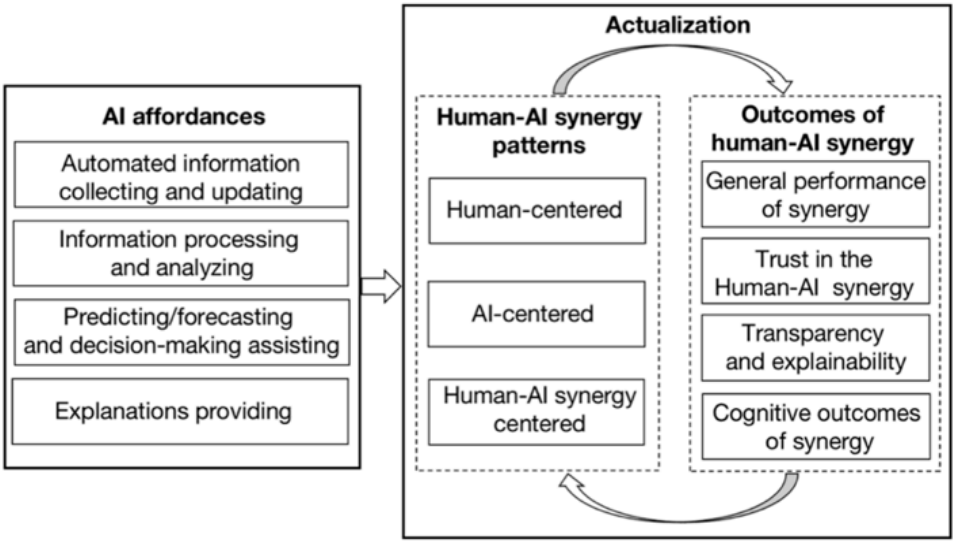


Figure 2.1: Synthesis of Research on Human–AI Synergy in Making Decisions (adapted from Lai et al., 2021)

In the realm of decision-making, especially within the context of AI and human synergy, three collaborative patterns emerge: AI-led tasks, human-led tasks, and those that involve equal participation from both parties. Recognizing these patterns can furnish valuable insights into harnessing the collective strengths of humans and AI for enhanced decision-making processes (Lai et al., 2021). Therefore as shown in figure 2.1 above, when analysing various decision-making tasks, it is imperative to consider these three perspectives; AI-centered, human-centered, and human–AI synergy-centered, to fully understand and optimise the potential of human-AI collaboration for achieving optimal decision-making outcomes (adapted from Lai et al., 2021).

Threat Trend	Description
Expanding Digital Footprint	Exponential growth in connected endpoints, systems, networks and critical infrastructure.
Accelerating Teachnology Adoption	New technologies – Cloud, Mobile and IoT introducing vulnerabilities.
State-Sponsored Campaigns	Geopolitics fueling nation-state cyber warfare capabilities.
Growth of Cybercrime	Transnational treat collectives pursuing ransomware, fraud and extortion.
Social Engineering Sophistication	Weaponisation of stolen data and deep fakes for personalised phishing and influence.
Personnel Shortage	**Global Deficit of 3.5 million cybersecurity professionals by 2025.**
Legacy Security Limitations	Perimeter defences struggle against zero – day threats. Compliance – driven approaches are reactive.

Table 2.1: Main Cyberthreat Trends Requiring Advanced Defences (Petrović and Jovanović, 2024)

As shown in table 2.1 above, addressing contemporary cyberthreats on a large scale requires an integrated approach that combines advanced technological capabilities with human expertise and interdisciplinary collaboration, all framed by proactive policy initiatives (Petrović and Jovanović, 2024). This comprehensive strategy emphasises the need for interdisciplinary approaches in cybersecurity research and development. Cybersecurity extends beyond the limitations of single disciplines, necessitating a holistic strategy that integrates computer science, engineering, social sciences, policy, law, and the humanities. Such collaborative efforts are crucial to effectively safeguarding digital infrastructures and

data. Central to this approach is the enhancement of ML technologies to improve their security and resilience, including the development of algorithms that are robust against various threats. As per Petrović and Jovanović (2024), advanced mathematical techniques also play a critical role in creating frameworks that protect privacy and ensure secure data processing. Additionally, the pursuit of technological innovation and the integration of human-centric design principles into security systems, which ensure that security measures are not only effective but also user-friendly, thus improving usability and encouraging wider adoption (Petrović and Jovanović, 2024).

2.1.2 Skills Gap

In an interview (2024) related to the AI and challenges in cybersecurity, Starnes who is Chief Security Strategist at (CapGemini, 2024) highlights the significant shortage of skilled professionals in the field, referencing a report that underscores a staggering 1.5 million unfilled cybersecurity positions globally. According to Ricci et al. (2024), research conducted by global organisations specialising in certifications and professional development for IT security and governance professionals for instance ISC2 and ISACA shows that roughly three million cybersecurity experts are missing worldwide. Cybersecurity education is a significant element in most strategies developed for tackling this workforce gap. This shows that this gap in cybersecurity expertise is not only a local but a global crisis, indicating a critical need for innovative solutions. Global cybersecurity CTO Delabarre, contributes to this conversation (CapGemini, 2024) by emphasising the increasing speed and sophistication of cyberattacks, which necessitate equally rapid and intelligent responses. Delabarre advocates for the integration of AI in cybersecurity practices, positing that AI can reduce the skills shortage by enabling smaller teams to efficiently manage and respond to threats. According to Delabarre (CapGemini, 2024), the advantage of AI lies not only in its ability to respond quickly, but also in its potential to do so with fewer human resources, thus addressing the dual challenges of escalating threats and a shrinking pool of skilled personnel. Both researchers agree on the potential of AI to transform cybersecurity practices by compensating for the human resource deficit and enhancing the speed and efficiency of responses to cyberthreats. This dialogue reinforces an agreement in the field that while AI cannot replace human expertise, it is an invaluable ally in the battle against cyberthreats, offering a sustainable solution to the pressing issue of workforce shortages (Capgemini, 2024).

The understanding that humans are fundamental to the delivery of effective cybersecurity is well-established, yet it is only within the last two decades that a significant body of social science research has begun to view cybersecurity through a socio-technical lens (Malatji et al., 2019). This perspective comprehensively explores how policy makers, security professionals, system designers, developers, and end users each play a role in shaping cybersecurity strategies (ENISA, 2018). This holistic view emphasises the interdependence of human actors and technical systems in creating secure digital environments.

Growing acknowledgment exists within the academic community regarding the limitations of purely technical cybersecurity measures. These measures must be integrated with human-centric strategies to be effective, reflecting an awareness that technical solutions alone

cannot fully address cybersecurity challenges (ENISA, 2018). This shift has led to an increased focus on the human elements of cybersecurity, aiming to create a resilient ecosystem where technological advancements and human insights are harmoniously integrated. Petrović and Jovanović (2024) emphasise the need for a multifaceted approach that combines ongoing research, development, and policy-making, tailored to the complexities of the digital age. By fostering this synergy, the goal is to cultivate a secure and resilient digital environment that leverages both human and technological resources effectively.

Moreover, considering the rapid evolution of AI technologies, Lai et al. (2021) recommend conducting periodic reassessment reviews. These reviews are crucial for ensuring that our understanding remains current and comprehensive, capturing the dynamic interplay between human expertise and AI capabilities in enhancing cybersecurity. In conclusion, integrating the socio-technical dimensions with technical cybersecurity measures is essential for developing robust security frameworks (ENISA, 2018). These efforts must continue to evolve, incorporating the latest research and technological advancements to address the increasingly complex landscape of cyberthreats effectively.

2.2 Artificial Intelligence Technologies in Cybersecurity

The increasing occurrence of significant cyber-attacks across the globe has underscored the critical need for organisations to prioritise the security of their data and information systems (Tao et al., 2021). Cybersecurity, a crucial aspect across various sectors, strives to safeguard information systems and secure personal and digital data from potential threats (Tao et al., 2021).

One of the main game changers in the area of cybersecurity is the development of tools and methods that are supplemented as a sub-group by AI and according to Azhar (2016), AI is no longer simply a trendy term; it is now being used widely across a wide range of sectors. Customer support, healthcare, and robotics are just a few of the many areas where AI has accelerated progress (Azhar, 2016). Additionally, it is making a major contribution to the continuing combat against cybercrime. Incorporating AI into cybersecurity provides innovative solutions across diverse domains. These cyber-attacks, often motivated by a variety of factors such as political competition, competitive advantages, international spying and predominantly target financial assets (Tao et al., 2021). Cybersecurity, essential for protecting digital infrastructure from internet-based attacks, is a key area where AI has shown significant promise. Stevens (2020), suggests that cyber attacks could evolve into prominent forms of terrorism, while Trappe and Straub (2021) emphasise the necessity of robust cybersecurity measures to safeguard organisations from potential threats, including competitive surveillance. The protection of confidential information is paramount, underscoring the importance of AI in developing advanced defences to ensure organisational and individual security (Ansari et al., 2022). As per Patel (2023), AI helps experts with crime analysis, research, and understanding, it has a favourable influence on cybersecurity. It strengthens the tools that businesses use to safeguard their networks, clients, and workers against dangerous online behaviour.

This literature review synthesises prior research exploring the integration of AI and cybersecurity, examining how AI technologies are utilised to strengthen defences against sophisticated cyberthreats. As per Ansari et al. (2022), AI, a crucial element in the modern technological progress, substantially enhances organisational efficiency and the quality of services provided. It is instrumental in the fight against cybercrime by rapidly identifying and mitigating security vulnerabilities, thereby strengthening data protection strategies. The advanced monitoring capabilities of AI play a vital role in maintaining system integrity, significantly improving encryption methods, and safeguarding sensitive information (Ansari et al., 2022).

Furthermore, according to Ansari et al. (2022) the pressing need to secure data has catalysed the expansion of the cybersecurity field, where AI has a great impact. This influence is particularly evident in the integration of ML technologies into recent cybersecurity advancements. Ansari et al. (2022) discusses the extensive effects of AI on cybersecurity, highlighting its role in enhancing existing security frameworks. The origins of AI date back to the 20th century, with the initial goal of developing systems capable of operating autonomously, without human intervention. This ambition has encouraged substantial research investments aimed at creating AI systems that mimic human behaviours and augment various industries.

According to (Patel, 2023) the widespread and essential use of internet services has increased exponentially from 2017 to 2023. This has directly resulted in an increase in cyber-attacks, with corresponding difficulties in effectively addressing them (Patel, 2023). For this reason, businesses and organisations, as part of a broader digital transformation, are utilising AI tools to provide an optimal solution in terms of cybersecurity (Patel, 2023). Cybersecurity in any environment aims to maintain the security of information systems and protect personal and digital data against any potential threats (adapted from Tao et al., 2021). The use of AI in cybersecurity offers solutions across various sectors that are discussed in this section, and shown in the figure below.'

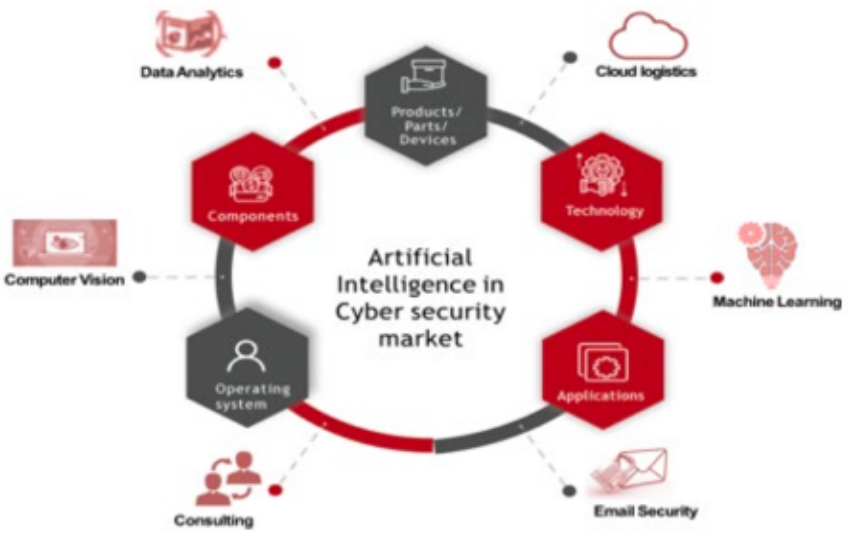


Figure 2.2: Applications of Artificial Intelligence in the Cybersecurity Industry (adapted from Tao et al., 2021)

Figure 2.2 displays various AI functions in cybersecurity. These applications include computer vision, consulting roles regarding the operating systems, application security, for instance email security, and areas involving ML and predictive analytics to form comprehensive solutions tailored to the specific needs of organisations or businesses. A significant and continuously expanding domain is pattern creation, which relies on gathering data from computing systems, network traffic, open data about known attacks within the global community, and other elements (Khraisat and Alazab, 2021). This data is then analysed, using data analytics to seize potential attacks (Ansari et al., 2022; Patel, 2023). Such measures are always based on the principle of security by design, as incorrect implementation and use of AI could unintentionally introduce vulnerabilities and new security issues, despite seemingly addressing the initial problem (Patel, 2023).

Various sectors, businesses and organisations with an interest in investing in AI-based cybersecurity technologies are numerous. Their common desire is to protect their data, whether financial, customer or production-related. As AI continues to evolve, it supports various sectors, enterprises and organisations in managing and deploying ML models. In the modern context, AI is crucial in addressing the escalating threats posed by cybercrime (Ansari et al., 2022). Moreover, AI's ability to process vast amounts of data for precise analysis and predictions has notably benefited sectors such as banking, telecommunications providers, healthcare, entertainment, online consumer goods retailers, banks, the retail sector, the automotive industry, and insurance companies all seek optimal cybersecurity solutions for their information systems, utilising either AI tools or integrated solutions.

2.2.1 Categories of Artificial Intelligence in Cybersecurity

The main categories of AI in cybersecurity include the following:

- Network Security
- Data Security
- Endpoint Security
- Identity and Access Security
- Application Security
- Cloud Security
- IoT Security

In the Capgemini Report (2019), 850 executives have been asked where they are using AI for cybersecurity in their organisations. Figure 2.4 shows that the main application was for network security, followed by data security and endpoint security.

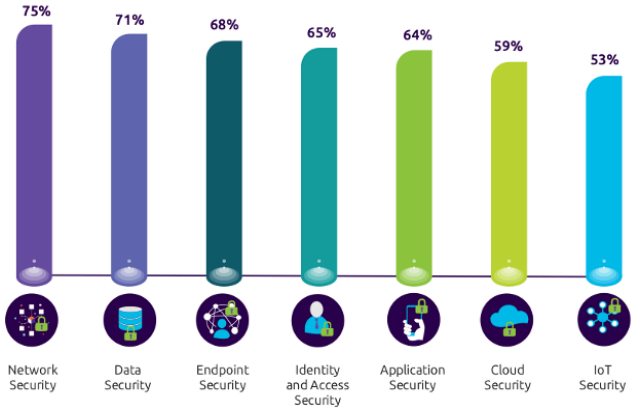


Figure 2.3: Network security has the highest deployment of AI in cybersecurity (adapted from Capgemini Research Institute, 2019)

Source: Capgemini Research Institute - AI in Cybersecurity executive survey, N = 850 executives

2.2.2 Machine Learning and Deep Learning Technologies in Cybersecurity

As per Ansari et al. (2022), in the field of cybersecurity, AI applications initially utilised signature-based techniques to identify patterns of attacks, significantly enhancing the rapid and effective detection of threats and malware.

However, in order for companies to manage the massive volumes of their data, and the complex cyberthreats, this traditional approach had to be replaced by AI. Organisations are increasingly turning to smart cybersecurity solutions to protect their digital spaces and assets from growing cyberthreats (Huyen and Bao, 2024). Cutting-edge technology, and behavioural analytics are used to detect and combat cyberthreats as they occur. Contrasting traditional methods, these intelligent solutions analyse and adapt to threats in real time, recognising unusual behaviours that may signal a threat (Huyen and Bao, 2024). They also consider various factors, such as how users behave and network traffic, to accurately assess and respond to threats. This forward-thinking strategy helps organisations seize attacks, minimising potential harm and disruption (Huyen and Bao, 2024).

Huyen and Bao (2024) emphasise how AI techniques are transforming cybersecurity, providing advanced tools to tackle the complex threats organisations face. The fast analysis of log files, network behaviour, infected programs, and the impact of attacks on IS has not only facilitated the precise prediction of potential threats and attacks but also their detection (Huyen and Bao, 2024). As per Huyen and Bao (2024), from these AI technologies, ML stands out, learning from data to identify anomalies, classify malware, and analyse user behaviour, enhancing the prediction and prevention of cyber incidents. In line with this is, Ansari et al. (2022) that ML technology plays a pivotal role in identifying and mitigating threats, enhancing data protection and highlighting AI's significant influence on cybersecurity. ML, a specialised subset of AI, excels in pattern recognition and data analysis; capabilities essential for automating repetitive tasks in cybersecurity (Shaukat et al., 2020). Prasad et al. (2020) noted that AI techniques, underpinned by ML algorithms, could instantly notify authorities of security breaches, thereby reducing response times dramatically.

Huyen and Bao (2024) also mention in their study DL, a more intricate form of ML, exploring deeper into data to detect threats in various formats. Further emphasising the evolution of AI in cybersecurity, Kioskli et al. (2023) explored the impact of DL. DL involves training multi-layered artificial neural networks to recognise intricate patterns in vast datasets. In cybersecurity, these algorithms are crucial for identifying and classifying advanced threats that avoid traditional, signature-based detection methods. DL not only aids in sophisticated threat detection by analysing substantial volumes of network traffic and security logs but also enhances authentication and access control systems (Kioskli et al., 2023). By analysing user behaviour to detect anomalies, DL algorithms help prevent unauthorised access and secure sensitive data against insider threats (Kioskli et al., 2023). Overall, the integration of DL in cybersecurity presents significant advancements in combating evolving cyberthreats. As these threats grow more complex, DL is prepared to become increasingly crucial in enabling organisations to promptly and effectively respond to potential security breaches (Kioskli et al., 2023).

Truong et al., (2020) in their paper explain that in order for AI to produce a new type of intelligent machine that responds like human intelligence, machines need to learn. They then introduced ML, a branch of AI that aims to empower systems by utilising data to learn and improve without being explicitly programmed. ML has strong ties to mathematical techniques that enable a process of extracting information, discovering patterns, and drawing conclusions from data. As shown in table 2.2 below, there are different types of the ML algorithms generally classified into three main categories; supervised learning, unsupervised learning, and reinforcement learning. In supervised learning a training process with a large and representative set of data has been previously labelled. In contrast to supervised learning, unsupervised learning algorithms use unlabeled training datasets. These approaches are often used to cluster data, reduce dimensionality, or estimate density. Reinforcement learning is a type of learning algorithm that learns the best actions based on rewards or punishment. Reinforcement learning is useful for situations where data is limited or not given (Truong et al., 2020). Additionally, reinforcement learning helps develop dynamic defence strategies, adapting to new threats to support cybersecurity measures *(*Huyen and Bao, 2024). In this section, an overview of the learning algorithms is given, a crucial concept of AI (Truong et al., 2020). Regarding cybersecurity, the standard ML algorithms are DT, SVM, Bayesian algorithms, KNN, RF, AR algorithms, EL, k-means clustering, and PCA (Truong et al., 2020).

Algorithm Type	Algorithms	Cybersecurity Applications
Supervised Learning	Decision Trees, Logistic Regression, Support Vector Machines	Malware Classification, Network Intrusion Detection
Unsupervised Learning	K-means Clustering, Isolation Forests, Autoencoders	Anomaly Detection, User Behaviour Profiling
Reinforcement Learning	Q-learning, Deep Q networks	Adaptive Network Security, Automated Red Teaming

Table 2.2: Common ML Algorithms Applied in Cybersecurity (Huyen and Bao, 2024)

Concerning DL, it uses data to train computers to perform actions and thoughts only humans are capable of at that time (Truong et al., 2020). Its motivation lies in the working mechanisms of the human brain and neurons for processing signals. The core of DL is constructed on more extensive neural networks, training them with as much data as possible and the performance increases. The most important advantage of DL over ML is its superior performance in large datasets. Similarly to ML methods, DL methods also have supervised learning, unsupervised learning, and reinforcement learning. Truong et al. (2020) mentions the typical DL algorithms frequently utilised in the cybersecurity domain which are FNN, CNNs, RNN, DBNs, SAE, GANs, RBMs, and EDLNs (Truong et al., 2020).

Despite the fact that AI-powered solutions can strengthen cyber defences and safeguard critical assets in our increasingly digital world (Nadella et al., 2024), AI's role in cybersecurity is dual-faceted. While AI and ML significantly shorten the duration needed for threat detection and response, these technologies also equip cybercriminals with tools to enhance the efficiency and success rate of their attacks, thus complicating the threat landscape for organisations (Prasad et al., 2020). The implementation of AI in cybersecurity raises substantial concerns over data privacy, scalability, and human-machine interaction (Nadella et al., 2024).

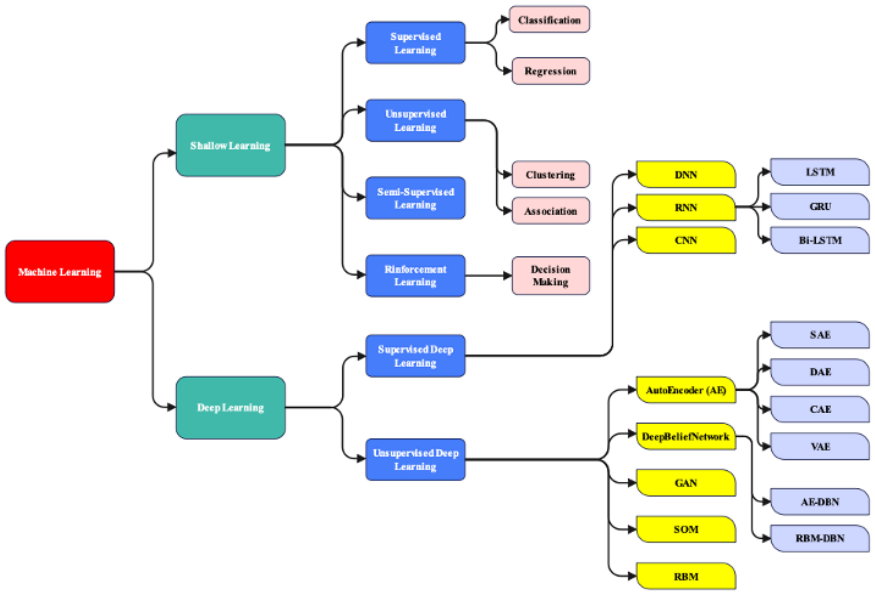


Figure 2.4: ML - Based Approaches for Cybersecurity (adapted from Djenna et al., 2023).

2.2.3 Artificial Intelligence System Lifecycle and Cybersecurity

This chapter briefly explores a structured approach to AI by breaking down the AI system lifecycle, which is crucial for identifying potential threats. It covers various stages, including design, development, deployment, and maintenance, highlighting the importance of data protection throughout. ML models are emphasised as key to transforming input data into valuable outcomes, serving as the core focus due to their significant role in current AI applications. The chapter also introduces a generic reference model to provide a common understanding of an AI system's components and their interrelations, helping in the systematic identification and management of security threats.

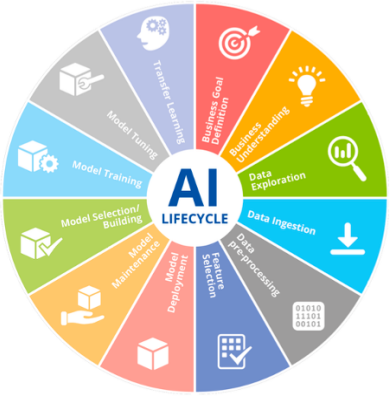


Figure 2.5: Stages of AI Lifecycle (adapted from Malatras and Dede, 2020)

Just as with any IS, software, or operating system, there is a specific development pathway. The same applies to an AI system. During the design phase, it's essential to define the data, requirements, implementation goals, and the approach, all while prioritising security from the outset. The components of an AI system are closely interlinked, aiming for development, evolution, and operation over time, starting from finite computational resources. ENISA has outlined a general representation of the AI system lifecycle, including the essential components or "assets" involved (Malatras and Dede, 2020).

In the field of AI, data is one of the most essential assets, undergoing continuous transformation throughout the AI Lifecycle (Malatras and Dede, 2020). Data evolves across various stages of this lifecycle, including Data Ingestion, Data Exploration, Data Pre-processing, Feature Importance, Training, Testing, and Evaluation. This transformation process within the AI Life Cycle includes a range of other assets, for instance the actors involved, computational resources, and software, among others. Additionally, intangible elements like organisational processes, cultural aspects, and the knowledge and experiences of actors play a crucial role, potentially introducing unintended risks (Malatras and Dede, 2020).

Figure 2.6: Data Transformation Along AI Lifecycle Development Stages (adapted from Malatras and Dede, 2020).

Defining the objectives and goals is considered the most significant event for an AI system, essentially the mission that the AI system's model is tasked with. Following this, as shown in figure 2.8 above, the most critical and substantial issue is the data, which will be sought, found, utilised, and processed by the system's model. The data factor is significant, both during the design phase and in the model development process of the AI system, as it

significantly impacts the system's security, making it crucial for development. (Malatras and Dede, 2020). In line with this is Pupillo et al. (2021) that emphasise that during the design phase of an AI system, it is essential to clearly define the problem and establish the model on which the solution will be based, utilising and analysing the relevant data. According to (Malatras and Dede, 2020) an AI system is an evolving entity, continuously fed and refined with data, fulfilling a higher purpose to successfully complete a specific process for secure inference extraction. In cases of failure, the system itself should be designed to allow self-improvement through algorithmic decision-making and ML. In an AI system, there are certain essential components and assets that are vital for its operation as seen in the figure below (Malatras and Dede, 2020).

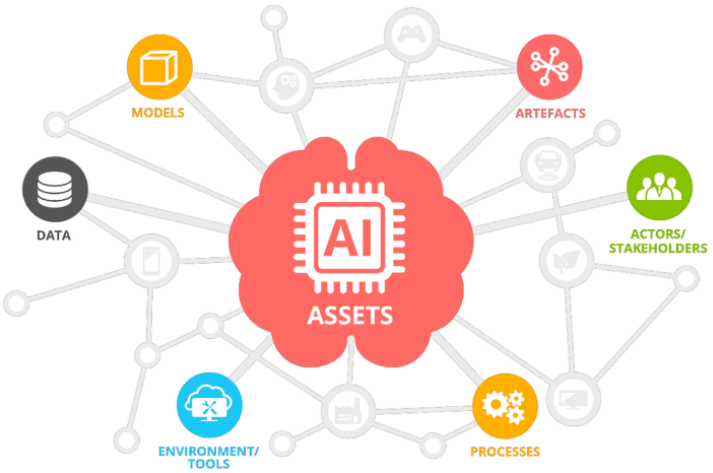


Figure 2.7: AI Assets Categories (adapted from Malatras and Dede, 2020)

In analysing the cybersecurity landscape, a fundamental element is the identification of asset categories vulnerable to threats. Malatras and Dede (2020) define assets as anything valuable to an individual, business, or organisation that requires safeguarding. In the context of AI, assets include essential components necessary for fulfilling their intended purposes. Beyond standard ICT assets such as data, software, hardware, and communication networks, AI introduces specialised assets like models, processors, and other elements. These assets are susceptible to compromise and damage from both intentional and unintentional actions (Malatras and Dede, 2020). For each stage of the AI lifecycle, Malatras and Dede (2020) identified the most crucial assets by considering the functional roles of specific stages. This approach not only captures components fundamental to AI but also includes assets that facilitate the development and deployment of AI systems. Additionally, because of their integrative role, processes related to AI are also recognized as key assets (Malatras and Dede, 2020). Assets are classified in six categories; Data, Model, Actors, Processes, Environment/Tools and Artefacts (Malatras and Dede, 2020).

Finally, it's important to acknowledge that the broad range of the AI ecosystem, combined with the dynamic progression of AI systems and methodologies, make asset mapping a

continuous effort that will require considerable time to evolve fully. This ongoing task is complicated by the multi-layered nature of AI systems, which involves a great array of techniques, deployment scenarios in various applications, and related domains like facial recognition and robotics. Furthermore, the AI/ML supply chain presents its own set of challenges due to its complexity and breadth, which significantly influences the asset and threat landscape. Addressing these challenges will be a key focus in the forthcoming evaluations of AI-related cybersecurity threats. This highlights how critical are the initial stages of developing an AI system, reflecting the technology's ongoing advancement and the iterative process of defining and understanding its key components (Malatras and Dede, 2020).

2.2.4 Types of Cyberthreats

Today's cyberworld consists of a sophisticated network of specialised tools and technologies, which may be kept on-site within an organisation, in the cloud, or a combination of both. As businesses and organisations navigate this complex environment, they must prioritise the protection of their information and the privacy of their operations (Aldawood and Skinner, 2020). The increasing occurrence and complexity of cyber-crimes today pose significant challenges to securing information systems, which are more vulnerable to attacks than ever before (Aldawood and Skinner, 2020).

As per Hawamleh (2023) a cyber-attack is described as a deliberate attempt by a group or an individual to breach the system's data and information for economic purposes or other purposes that are described below or steal data from the targeted systems. According to Basholli et al., (2024), recently, cyber-attacks are modified, analysed and well prepared to penetrate into the organisation's system they are targeting. Basholli et al., (2024) also emphasises that the best protection against cyber attacks is achieved when there is knowledge and a deep understanding of how these cyberattacks work. In line with this is Kalhoro et al. (2021) who emphasise that while cyber security is the measurement of behaviours and actions taken to maintain security and strengthen defences against cyber-attacks, cyber hygiene relates to internet security knowledge and practices related to further enhancing security.

Advancements in ICT have made countries more dependent on network infrastructures, while the rapid growth of smart technology introduces significant cybersecurity risks and challenges (Luknar & Jovanović, 2024; Nadella et al., 2024). In their paper, Nadella et al. (2024) it is also emphasised that with the digitization of various businesses, organisations and sectors, cyberthreats such as ransomware, phishing, malware, and DoS attacks are escalating into significant dangers. This section explores and defines various threats, many of which are relevant today and expected to remain significant over the next few years. According to Lella et al. (2022), their characteristics will change due to increased advancements in new technologies. In the field of cybersecurity, delaying preventive and mitigative actions is not advisable; it's crucial to stay alert to emerging threats. At the same time, these efforts should complement ongoing, essential cybersecurity practices like education, awareness, and regular updates (Lella et al., 2022).

According to (Luknar and Jovanović, 2024) it is crucial for governments to implement preventative measures against various cyberthreats nowadays. Effective cyber defence should encompass all technological components of critical infrastructures, ensuring a high level of readiness against cyber vulnerabilities. While less economically developed countries may struggle with the costs of high-tech solutions, they should still explore all possible measures to protect these critical systems (Luknar and Jovanović, 2024).

This section provides a brief description of the primary threats identified and reported at the annual report by the European Union Agency for Cybersecurity (ENISA Threat Landscape, 2022) with some visuals in figures 2.10 and 2.11 to display the numerical distribution.

Malicious Software, Malware: Also referred to as malicious code and malicious logic**,** is a general term used to describe any software or firmware intended to perform a negative impact on the confidentiality, integrity, and availability of a system. Some examples of malicious software include viruses, worms, trojan horses, spywares, adwares, or any other entity that relies on code aimed at harming the operation of a computer system or its data (Lella et al., 2022). Malware attacks have shown a concerning level of advancement and diversification in recent decades, especially in the last ten years (Xu et al., 2020, Falowo et al., 2024). These malicious software attacks have caused extensive damage and implications, leading to loss of sensitive data, financial losses, and loss of consumer trust on many occasions (Xu et al., 2020, Falowo et al., 2024).

Ransomware Attacks: This is one of the prime threats and is one of the fastest growing cyber-attacks according to Basholli et al. (2024). As stated by Lella et al. (2022) and the report by ENISA (Threat Landscape for Ransomware Attacks), ransomware is defined as a type of attack where cybercriminals take control of a target's assets and demand a ransom, in exchange for the return of the asset's availability. Basholli et al., (2024), mentioned a particular cyber attack, the WannaCry, which encrypts your data on the personal computer and then asks for an amount of money to decrypt your data by sending you a Key. This virus began its operation on May 12, 2017, where within 48 hours it reached about 230,000 victims from 150 different countries of the world.

Distributed Denial of Service attacks (DDoS): DDoS attacks, characterised by their ability to massively disrupt services by overwhelming systems with a flood of internet traffic, have become a dangerous tool of choice for cybercriminals (Lysenko et al., 2020). These attacks not only cause immediate operational disruptions to private and public enterprises but also serve as a smokescreen for more harmful activities, such as data security breaches (Lysenko et al., 2020). The public nature of the Internet makes it particularly vulnerable to DoS attacks that go so far as to question the validity of a server (Singh et al.,2024, Basholli et al., (2024)). As emphasised by Lella et al. (2022) however, it is highlighted that these attacks are getting larger and more complex and also moving towards mobile networks and IoT and are being used in the context of cyberwarfare. During the reporting period (ENISA Threat Landscape, 2022), DDoS and ransomware rank the highest among the prime threats (Lella et al., 2022).

Figure 2.8 (left): Prime Cybersecurity Threats 2022 by ENISA (Lella et al., 2022)

Figure 2.9 (right): Prime Cybersecurity Threats for 2030 by ENISA (ENISA, 2030)

Adapted from "ENISA's Foresight Analysis: top cybersecurity threats likely to emerge by 2030". Retrieved from https://ec.europa.eu/newsroom/ECCC/items/766303/en

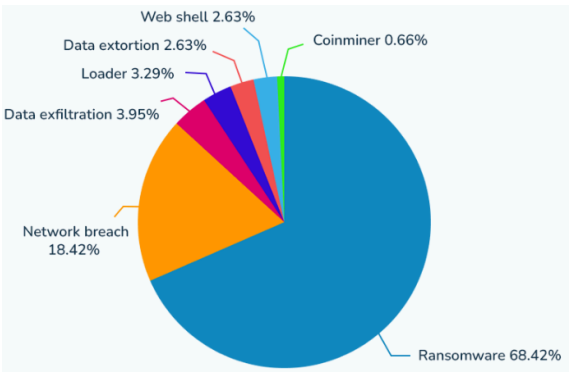
Social Engineering: Social engineering is defined by (Aldawood and Skinner, 2020) as manipulating and encouraging people to reveal sensitive information through online networks or by granting access to restricted areas or systems. In addition, as mentioned by Aldawood and Skinner (2020), generally, cyber-attacks may target the technical part of a system, but socially engineered attacks are designed to target the human element and rely on personnel vulnerabilities. In particular, socially engineered threats psychologically manipulate humans to perform a specific action that can potentially lead to leakage of confidential and classified information that can be used to damage an organisation's resources or harm its reputation. In line with this is (Lella et al., 2022), who emphasise in their report that, in cybersecurity, social engineering baits users into opening documents, files or emails, visiting websites or granting unauthorised persons access to systems or services. The most widespread methods used in this category include, for example, phishing, spear- phishing, whaling, smishing, vishing, BEC, fraud, impersonation and counterfeit, which are analysed in the relevant chapter (Lella et al., 2022).

Threats Against Data: Data threats cover a range of attacks targeting data sources to gain unauthorised access and exposure, or to manipulate data, impacting system behaviour. Lella et al. (2022) discuss in their report that these threats structure the foundation for many related threats such as ransomware, RDoS and DDoS, which specifically aim to block access to data and often demand payment to restore it. Lella et al. (2022) also categorises the threats against data as data breaches and data leaks. A data breach is a purposeful attack by cybercriminals to access and release sensitive, confidential, or protected data without authorization. Instead, a data leak occurs when such data is unintentionally released, often due to configuration errors, vulnerabilities, or human errors (Lella et al., 2022).

Threats Against Availability - Internet Threats: For many people, access to the internet has become a basic necessity to work, study, and to interact socially. However, the essential and daily use of the internet by a large number of members of our society makes them a target for attackers. Internet threats that impact availability include, for example, BGP hijacking (Lella et al., 2022).

Disinformation - Misinformation: This threat refers to false and problematic information deliberately employed to mislead and manipulate, resulting in public harm for financial or ideological advantages (Lim et al, 2024)**.** According to (Lella et al., 2022), the rise of disinformation and misinformation campaigns continues as, nowadays, digital platforms, including social sites, news outlets, and even search engines, have become primary sources of information for many people. These platforms often prioritise content that attracts more viewers to generate traffic, sometimes promoting information without proper validation. The definition of misinformation and disinformation is essential, distinguishing between unintentionally incorrect information and deliberately falsified content (Lella et al., 2022).

Supply Chain Attacks: Supply chain attacks are well-known cyberthreats (Haider et al. 2024), targeting both the supplier and the customer (Lella et al., 2022). SolarWinds was one of the first expose of this kind of attack and showed the potential impact of supply chain attacks (Lella et al., 2022). Cybercriminals penetrated SolarWinds' software by embedding malicious code into the software updates. This sophisticated operation resulted in significant financial losses and affected numerous organisations (Haider et al. 2024).



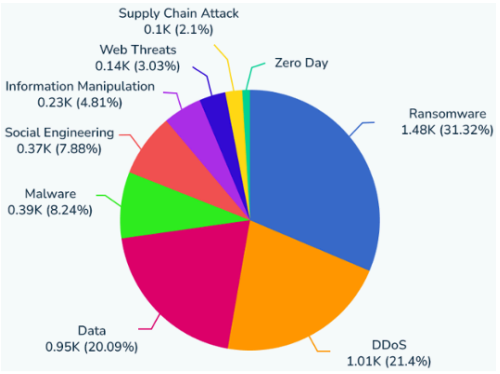


Figure 2.10 (left): Distribution of Detected Cyber Attacks Worldwide in 2022, by type (StationX, 2024).

Figure 2.11 (right): Breakdown of Analysed Incidents by Threat Type in Europe from June 2022 to June 2023 (StationX, 2024).

2.3 Artificial Intelligence Integration into Cybersecurity Frameworks

In the digital age cybersecurity is a critical concern, and various frameworks have been developed to guide organisations in protecting their information systems. According to ENISA (2021), there is a general agreement that the adoption of AI will lead to substantial economic gains, even though calculating these gains exactly is a difficult task. The integration of AI into cybersecurity frameworks is a critical step in addressing increasingly sophisticated cyberthreats. Several papers discuss how AI technologies, including ML and DL, offer promising solutions to enhance the detection and mitigation of cyberattacks as they offer improved detection and prevention of cyberthreats (Gulati et al., 2023, Lourens et al., 2022, Zeadally et al., 2020). Some notable cybersecurity frameworks that exist are described according to the literature in this next section.

The ISO/IEC 27000 series framework offers a comprehensive set of standards for the security of information management systems, providing guidelines for organisations to build, implement, maintain, and continually improve their cybersecurity measures (Proença and Borbinha, 2018). Within this framework, specific standards such as ISO/IEC 27001 and ISO/IEC 27002 outline requirements and best practices for the implementation of security controls and risk management processes (Proença and Borbinha, 2018). ISO/IEC 27001 does not specifically address AI technologies, but within their IS structures, organisations can leverage AI to enhance security capabilities for threat and anomaly detection, pattern recognition, and automated incident response, all of which contribute to a more robust cybersecurity resilience.

ISO and IEC are globally recognized bodies that develop and publish international standards for a wide range of industries, including IT and cybersecurity. These standards aim to ensure quality, safety, and efficiency, helping organisations worldwide to improve their operations and meet regulatory requirements.

The document ISO/IEC AWI 27090 is currently in its preliminary stages and is being drafted as an Advanced Work Item (AWI). Authored by Soler Garrido et al. in 2023, this standard is focused on "Cybersecurity – Artificial Intelligence." It specifically aims to provide guidelines on how AI can be utilised within cybersecurity to help institutions bolster their defenses against cyberthreats. Another related document, ISO/IEC CD TR 27563, is in the committee draft stage, indicating it is a draft technical report still under review by an ISO/IEC technical committee. This report is designed to assist healthcare institutions in effectively leveraging AI to enhance patient care, diagnosis, treatment, and overall healthcare outcomes. It also emphasises the importance of aligning with established standards and guidelines to ensure safe and effective implementations, as noted by Schmittner and Shaaban in 2023.

These standards are crucial as they provide authoritative guidance and best practices, helping organisations integrate advanced technologies like AI into their critical operations safely and effectively.

The NIST RMF provides a methodical and systematic approach that brings together information security and risk management operations within the system development life cycle (McCarthy and Harnett, 2014). These are explained in the steps below:

1. Classify the information system and the data processed, stored, and transmitted by it, according to an impact analysis.

2. Choose an initial set of baseline security measures for the information system based on its security classification, customising and adding to these measures as necessary following an organisational risk assessment and local circumstances.

3. Deploy the security measures and delineate their application within the information system and its operational environment.

4. Evaluate the security measures using suitable assessment methods to ascertain their correct implementation, intended functionality, and efficacy in meeting the system's security prerequisites.

5. Authorise the operation of the information system after evaluating the risks posed to organisational functions, assets, individuals, external entities, and the nation, concluding that such risks are acceptable.

6. Continuously monitor the security measures within the information system, including assessing their effectiveness, documenting any system or operational environment modifications, conducting security impact assessments for these changes, and reporting the system's security status to designated organisational authorities.

In the field of automated vehicles, there is a need for increased security due to the interconnectedness of the technologies that are used. For example, the Jeep 2015 model had an entertainment system that used cellular networks and compromised an estimated 1.4 million cars to remote cyber-attacks which controlled various parts of the vehicles. Certain testing certifications and compliance processes have been adopted to ensure that there is safety even in the era of AI, some of which are outlined in the JRC Science for Policy Report (Baldini, 2020). Kaloudi and Li (2020) indicate that AI-based cyber assaults have the potential to inflict considerable harm, and understanding how they are classified and identified can help develop defences against them.

2.4 The Role of AI in Cybersecurity Landscape

The introduction of AI presents a unique plethora of challenges towards information security at a global scale due to the broad impact of the technology (UNIDIR, 2023). An article published by ISACA on the Seven Trends to Track for Cybersecurity in 2024 stated the main trend to be the Rise of AI in Cybersecurity (ISACA, 2024). In line with this is the NSCAI Final Report (2021) acknowledges that "*AI technologies will be a source of enormous power for the companies and countries that harness them*" (p7). In light of that, this section seeks to discuss the various and broader AI strategy or policies, if relevant, to understand the larger context of AI on cybersecurity.

Due to the interconnected nature of the modern digital landscape, much benefit can be derived from collaborative efforts for cyber defence (Vadiyala, 2019). Many nations have acknowledged the need for new cybersecurity guidelines to safeguard the integrity of the democratic voting process (Segal et. al., 2020). Vadiyala (2019) states that "*next-generation cybersecurity frameworks rely on threat intelligence, which collects, analyses, and shares cyberthreat and vulnerability data*" (p.9) and they often operate in real-time to monitor and detect cyberthreats.

As a world-leading digital economy, China is one of the most active states in Asia Pacific, invested in gaining influence in leveraging cybersecurity to promote its economic and political pursuits (Zeng, 2022). China considers its cybersecurity as utmost critical to its sovereignty (Austin, 2018). Another Asian state of note is North Korea, whose cyber infrastructure was established in the 1990s, and cyber crimes had become sophisticated enough to attack the Bangladesh Central Bank to steal up to USD 81 million through Society for Worldwide Interbank Financial Telecommunication (SWIFT) by the 2010s (Segal et al., 2020).

In the United States of America, the NIST reports that AI risk management needs to be "*incorporated into broader enterprise risk management strategies and processes*" (p.8), as addressing these along with cybersecurity contributes to more efficient organisational outcomes (US Department of Commerce, 2023). With the aim of exchanging threat information, joining forces on responding to incidents, and working together to fight against cyberthreats, there is value in combined efforts for cyber defence to incorporate collaborations between government institutes, organisations, and other stakeholders (Vadiyala, 2019). The USA government supports the view and presents various possibilities under which the EU should work closely with the USA to address challenges in transatlantic cooperation on AI (Schmidt et al., 2021). According to Schmidt et al. (2021), if ongoing trends persist, China has the capability, expertise, and aspirations to outpace the USA and emerge as the global leader in AI within the coming decade. Concurrently, the spread of AI intensifies the risks associated with cyber attacks and dissemination of false information, tactics employed by countries like Russia and China to infiltrate societies, pilfer and undermine processes.

Kabanda (2021) highlighted that in Sub-Saharan Africa, there is a need to establish "an innovation-led knowledge economy" in order to counter the challenges faced around economic sustainability. The creation of regulatory frameworks in cybersecurity that address AI technologies can aid in managing different corruption issues that often harm the growth of political stability (Couchoro et al., 2021). It goes without saying then that a necessary policy implication in achieving effective control over ML in Sub-Saharan Africa demands investment in AI systems to enhance control measures (Kabanda, 2021). In the current digital era, Kabanda (2021), highlights that strengthening cybersecurity is indispensable for combating threats connected to ML. In terms of developing an AI policy or framework, efforts are isolated at the moment as different countries are working individually towards their own frameworks, instead of pulling resources together to find collective framework solutions (Creemers, 2022).

In the EU, AI technologies have been acknowledged to have the potential to improve many economic sectors, including health, finance, transport and agriculture amongst others.

Through the legislative framework of the AIA, guidelines have been proposed to govern various aspects of AI including data governance, accountability and risk assessment (European Parliament, 2024). A recent survey conducted by ENISA (2022) to assess the measure of preparedness of national competent authorities to adopt cybersecurity AI requirements is currently low and more needs to be done to persuade them. The AIA, NIS and NIS 2 demands that AI suppliers be mandated to report to the national competent authorities whenever significant incidents occur, making it easier to address and regulate (ENISA, 2022).

According to Jada and Mayayise (2023), AI's most significant influence lies in the realm of vulnerability management, especially in intrusion detection. It also plays a crucial role in bolstering the security of organisational networks and systems against cyberthreats. The positive effects of AI on cybersecurity encompass various facets, including predicting cyber incidents and aiding in data recovery, ultimately contributing to an organisation's competitive edge. It is helpful then, to categorise the risks that AI potentially holds from a holistic perspective in order to better understand how to mitigate them. Figure 2.1 below shows this:

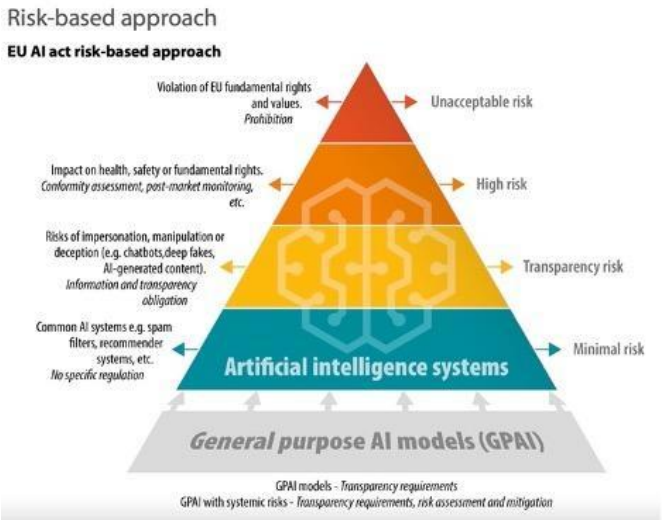


Figure 2.12: EU AIA Risk- Based Approach, source: European Commission

Unacceptable Risk: AI systems engaging in subliminal, manipulative or deceptive tactics to alter behaviour and undermine informed decision-making, as well as exploiting vulnerabilities related to age, disability, or socio-economic status, can cause significant harm. Additionally, biometric categorisation systems inferring sensitive attributes or evaluating individuals based on personal characteristics may lead to unjust treatment, especially in contexts such as law enforcement or workplace surveillance.

High Risk: The AIA defines high risk AI systems by how they might affect health, safety, or basic rights, depending on their intended use and their function. It stresses creating an EU database and a "filter provision" exempting AI from high-risk status if they're not risky or don't profile people.

Transparency Risk: AI systems, including chatbots and content generators, pose transparency risks necessitating disclosure to users and robust detection methods like watermarks, especially in workplace contexts.

Minimal Risk: Systems with minimal risk to individuals, such as spam filters, will not incur additional obligations beyond existing legislation, such as the GDPR which is explained further in the next paragraph.

GDPR introduced strict rules on the handling of personal data, stipulating that organisations ensure that their AI algorithms comply with GDPR requirements when processing personal data to detect and respond to security threats (European Parliament, 2016). In conclusion, the National Security Commission on Artificial Intelligence, as well as experts within the European Union acknowledge that so much more still remains to be unearthed about AI and its future applications.

2.5 Summary of Literature Review

The literature review chapter aims to provide a comprehensive overview of existing research and insights into the cybersecurity landscape. By examining a variety of studies, articles, and reports, this chapter seeks to establish a foundational understanding of the key concepts, challenges, and opportunities associated with the role of AI in the cyber security landscape and its integration into cybersecurity frameworks. Through this exploration, the review highlights the evolving dynamics between technological advancements and human input, setting the stage for further analysis of their combined impact on cybersecurity effectiveness.

Themes	Sub-Themes	References
Human-AI Synergy in Cybersecurity	• Collaboration between Humans and AI • Skills Gap	Patel (2023), Sinclair (2023), Nielsen, P., 2023, Petrović and Jovanović (2024), Bao et al. 2023, Lai et al. (2021), Järvelä et al. (2023), Lawrence (2023), Cheng et al. (2019), Stevens (2020), Trappe and Straub (2021), Kioskli et al. (2023), (Prasad et al., 2020), CapGemini (2024), Ricci et al. (2024), Malatji et al. (2019), ENISA (2018).
AI-Technologies in Cybersecurity	• Categories of AI in Cybersecurity • ML & DL Technologies in Cybersecurity • AI System Lifecycle and Cybersecurity • Types of Cyber Threats	Tao et al. (2021), Azhar (2016), Stevens (2020), Trappe and Straub (2021), Ansari et al. (2022), Patel (2023), Khraisat and Alazab (2021), Capgemini Report (2019), Huyen and Bao (2024), Shaukat et al. (2020), Prasad et al. (2020), Kioskli et al. (2023), Truong et al. (2020), Nadella and Gonaygunta (2024), Malatras and Dede (2020), Pupillo et al. (2021), Aldawood and Skinner (2020), Hawamleh (2023), Basholli et al. (2024), Kalhoro et al. (2021), Luknar and Jovanović (2024), Lella et al. (2022), ENISA Threat Landscape (2022), Xu et al. (2020), Falowo et al. (2024), Lysenko et al. (2020), Singh et al. (2024), Lim et al. (2024), Haider et al. (2024).
AI integration into Cybersecurity Frameworks		ENISA (2021), Gulati et al. (2023), Lourens et al. (2022), Zeadally et al. (2020), Proença and Borbinha (2018), Soler Garrido et al. (2023), Schmittner and Shaaban (2023), McCarthy and Harnett (2014), Baldini (2020), Kaloudi and Li (2020).
The Role of AI in Cybersecurity Landscape		UNIDIR (2023), Rende (2023), NSCIA Final Report (2021), Vadiyala (2019), Segal et. al (2020), Vadiyala (2019), Zeng (2022), Austin (2018), Segal et al. (2020), US Department of Commerce (2023), NSCIA (2021), Kabanda (2021), Couchoro et al. (2021), Creemers (2022), European Parliament (2024), ENISA (2022), Jada and Mayayise (2023).

Table 2.3: Overview of Theoretical Background

3 Methodology

This chapter outlines the research philosophy in our study, including the design of our research, the research philosophy that supports it, and the scientific approach we have taken. The research philosophy will be presented along with literature collection methods, data collection methods, data analysis methods, ethical considerations and scientific quality.

3.1 Research Philosophy

This thesis employs a qualitative empirical research methodology using semi-structured interviews to engage with organisations and experts in the governance and practice fields of AI and cybersecurity. Given the focus on the cyberthreat environment in the EU and the intersection of AI and cybersecurity, a pragmatic approach that primarily utilises interpretivist methods has been adopted. Interpretivism aligns well with the qualitative nature of our study, offering the most suitable framework to gain deep insights into this complex context (Alharahsheh and Pius, 2020).

Interpretivism allows us to explore the subjective nuances inherent in the integration of AI and cybersecurity, emphasising the significance of human perspectives, beliefs, and values in shaping policies and practices. This approach facilitates a deep understanding of the contextual complexities of decision-making processes and societal attitudes toward these technologies. By adopting the interpretive paradigm, our research achieves high validity, as it relies on personal contributions while considering various variables (Myers, 2008). The overarching goal is to consider the subjective realities and interpretations that influence the convergence of cybersecurity and AI within the dynamic European landscape. Alharahsheh and Pius (2020) support this approach, noting that interpretivism assumes reality is subjective and varies between individuals.

3.2 Research Approach

In the field of information systems, where studying technically implemented social systems is the focus, having a variety of perceptions is essential (Ågerfalk, 2013). While we recognise the value of quantitative data in providing objective and measurable insights into cybersecurity threats and AI efficiency, we also believe in the importance of understanding the subjective human experiences and perceptions of individuals and organisations affected by these technologies. The thematic exploration of perceptions and experiences allows for a comprehensive understanding. Qualitative research focuses on quality attributes, related to events or phenomena under investigation, without emphasis on quantitative attributes (Mbanaso et al., 2023).

From an ontological perspective, we will adopt a moderate form of realism in our research design. We acknowledge that while there are objective truths in cybersecurity and AI,

specifically related to data violations, risk patterns, and AI algorithms, these truths are often observed and interpreted through subjective human experiences. This recognition of objective realities, mitigated by subjective interpretations, is essential in understanding the complex dynamics of cybersecurity threats and AI applications.

3.3 Literature Collection Methods

The aim of this section is to explain how the literature review in Chapter 2 was gathered and identified to support the relevant foundational concepts of this research. The literature was collected by a systematic process that was followed, involving the searching of academic databases on Lund University's (LUBSearch) as well as Google Scholar. These databases enabled access to vital literature, including academic journals, e-books, scholarly articles, and conference papers. The study also recognizes the use of non-peer-reviewed sources, like white papers, in specific cases to provide figures as well as to clarify and define certain terms. Some parts of the literature that required legal documents, and the sources used were direct official websites (e.g. ENISA, NIST etc.) and Overton, (which is provided by Lund University Lubsearch, a collection of policy documents, parliamentary transcripts, government guidance and think tank research).

Boolean operators were used in some of the searches to ensure that a wider range of relevant literature was yielded. According to Colaric (2003), part of the success of a search is assured when the concept of Boolean operators is understood. Using OR retrieved more general results that AND, and so the latter was selected instead, the use of "*" ensured that similar results came about in the search AND placing keywords in inverted commas " " also gave more specific results.

The keywords specified below were used along with Boolean operators in the search:

- Cybersecurity
- Human AI synergy
- Cyberthreats
- AI Technologies,
- Cyberthreat* in EU
- Skills Gap in cybersecurity
- AI AND Cybersecurity frameworks
- Cybersecurity frameworks AND Asia
- Cybersecurity frameworks AND Africa
- Cybersecurity frameworks AND the "European Union"

Once results were yielded, the researchers chose to focus on results from the past ten years, due to the rapidly evolving nature of the research scope and to ensure there was more reliable and current data. Each selected piece of literature was read from the title to the subheadings and then the content was schemed through to ascertain its relevance. For academic documents, reading through the discussion and conclusions of each article was also useful. Once an article was found to be useful, the researchers took note of other relevant literature in the reference list, (some of which were relevant to the research) and used them as well.

Due to the interdisciplinary nature of the topic being researched, the sources came from other subject-specific journals from similar disciplines However, care was applied to ensure that the majority of the literature was from the IS field.

3.4 Data Collection Methods

For the data collection phase for our thesis, the researchers conducted interviews with three professional experts from ENISA who are based in Athens, Greece, two professionals from two different companies in Sweden and also two cybersecurity experts from FMV in Sweden. ENISA is an agency of the EU dedicated to improving network and information security across the EU member states. It was established in 2004 and plays a significant role in enhancing the overall cybersecurity posture within the EU by providing expertise, advice, and support in various cybersecurity-related areas. FMV, Försvarets Materielverk, is the Swedish Defence Materiel Administration. This government agency operates under the Swedish Ministry of Defence and is tasked with the procurement, development, and supply of defense equipment and systems for the Swedish armed forces. FMV's responsibilities include ensuring that the Swedish military is effectively equipped with the necessary technology and materials to maintain national security and defense capabilities. Collaborating with ENISA, FMV and the two other companies would provide access to a broad variety of relevant data, expertise, and a network of EU member states, making it an ideal scope for conducting this research.

The interviews focused on the experts' insights and experiences regarding the role of AI technologies in cybersecurity and cybercrime within the EU. The interviewees were selected based on their expertise in AI, cybersecurity, and cross-border data issues in roles such as cybersecurity experts, IT managers, policy advisors and key stakeholders in organisations that have familiarity with AI-driven cybersecurity solutions. These interviews aimed to explore experiences, perceived benefits, challenges, and the overall impact of these tools on their cybersecurity strategies.

Each interview was anticipated to last between thirty to sixty minutes, offering a comprehensive understanding while respecting the interviewee's time. To create the interview procedure and select interviewees for the study, the researchers referred to the study of Foddy (1993) as well as Brinkmann and Kvale (2015). Their studies highlight the need for a detailed and systematic preparation and clarity in scientific data collection. It is essential to consider

that interviewees might have their own clarifications of questions, so defining the research context and clarifying terms is vital for meaningful responses. In addition, assessing the organisation's information security posture involves measuring attitudes, requiring clear standards for comparison in the questions. To ensure the researchers collected useful and quality data from the interviews, they ensured that they had well-designed questions and made sure that respondents clearly understood them.

Before starting the procedure of conducting the interviews, participants were briefed on the objectives of the interview and assured of the confidentiality of their responses. To enhance the comprehensiveness of the interview notes and subject to the consent of the interviewees, audio recordings were made. In instances where face-to-face interviews were not feasible, web conferencing tools were used. Measures were taken to ensure the encryption and security of the recordings, with access strictly limited to circumstances with explicit consent from the interviewees.

The interviews were semi-structured, covering topics related to AI Technologies and Threat Detection, Human-AI Collaboration, AI's effectiveness in cybercrime detection, types of cyberthreats, challenges due to the EU's diverse legal landscape and the future trajectory of AI in cybercrime prevention. Semi-structured interviews, as outlined by Wilson (2013), provide flexibility in exploring topics that emerge during the conversation. By using semi-structured interviews, new issues were revealed through further questions and clarifications and as the researchers and the interviewers were more flexible, complex subjects were addressed and additional topics were discussed (Wilson, 2013).

3.4.1. Selection of Organisations

The selection of organisations for this study was strategically aligned with its objectives. The primary criterion was to engage with EU cybersecurity agencies that are pivotal in providing expertise and advice on cybersecurity policy issues to the EU and its member states, with Sweden being the main focus. We selected four organisations, including ENISA and FMV, which are detailed in the table below. The other two organisations, chosen for their significant roles within the cutting-edge technologies industry, requested anonymity and are therefore not explicitly named. These organisations were selected for their diverse contributions to the cybersecurity field and their varied service models, which collectively provide a comprehensive view of the sector. This selection enriches the study by offering a broad perspective on both the cybersecurity landscape and AI technologies, thereby enhancing the depth and relevance of the findings.

ENISA is the EU Agency for cybersecurity. ENISA, is a central entity based in Greece dedicated to enhancing cybersecurity across the EU. Established in 2004 and headquartered in Athens, ENISA assists EU Member States, institutions, and businesses in enhancing their cybersecurity capabilities. ENISA plays an essential role in developing a high common level of cybersecurity across Europe by providing expert advice, promoting best practices, and facilitating information exchange among stakeholders. ENISA also supports the development and implementation of EU policy and law in cybersecurity, making it a key player in Europe's digital security landscape.

FMV is the Swedish Defence Materiel Administration, an agency responsible for the acquisition and development of technology and equipment for the Swedish military. Based in Sweden, FMV ensures that the Swedish armed forces are equipped with the necessary resources to perform their duties effectively. The agency handles everything from procurement to testing, evaluation, and maintenance of defense material. Additionally, FMV provides expert technical and operational support, contributing significantly to national defense and security infrastructure.

Organization Name	Type of Organization	Country of Origin	Role	Contribution to Study	Reason for Selection
ENISA	EU Agency	Greece	Policy advisory and cybersecurity regulation	Provides insights on EU-wide cybersecurity policies	Expertise in EU cybersecurity initiatives
FMV	Government Agency	Sweden	Defense material and technology procurement	Insights into governmental cybersecurity standards	Role in national security
Company 1	Private Company	Sweden	Supply Chain	Insights into securing industrial operations and data	Demonstrated leadership in securing industrial operations
Company 2	Private Company	Sweden	Internet-of-Things	Expertise in IoT security solutions and technologies	Specialization in connected devices and network security

Table 3.1: Selected Organisations

3.4.2. Selection of Participants

In line with qualitative research practices, the selection of participants for this study was a thoughtful process aimed at accessing a distinct group of experts and professionals from a larger, limited target population that was central to our research focus (Miles et al., 2013). This selection was not only about identifying potential participants but also about gaining actual access to them, a process well-documented in the literature as being crucial yet challenging (Van De Ven and Johnson, 2006).

For broader insights, particularly from ENISA, a targeted approach was employed. This involved selecting and contacting experts through LinkedIn, with three experts agreeing to participate out of ten who responded. The process of maintaining access with each participant was essential, ensuring that each could freely share their expert knowledge (Saunders et al., 2016). Notably, funding from Lund University facilitated travel to Athens, Greece, enabling in-person interviews with key ENISA experts. This financial support was crucial in overcoming potential limitations in data collection and ensuring comprehensive engagement with the selected participants.

The snowball sampling technique further enhanced our access to relevant participants. A recommendation from one ENISA professional led to an interview with a former colleague

who now is employed by FMV. This method not only expanded our participant base but also enriched the quality and authenticity of the data collected.

Finally, we utilised personal networks to secure interviews with professionals at companies A and B, using our existing friendships to facilitate entry into these organisations. Additionally, the availability of time constrained and shaped our approach to data collection.

Participant	Job Role	Company	Industry	Format	Duration	Date
P1	Head of Unit - Market Certification and Standardisation	ENISA	Information Security Governance	In Person	1:03:40	08-04-24
P2	Team Leader - Knowledge & Information	ENISA	Information Security Governance	Online - Zoom	36:57	10-04-24
P3	Senior Telecommunications Expert	ENISA	Information Security Governance	Online - Microsoft Teams	50:02	11-04-24
P4	Data Scientist	Company 1	Supply Chain	In Person	49:23	27-04-24
P5	Expert Software Engineer	Company 2	Internet-of-Things	In Person	46:20	29-04-24
P6	Cybersecurity Expert - Rådgivare/Advisor	FMV/ICC	Defence	Online - Skype	51:41	08-05-24
P7	IT – Cybersecurity Expert	FMV	Defence	Online - Skype	51:41	08-05-24

Table 3.2: Summary of Participant and Interview Details

Interviews	Appendices
Interview guide / questions	Appendix 1
R1	Appendix 2
R2	Appendix 3
R3	Appendix 4
R4	Appendix 5
R5	Appendix 6
R6 & R7	Appendix 7

Table 3.3: Organisation of Interview Documents and Corresponding Appendices

3.4.3. Conduction of Interviews

The preparation for conducting the interviews involved several key steps to ensure both clarity for the respondents and adherence to ethical standards. Initially, respondents were informed a few days prior to the interview about the schedule and provided with essential

documents including the interview guide and the interview questions. An email was sent prior to the interview entailing practical aspects of the interviews and outlined the respondents' rights, ensuring that all ethical considerations were met. The interview guide was distributed in advance to allow respondents time to understand the structure and content of the interview, fostering a more informed and thoughtful discussion. Interviews were conducted in two formats: three were held online using Zoom, Microsoft Teams, and Skype, and three were in-person. They varied in duration from approximately 35 to 65 minutes, with an average of 50 minutes. Notably, the final interview involved two respondents, whereas all others were one-on-one sessions.

Each session began with respondents describing their job role and their organisation's role. To accurately capture and later analyse the responses, all interviews were recorded, except one. Recording the interviews, allowed us, the interviewers, to focus more attentively on the respondents rather than on note-taking. Following the interviews, the recorded data was used to initiate the interpretative process, a crucial part of our data analysis (Davidson, 2009). Consistent with best practices in qualitative research, the recordings were transcribed using the Whisper Transcription application after being captured with the Voice Memos application on an iPhone. This transcription was essential for the detailed analysis that followed.

The interviews, conducted with ethical considerations, including consent for recording and confidentiality, were transcribed and analysed qualitatively. Questions that were used as a guide to gather in-depth, qualitative insights can be found in Appendix 1. The insights gained from these questions are designed to directly address our thesis's primary research question, a comprehensive understanding of the cyberthreat environment in Europe. From the interviews, we were able to understand the practical applications and challenges of AI in cybercrime detection in the EU, thereby enriching the thesis with expert, practical perspectives.

3.5 Data Analysis Methods

In our study, NVivo and Microsoft Excel were employed for analysis. NVivo is a specialised software designed for qualitative data analysis that offers a strong set of features, specifically tailored for analysing text-based data such as interviews. Data analysed in NVivo was then exported to Excel for further manipulation. This integration of Nvivo and Microsoft Excel ensured a thorough analysis and effective presentation of the research findings.

The qualitative data gathered from interviews went through thematic analysis to identify and interpret patterns in the responses. This method involves transcribing the interviews, reading through the transcripts various times, and coding the data to highlight important themes and concepts. In more detail, at the initial stage of thematic analysis, the task of the researchers was to get acquainted with the data (Terry et al., 2017), a step that commenced after data gathering. Subsequently, the second stage entailed the creation of codes, which allowed the opportunity to delve deeper into the data and lay the groundwork for the analysis. As the coding advanced, the task was to find recurring patterns and similarities within the data.

3.5.1 Thematic Analysis

The thematic analysis of the interview transcripts was conducted using NVivo, a software designed to facilitate the efficient handling and analysis of qualitative data. This section outlines the process of thematic analysis and coding executed within NVivo, followed by the organisation of data using Microsoft Excel for collaborative review and refinement.

Step	Tools Used	Activities Performed
Importing and Familiarisation	NVivo	Initially, all interview transcripts, formatted as PDFs, were imported into NVivo. The first step involved a thorough reading of the transcripts to gain an in-depth understanding of the content. This reading phase was essential for the identification of initial codes, which were assigned to significant text sections that directly addressed the research questions.
Initial Coding	NVivo	Using NVivo's coding features, text segments considered relevant were highlighted and annotated with initial codes representing key concepts, ideas, or phrases relevant to the research aims.
Theme Identification	NVivo	After the initial coding, these preliminary codes were analyzed to identify patterns that suggested broader themes. NVivo's organisational tools were used to group related codes into categories that represented these themes.
Theme Review and Definition	NVivo	The identified themes were continuously reviewed and improved to ensure they accurately reflected the coded data and maintained consistency across the dataset. Each theme was clearly defined and named, capturing the meaning of the insights derived from the data.
Data Export and Organization in Excel	Microsoft Excel	To facilitate further analysis and clearer presentation, the coded data was exported from NVivo to Microsoft Excel. This spreadsheet was then uploaded to Google Drive, enabling real-time collaboration among the researchers. The data in Excel was organised into columns specifying the themes, with rows detailing responses from each participant. This structured approach enhanced clarity and accessibility, allowing for detailed analysis and discussion of the findings.
Integration into the Thesis	NVivo & Microsoft Excel	The use of NVivo for thematic analysis supported a systematic and comprehensive exploration of the interview data, significantly enhancing the reliability and validity of the findings. Subsequent export to Excel permitted additional data manipulation, which made the insights gained from the analysis more accessible and interpretable, therefore enriching the overall research narrative.

Table 3.4: The Process of Thematic Analysis

Themes	Codes
Enhancing Cybersecurity with Human-AI Collaboration	• Decision-Making • Cybersecurity & AI Education • Skills Gap
AI-Technologies in Cybersecurity	• AI-driven Threat Detection • ML & DL Deployment • Importance of Data • Missinformation
AI integration into Cybersecurity Frameworks	• Regulatory Compliance • AI Policy Development • AI gaps & Limitations in Cybesecurity • AI Lifecycle Methodologies
EU Cybersecurity Frameworks	• Standardization Initiatives • Legal Aspects • Relation with ENISA
Future Work	• Research Development • Technology Advancement

Table 3.5: Themes and codes from the interviews

3.6 Ethical Considerations

Ethical consideration in this research lies in the handling and reporting of sensitive information related to cyberthreats and vulnerabilities. As the study delved into the landscape of cybercrime within the EU, the ethical aim is to ensure the responsible and secure collection, storage, and dissemination of potentially confidential data. The researchers had the responsibility to uphold certain standards of professional conduct. Walsham (2006) pointed out three ethical areas of focus whilst conducting interpretive research in the information systems field which include confidentiality and anonymity, working with the organisation and reporting in the literature. It is important to keep in mind that cybersecurity threat intelligence often includes details about vulnerabilities that, if disclosed without proper precautions, could be exploited by malicious actors.

And so the researchers took care to ensure that this thesis study contributes positively to cybersecurity knowledge without inadvertently jeopardising the security of the participants involved. Before agreeing to participate in the study, the interviewees were informed that they would be assured the right to anonymity if they so wished, to confidentiality of any parts of the research that they did not want to be shared publicly and the right to withdraw at any point as recommended by Oates et al. (2022). This includes behaving with integrity in handling the data collected and ensuring that they respect the rights of the interviewees. Ethical considerations in handling and reporting data are essential to maintain the integrity of the research while prioritising the security and privacy of the individuals and organisations involved.

3.7 Scientific Quality

It is quite crucial to acknowledge that the scientific quality of this work is maintained. Scientific quality plays a pivotal role in a research proposal by ensuring that the proposed research project is well-conceived, methodologically sound, and has the potential to contribute meaningfully to the field of study (IS). Below are the identified relevant considerations that were made to ensure the most appropriate and relevant process for a research study.

To ensure internal validity, the study employed rigorous data collection and analysis techniques, controlling for confounding variables and minimising bias. This included employing standardised measures and double-blinding when applicable. To enhance external validity, the study aimed to generalise its findings to a broader population or context. This involved selecting a representative sample, employing a longitudinal design, and carefully considering the sampling strategy. Enhancing ecological validity was achieved by ensuring that the study was conducted in real-world settings that reflected the natural context of cybersecurity and AI. This allowed for a more authentic understanding of how these technologies operate and interact. To ensure construct validity, the measures used in the study aimed to accurately and reliably capture the constructs of interest. This involved carefully defining the constructs and selecting appropriate measurement tools.

The study was also conducted with transparency and openness, making clear the methodology, data collection procedures, and analysis techniques. This fostered credibility and allowed for replication and verification. The study's procedures were documented in sufficient detail to allow for external auditing, enabling independent reviewers to assess the rigour and thoroughness of the research. The study adhered to ethical principles of data handling and privacy protection, ensuring that participants' data was confidential and secure.

4 Results

The results from the study are presented below. Based on the findings from the thematic analysis and coding process, identified themes and subthemes are discussed in the following section.

In this chapter, the researchers present findings from the semi-structured interviews that took place with seven different interview participants. Issues, concerns and suggestions that arose from the conducted interviews are presented here. The interviewees are listed as numbers from 1 to 7 in order to keep the participants anonymous and they have been specified as P1, P2, P3, P4, P5, P6 and P7. In the analysis that follows, specific references to the data are denoted using a participant and line number format. For instance, "(P5:L13)" refers to the statement made by Participant 5 on line 13 of their interview transcript. The interview participants were selected based on their work description, connection and relevance to the topic of this Master's thesis study. Focus was put on interviewing a blend between cybersecurity industry professionals, experts from FMV within Sweden and experts from ENISA.

4.1 Enhancing Cybersecurity with Human-Artificial Intelligence Collaboration

The interviews highlight a critical agreement on the need for effective synergy between human capabilities and AI technologies in cybersecurity. (P5:L25) discusses the current role of humans in pattern recognition and proposes a future where AI automates this task, with humans overseeing and verifying the output. This approach aims to influence AI for efficiency while maintaining human oversight for quality control, representing a collaborative synergy that improves both speed and reliability in cybersecurity measures. (P5:L23), emphasises that despite the automation, there is a clear need for human oversight. AI-generated patterns still require a human to review and verify them to ensure they are reasonable and accurate. The organisation where P5 currently is employed, has a team of three people dedicated to these tasks, referred to as cybersecurity coaches (L25), who work alongside regular developers on a part-time basis. According to (P6:L25), initially, IT consultants who specialise in security work, incident handling, and other related IT security tasks were not necessarily labelled as cybersecurity experts. However, due to the expansion of the cybersecurity sector to include these activities under the umbrella of "managed security services," these IT consultants are now recognized as cybersecurity professionals. Asking how the future looks like for the number of employees working on these operations, (P5:L29) expects the possibility of increasing the number of personnel dedicated to these tasks as the scale of cybersecurity operations grows.

Cybersecurity professionals, including (P2:L14), traditionally focused on studying network protocols, computer software programming languages, and device configurations. However, as P2 stated, they were not trained to work with advanced intelligence systems that are

rapidly progressing today. When presented with an AI solution, even the most experienced cybersecurity professionals face a significant learning curve. They must adapt to the fact that AI does not follow a deterministic model, which is common in other IT systems. Instead, AI operates on a probabilistic model, which requires analysis in conjunction with the data used for its training. This necessitates a different mindset. Consequently, within the intersection of AI and cybersecurity, there are relatively few professionals who are proficient in both areas. An important theme across the interviews is the existing skills gap within the cybersecurity personnel, particularly concerning AI. (P2:L14) explicitly emphasises this gap, stating, "If you imagine a Venn diagram of AI and Cybersecurity, there are not that many people, both experts in AI and cybersecurity." According to P2, this gap is significant enough that it is considered the second biggest threat in the field by 2030, as noted in one of their articles. The gap is not just an EU issue but a global concern. This respondent further highlights the need for current professionals to go through retraining to bridge this gap, suggesting an adjustment in training methodologies to include AI-focused curricula in cybersecurity education programs. More specifically, the areas lacking include automation, algorithms, and the overall analytical approach required to implement AI effectively. This lack of expertise limits the potential benefits that could be gained from AI, emphasising the need for targeted training and education. In addition, after being asked whether there are cybersecurity policies that hold back organisations and businesses from using AI technologies for threat detection, P2 clarifies that there are no significant policy barriers that hinder the use of AI technologies in cybersecurity. Instead, European policies are designed to actively foster the development and integration of AI, with significant funding directed towards AI-powered solutions. The EU policy environment is supportive, aiming to encourage research and the development of AI tools in cybersecurity. Moreover, (P6:22) described the skills gap in the cybersecurity field, as a significant concern, especially given the daily challenges in recruiting qualified personnel. As P6 mentioned, the need for diverse expertise is evident in the requirement for technical experts, lawyers, and administrative staff to work together, particularly in preparing laws and regulations that guide workplace procedures. This interdisciplinary approach ensures that legislative frameworks remain connected to real-world applications, fostering more effective and relevant policies.

Regarding certifications, (P6:L25) mentions the CISSP, a globally recognized credential that validates an individual's expertise in designing, implementing, and managing a best-in-class cybersecurity program. With the growing demand for skilled professionals, (P6:25), emphasised the existence of various certifications available, emphasising that the aim is to establish a certification scheme aligned with the CSA to address specific skills within the sector. Furthermore, P7 highlights a "grey zone" between national security and the internal market, pointing out that the CSA primarily focuses on internal market-based legislation. The goal here is to ensure that trusted services are strictly skill-based, enhancing the alignment between legislative requirements and actual cybersecurity expertise in the marketplace.

As noted by P1, one of the roles of ENISA is to promote cybersecurity skills not only among organisations and businesses but also the young generation. The interviewee mentioned that through competitions and challenges, cybersecurity is promoted to the youngsters aiming to enhance their cryptography skills, fundamental for cybersecurity. The interviewee related these competitions to major sporting events. As stated, "These cryptography competitions are

like the World Football or the European Football Championship for cryptographers". This not only develops skills but also brings together member states in a co-operative effort. However, there is an acknowledgment that while building capacity is crucial, there is also a need to maintain existing systems and frameworks, as noted by the same interviewee, suggesting a balanced approach between development and maintenance. This requires professionals who not only can develop new systems but also those who can manage, update, and maintain existing systems effectively. In line with this is (P5:L35), who also emphasises the importance of reinforcement of specific training programs, with a need to tailor these programs not just to departmental requirements but also to broader organisational cybersecurity practices.

In addition, (P5:L39) mentioned that their organisation provides cybersecurity training that is tailored to specific departments within the organisation, indicating a targeted approach to skill development based on the unique needs and roles within different areas of the company. Furthermore, all employees, regardless of department, are trained to maintain basic cybersecurity hygiene. This kind of training typically covers fundamental security practices to prevent common cyberthreats. Similarly, as P4 stated, their company offers a range of cybersecurity courses designed to educate and train employees. Participation in some of these courses is mandatory, while others are optional, allowing them to choose based on their interests and career needs. The training includes crucial topics on cyber hygiene to enhance their knowledge and skills in protecting the company's digital environment. P4 then stated that as an employee, it is crucial to understand that they hold responsibility for any data breaches that occur due to their actions. This policy underscores the importance of the training provided and their role in maintaining the company's cybersecurity integrity. Generally, the findings indicated a strong agreement on the importance of augmenting human-AI synergy in cybersecurity, addressing the significant skills gap, and adapting training and frameworks to meet future needs. While the integration of AI offers promising enhancements to cybersecurity measures, it also requires an adjustment of skills, policies, and frameworks to ensure that both human expertise and AI capabilities are optimally utilised.

4.2 AI Technologies in Cybersecurity

4.2.1. Integration of Artificial Intelligence in Cybersecurity in the European Union

As per P1, ENISA is actively assessing and guiding the integration of AI technologies within European cybersecurity frameworks. (P1:L15) recognizes the gap in Europe's capabilities in AI, stating that while the continent may lag behind in developing LLMs and generative AI, it remains competitive in AI technologies with narrowly defined applications. Similarly, (P2:L20), also stated that there seems to be a gap in fully leveraging AI capabilities to enhance security measures, suggesting room for greater innovation and application in the field, in the EU. (P1:L15), then stated that this acknowledgment steers ENISA's focus towards enhancing specialised AI applications that are tailored to meet specific European needs. A significant aspect of ENISA's strategic approach involves improving AI systems by training them on diverse datasets that are representative of various European markets. This method ensures that AI technologies are not only advanced but also practical and relevant to specific regional demands.

Looking ahead, ENISA expects the establishment of a certification process for AI technologies. This prospective certification will define the necessary cybersecurity controls for AI applications, underscoring ENISA's integral role in safeguarding the security integrity of AI within Europe. The aim is to synchronise the evolution of AI technologies with strong regulatory and security standards, thereby developing a secure and reliable AI ecosystem across the EU. When our discussion centred on the role of AI in cybersecurity, specifically within the context of certification, (P7:L13) mentioned their involvement in an AI feasibility study for cybersecurity certification, indicating that various AI technologies, including ML and DL, could potentially be certified for cybersecurity applications. However, the scope of their current work is strictly focused on certification processes. (P7:L10) also emphasised that their project does not limit itself to a specific type of AI model; rather, it considers a broad range of AI technologies that could be applicable for certification. This implies a flexible approach to evaluating different AI models for their potential use in enhancing cybersecurity measures. The discussion also touched on the broader landscape of AI and cybersecurity in Sweden, mentioning the existence of an AI commission and various other agencies, which might be more directly involved in broader AI initiatives than the interviewee's agency. They noted that their agency's involvement is quite specialised and limited to certification aspects of cybersecurity.

Asking about the implementation of AI technologies and ENISA's role in that matter, (P2:L2) stated that ENISA began formally focusing on AI in early 2020, following a directive from the European Commission. This directive was part of a broader action plan for AI in Europe, which tasked ENISA with assessing the AI threat landscape, in other words to gain knowledge regarding the cybersecurity threats associated with AI. To tackle this challenge, ENISA first required to define what makes AI more established, exploring its various technologies, processes, actors, and assets. According to (P2:L2), the goal was to identify and categorise potential threats across these elements, leading to a dynamic and evolving nature of AI technology through a lifecycle model. This model outlines the stages of AI system development, including design, implementation, deployment, training, and adaptation. To enrich this analysis, ENISA formed an expert group comprising approximately twenty-five stakeholders from academia, industry, the public sector, private sector, SMEs, and other European agencies such as the European Defense Agency and Europol. This collaborative approach helped to establish a comprehensive understanding of the AI cybersecurity threat landscape, providing a foundation for ongoing evaluation and response to AI-related security challenges.

As per (P3:L2), AI is a powerful tool in combating cybersecurity threats due to its speed and scale. However, its fast evolution also presents challenges in maintaining effective control. As (P3:L2) further explains, attackers can misuse AI to launch cyberthreats, emphasising the technology's dual use nature. In line with this was P5, who stated that one potential benefit of the regulation of AI within the EU is that it could provide clearer guidance on what is permissible to develop and what is not. If we design a system according to the guidelines and report everything appropriately, but it still ends up being used for harmful purposes, we can point to the EU's approval as a defence, indicating that we complied with all the required standards. Therefore, as per (P3:L2), the AIA remains intentionally nonspecific, adopting a "wait and see" approach due to the unpredictable nature of AI advancements. A

recommended strategy to reduce risks without imposing strict regulations is to promote a diverse ecosystem of open-source AI initiatives. This approach prevents any single entity from dominating and encourages a self-regulating environment. Embracing open source can improve collaborative efforts in cybersecurity, fostering a dynamic and responsive AI landscape.

4.2.2 The Role of AI Technologies in Cybersecurity

As per (P1:L25), organisations are increasingly integrating AI technologies, emphasising the utility of ML, to increase performance and efficiency. ML represents a significant advancement beyond earlier technologies such as NN. It involves continuously training algorithms on new data sets to improve their accuracy and reduce failures. According to (P2:L2), ML is identified as the most effective and widely deployed AI technology within cybersecurity applications. Its occurrence is due to the availability of advanced, pre-developed models from open-source libraries, which organisations can quickly implement. According to (P2:L16), cybersecurity professionals currently employ AI primarily for pattern matching to identify network threats and automate the processing of large data volumes. While there is potential to expand AI usage to adaptive security controls, this area remains underexplored within the community. As (P2:L10) mentioned there has been a focused effort to study ML algorithms, within the cybersecurity domain emphasising the importance and complexity of integrating ML into cybersecurity practices, highlighting both its potential and the cautious approach required in its application.

When P5 asked how its organisation is prepared proactively against cybersecurity scenarios, P5 provided an in-depth look into the security protocols employed by their company, focusing on a combination of threat modelling, encryption, input validation, and dedication to established security patterns. The first line of defence, as described by the interviewee, involves threat modelling. This process entails a detailed analysis of the product by mapping all the data paths involved. (P5:L53) continues that in order to secure the data transmission between clients and the web server, the company utilises TLS. TLS plays an essential role in encrypting the data as it moves across the internet, ensuring that any data intercepted during transmission remains unreadable and secure from unauthorised access or manipulation. Another significant aspect of the organisation's security strategy involves rigorous inspection of data inputs. The company checks for potentially malicious input that could compromise the system. This step is essential for defending against common cyberthreats where attackers misuse input data to breach the system. As (P5:L23) stated, while the potential of using DL models to automate the generation of security protocols is acknowledged, the interviewee highlighted that the company currently relies on traditional methods. In particular, they utilise established security patterns which are formulaic but highly effective, especially for commonly used system architectures like web services with databases. By employing these recognized patterns, the company ensures the consistent application of proven security measures, thus maintaining strong protection across their digital infrastructure.

As mentioned earlier, the effectiveness of ML is depending upon the quality of the algorithms and the relevance of the data used. (P1:L17), gave an example of traffic data from one city

that cannot accurately predict traffic patterns in another due to unique local conditions. This specificity is also critical in sectors like eHealth, where applications must be tailored to distinct health data and outcomes. Moreover, (P1:L15:L17), emphasised that the ongoing development of AI applications is not just about refining algorithms but also about ensuring they are trained with high quality data. This process is complex and time-consuming, often involving various interdisciplinary elements from cloud infrastructure to semiconductor technologies. In line with this was P2, stating that the adoption of these models necessitates careful evaluation, particularly in terms of potential data biases and the training processes used, to ensure they are suitable for specific security contexts. Thus, as (P1:L15) mentioned, AI development is likened to constructing a building; it is a comprehensive process that requires attention to numerous underlying and interconnected components.

4.2.3 Integrating Artificial Intelligence into Data Management and Cybersecurity

When it comes to integrating AI into data management and cybersecurity practices, insights gathered from both ENISA experts and industry professionals offer a comprehensive understanding of the opportunities and challenges. This analysis draws from the experiences and perspectives shared by the seven interviewees, each providing a unique point on the implications of AI in their respective fields.

(P5:L19) raised critical concerns regarding the deployment of LLMs for significant applications. According to P5, the primary challenge involves the uncertainty around data handling and the potential biases within AI models. This interviewee's perspective underlines a major issue in AI deployment; the difficulty in tracking and controlling where and how data is processed. As a result, organisations may find themselves limited to using LLMs for less critical tasks, such as drafting routine communications rather than for processes where data sensitivity is high. (P2:L2:L28) emphasised the vital role of data as the backbone of AI efficacy. The insight provided by this interviewee highlights that the utility of AI technologies heavily depends on the contextual accuracy and relevance of the data they process. (P3:L10:L12) expanded on the risks associated with AI, particularly focusing on misinformation as a growing threat. P3 emphasised the ease with which AI can be employed to manipulate information, thus influencing outcomes in critical areas such as electoral politics. The potential of AI to produce incorrect outcomes based on improperly managed data further complicates its application, emphasising the need for strict controls over data inputs to prevent faulty decision-making processes. P4 offered a practical viewpoint on the internal strategies for managing data within their organisation.

Mentioning the use of data lakes and strict authentication and authorization protocols, P4 highlighted the measures necessary to secure data integrity in their organisation. More specifically, their company utilises a data lake where data engineers deposit the data collected. A data lake serves as a centralised repository that allows for the storage of structured and unstructured data at scale. This system facilitates the efficient management of big data volumes, making it easier to apply analytics and derive insights. As their company follows strict privacy protocols, particularly regarding internal data sharing, certain sensitive information is intentionally withheld from being shared among colleagues to prevent

unauthorised access and maintain confidentiality. Access to protected data is managed through the use of Git and personal identification techniques. According to P4, employees must send specific code requests to access certain datasets, ensuring that only authorised personnel can view or manipulate sensitive data. To further secure data, the company has implemented strong authentication mechanisms. These measures are critical for safeguarding the integrity and security of data against unauthorised access or breaches. Regarding the distribution of analytical results, the company employs tools like PowerBI. This allows for the efficient transformation of data into actionable insights, which are then securely shared with the necessary stakeholders within the company.

Overall, the company's approach to data management is methodical and security-focused, ensuring that all data handled is well-protected, compliant with legal standards, and accessible only to those with legitimate need. While P4 provides a more detailed view of internal data management policies and practices, P5 focuses more on technical measures to secure software and data transmission. For instance, (P5:L53) highlighted that their company protects the software running on devices by cryptographically signing it. This security measure ensures that only authorised, verified code can be installed and run on the devices, providing a fundamental layer of protection against unauthorised or malicious software modifications. (P5:L53) also mentioned the use of TLS to secure network connections, ensuring that the data remains confidential and intact. TLS is the security component behind HTTPS (indicated by the 'S' in HTTPS), which secures websites by encrypting the data exchanged between the user's browser and the website. Both responses from P4 and P5 reveal a structured approach to cybersecurity, emphasising the importance of secure data handling practices, authentication, and controlled access.

4.2.4 Limitations, Challenges and Opportunities

Moreover, according to P1, one of the significant challenges ENISA faces in integrating AI into existing cybersecurity frameworks concerns the broader ecosystem, encompassing both policy and user engagement. (P1:L19), referred to the advancement of cutting-edge tools like ChatGPT as extensive solutions, but explained that this is not necessarily true, because such products or services are insufficient; rather, it's simply premature to consider these technologies as comprehensive solutions. In areas like threat detection, AI has not yet reached a level of maturity where it can fully replace existing methods. Using AI as a supplementary tool for specific tasks such as data analysis or code translation across different programming languages could be highly beneficial. However, the expectation that AI alone can address all aspects of threat detection is unrealistic, as (P1:L19) stated. Users should maintain a balanced approach, integrating AI to augment capabilities while continuing to rely on established human-driven processes.

According to (P3:L6), at ENISA they have been concerned about the potential widespread use of AI in telecommunications, particularly as they work on securing 5G networks. However, nothing more could be said or explained further in detail apart from the shift that introduces more cybersecurity risks is the fact that as more virtualized networks with AI agents increase the vulnerability to attacks. The move towards virtualization and reliance on AI creates a larger attack surface, making it easier for cyber attacks to occur. The concern is not just the virtualization itself but the potential for massive disruptions like denial of service

attacks that AI could execute on a large scale. Moreover, biometrics and personal data protection remain dominant due to their sensitivity. Another prime risk is the misuse of personal data through cyber terrorism, which does not necessarily involve sophisticated AI but could be as simple as manipulating social media profiles. This type of threat highlights the wider challenge of maintaining security in a highly connected world, where continuous connectivity can expose individuals to constant cyberthreats. The European Commission is addressing these concerns by proposing measures to ensure consistent connectivity without compromising security, indicating the complexity of cybersecurity in an interconnected environment.

4.2.5 Future Directions

(P1:L25) after being asked about the integration of AI technologies into cybersecurity practices outlined the organisation's vision and believes that the establishment of legal frameworks will gradually enhance public understanding of AI's role in cybersecurity, though this clarity might take a decade or more to fully develop. Reflecting on past experiences with personal data regulation, the interviewee suggests that while AI development might not require as long, due to faster development vectors in today's technology landscape. However, (P1:L25) emphasised that while some cybersecurity operations could be increasingly automated, complete automation, especially in decision-making, remains challenging. AI's current utility is predominantly in sorting, collecting, cross-analyzing, and aggregating data, tasks that historically leverage computational power. In addition, the increase of data sources and the exponential increase in data volume are noted. The interviewee recognizes that AI, despite its advanced heuristic capabilities, primarily serves as a tool for managing large and complex datasets. This underscores the continuing need for AI to complement human capabilities rather than replace them, reflecting a realistic view amongst common fears of AI supplanting human roles. This approach aims to harness the potential of new technologies to drive economic advancement in the EU.

4.3 European Union Cybersecurity Frameworks and Landscape

When asked to describe their current job role and how it is connected to cybersecurity, P1, P2 and P3 all indicated that they serve in different capacities at ENISA in providing guidance to support member states of the European Commission around the development of information security policy. (P3:L17:L33:L57) specifically indicated that they served more in a role that created research reports that build towards network equipment and micro chip cards in the certification of 5G. (P1:L2) was more involved in a market certification standardisation role by indicating that "*we just take snapshots of market segments and we analyse them…with a view to draw conclusions for policy makers primarily, but also for industry.*" (P2:L6) clarified that ENISA does not have any regulatory power, "*so whatever ENISA comes up with, it is guidelines I would call them, there's no legal enforcement*".

P4 and P5 were more involved at an industry level and so their connection to ENISA is more on the level of application of the guidelines. (P5:L12) who works in the IoT Industry shared that their closest connection to ENISA is through the Connected Standards Alliance

regulatory working group and also through "*fulfilling those requirements that are very hard to promise because they are so loose*". P4 who serves in the supply chain industry in more of a data science forecasting role, indicated that the company has clear policies and procedures for how to collect, store, access and use data well in a manner that ensures compliance with regulation and industry standards.

In a later interview with P6 and P7 who are employees of FMV, different perspectives were brought up in connection with the focused work the professionals do in certification of security products and services. (P6:L5) comprehensively explained the connection between their organisation and ENISA "*ENISA (drafts certification frameworks) together with an ad hoc working group with stakeholders from different constituencies, from the private stakeholders, researchers, member state authorities and these kinds of things. Before this draft from ENISA goes to the Commission, they have to consult… a group of national agencies on cybersecurity certification. And we are the Swedish agency in that group*". "*And then there's a public consultation that ENISA makes on his draft. When ENISA is ready and thinks that they have something, they send it to the European Commission to become legislated. And the European Commission transposes that draft into an implementing regulation. They make a proposal and then the Commission negotiates that proposal together with the EU member states. And once adopted, you have certifications.*"

When asked about the connection to industry professionals, (P6:L7) explained that whilst there is public consultation on the draft proposal by the European Commission on their website called "*Have Your Say*", the negotiations and documents are not meant to be publicised but "if you know anything about EU Policy, you know that every version will leak, especially if it's politically interesting". And yet, a lot of people still complain about transparency, which P7 believes is partially right.

Both P4 and P5, when asked about how they see AI integrating with existing cybersecurity frameworks within industrial environments, highlighted that "*there are a lot of rules and standards we have to follow, especially in value-chain industries. We need to make sure our systems meet all the legal requirements*". In this industry, the cost in addition to the daunting task of knowing which new smart technologies will be the most ideal to the unique setting, make companies somewhat hesitant about investing in new systems.

P5 shared their understanding of the process of the implementation of legal frameworks with a vague process explanation that began with the European Commission Parliament who set requirements that companies in industry are required to follow. This entails how the devices should be stored on the network and that there should be no impersonation thereof. P5 was of the opinion that the requirements are hard to fulfil because they are so loose. However, when it comes to complying to ENISA standards, (P5:L12) stated "*that provides sort of like a framework for if we certify or comply with those requirements, we can be quite sure that we have fulfilled the delegated act requirements*".

Regarding the implementation of AI into Cybersecurity frameworks, (P6:L28) stated that it is not currently mentioned in the schemes right now. However, "*you have the AI Act with some security requirements, the Cyber Resilience Act with some is directed with some ideas with some subject security requirements on electronic ID. And you have a handful more; some of them are pointing to the Cybersecurity Act and Cybersecurity Act Certification on the security features. Some of them don't.*"

In addressing the processing of these frameworks, (P2:L6), clarified that "*ENISA doesn't have any regulatory power. So whatever ENISA comes up with, it's… guidelines would call them. If there's no legal enforcement, so when ENISA came up with this, you have to do this.* ". The European Commision develops legal requirements and whilst ENISA's guidelines are not compulsory for anyone, they are recommendations. When asked about existent policy frameworks, (P3:L17) shared that, "*What can help is the collaboration between the industry, the people that are implementing, and some like code of conduct for AI.*" In addition (P3:L17) said that when ENISA was asked to do a feasibility study on AI certification, they were not sure where to start from.

(P1:L8) indicated that the industry which suffers the most from cyber attacks is the public sector as perpetrators perceive it as likely to yield maximum benefits. (P2:L14) mentions that it is all of the sectors in their opinion "*because AI is everywhere. You see it even in communications people, communications projects have to struggle every day with fake news and help to identify manipulated information and what is needed.*" In terms of the demographic threat landscape, (P3:L33) mentions that some geopolitical challenges exist with the impact that AI has introduced and that Europe is trying to adjust to the challenges and suggests making some projects open source, as a possible solution.

In response to what challenges ENISA is facing in integrating AI into cybersecurity frameworks, (P1:L19) indicated that "*I think the challenge is primarily for the ecosystem. So for policy or for the users when they are confronted with hyperscalers who say "Ah, ChatGPT, that's the thing" and then the part gives you answers to everything, don't buy it. Not because it's a bad product or an appropriate service, it's not that. It's too early to call it a day. We're not there yet. So even in terms of threat detection using AI, we're not quite there as well."* ENISA has been working on this concept which is hard to define, in order to carve a role for itself and help others understand what the role of AI will be. More specifically, (P1:L15) stated that "when it comes down to the LLMs and the generative models, Europe is not very strong. But in more closely defined ones, we're not that far behind either. And I think that's good news." They further explained that the goal is to scale up and to build on the credibility of LLMs such that specific data sets that reflect the reality on the ground are adopted, that will improve the European market. In terms of the formulation of legal frameworks, ENISA could make an observation by just parsing through the AIA that at some stage there will be certification for AI.

5. Discussion

In this section, the results gathered from the interviews will be discussed and compared to the literature review presented in chapter two. The results will be analysed in order to be able to draw conclusions from the collected data.

5.1 Human - Artificial Intelligence Synergy

The literature strongly supports the integration of AI as a means to augment human expertise within cybersecurity frameworks (Sinclair, 2023; Nielsen, 2023; Bao et al., 2023). These scholarly views emphasise that AI is not a replacement for human judgement but a complementary tool that enhances human decision-making capabilities. This partnership aims not to replace human intelligence but to augment it, fostering a cooperative intelligence that leverages the collective strengths of both humans and machines (Petrović and Jovanović, 2024). Insights from P5 emphasise this belief by detailing current practices where AI automates routine pattern recognition tasks, thus allowing cybersecurity professionals to focus on more complex decision-making processes. This is verified in the literature related to AI-enhanced human expertise and also illustrates the subtle balance required between automated solutions and human oversight.

Kioskli et al. (2023) and Petrović and Jovanović (2024) propose that cybersecurity solutions should prioritise a human-centric AI approach, which is confirmed in the operational strategies discussed by interviewees P4 and P5. This approach ensures that while AI handles the breadth of data processing and threat detection, humans remain integral to the strategic decision-making process, particularly in high-risk scenarios. Petrović and Jovanović (2024) more specifically argue that human analysts are crucial due to their unique capacity for judgement and detailed response. AI should be viewed as a supportive tool that enhances human capabilities, allowing analysts to shift their focus from routine tasks to strategic decision-making. This alignment between theory and practice highlights the potential for AI to improve rather than intrude upon human capabilities, ensuring that cybersecurity operations remain adaptable and ethically grounded.

The significant global shortage of cybersecurity professionals is a pressing issue identified both in the literature (Starnes, 2024; Ricci et al., 2024) and the interviews. The discussion around this theme reveals a crucial gap between the demand for skilled cybersecurity professionals and the available talent group. P2's emphasis on training, retraining and integrating AI-focused curricula into educational programs suggests a proactive approach to bridging this gap. This recommendation aligns with the scholarly call for enhanced educational strategies and highlights a practical response that addresses both immediate and long-term needs in the cybersecurity workforce. In particular, according to P2, this gap is significant enough that it is considered the second biggest threat in the field by 2030, as noted in the literature (ENISA, 2022). Moreover, responses regarding the skills gap suggests that the field of cybersecurity has broadened its scope beyond traditional roles. Initially, IT consultants or developers were not necessarily labelled as cybersecurity experts. However,

due to the expansion of the cybersecurity sector to include these activities under the umbrella of "managed security services," these IT consultants and developers are now recognized as cybersecurity professionals. This shift indicates that as the demand for cybersecurity expertise exceeds the supply of trained professionals, roles that were once considered distinct areas of IT are now integrated into the broader category of cybersecurity. The term "managed security services" as mentioned by P6, refers to outsourced services provided by these professionals to handle an organisation's cybersecurity needs comprehensively. This evolution in the field also highlights the skills gap, as there is a pressing need for more individuals who are formally trained and recognized as cybersecurity experts to meet growing security demands.

Petrović and Jovanović (2024) emphasise the importance of adopting a comprehensive strategy that integrates continuous research, development, and policy formulation, all of which are crucial in addressing the complexities of today's digital world. This integrated approach aims to develop a digital ecosystem that is both secure and resilient, effectively utilising both human and technological assets.In agreement with this was our second interviewer, P2, who highlighted that the policies within Europe are structured to actively promote the growth and incorporation of AI technologies into cybersecurity. The policy landscape in the EU is therefore supportive, designed to stimulate both research and the creation of new AI tools for cybersecurity.

Lai et al. (2021) underscore the importance of conducting periodic reassessments of AI technologies to stay well informed of rapid advancements and ensure that the integration of AI into cybersecurity remains effective and current. These periodic reviews are essential for enhancing our understanding of the dynamic relationship between human expertise and AI capabilities and for maintaining a comprehensive approach to cybersecurity. In line with this recommendation, P1 acknowledged the dual necessity of developing new capabilities while also sustaining existing systems. This perspective highlights a critical balance required in cybersecurity management; professionals must be skilled at both innovating new solutions and maintaining and updating existing frameworks effectively. This balanced approach ensures that while the sector advances, it does not do so at the expense of existing system integrity. Further emphasising the importance of ongoing education and capacity building, P1 discussed ENISA's role in promoting cybersecurity skills among organisations and the younger generation. The use of competitions and challenges to enhance cryptography skills among youth illustrates a proactive approach to encouraging and developing a skilled workforce. Similarly, P5 pointed out the significance of maintaining robust systems and frameworks alongside new developments. This mirrors the strategic emphasis in the literature on tailored training programs that are designed to equip professionals with the necessary skills to navigate the rapidly evolving cybersecurity landscape efficiently. These insights collectively illustrate a strategic approach ensuring that as the field evolves, it does so with a workforce that is not only technically proficient but also deeply aware of the foundational systems that protect our digital environments.

5.2 Artificial Intelligence Technologies used for Protection

5.2.1. The Role of Artificial Intelligence Technologies in Cybersecurity

In the integration of AI technologies within organisational frameworks, particularly in the field of cybersecurity, an emphasis is placed on the use of ML. As P1 stated, the deployment of ML technologies is driven by their potential to significantly improve operational performance and efficiency. ML represents a significant advancement beyond earlier AI applications such as neural networks. ML's ability to continuously train on new datasets ensures both improved accuracy and reduced failure rates. Supporting this view, P2 points out that ML is not only the most effective but also the most widely deployed AI technology in cybersecurity settings. This dominance is largely facilitated by the accessibility of advanced, pre-developed ML models available through open-source libraries, allowing for quick adoption and implementation within organisations. Moreover, P2 discusses the primary application of AI in pattern matching, aimed at detecting network threats and managing vast data volumes efficiently. Although there is a recognized potential for extending AI applications to include adaptive security controls, this aspect remains largely underexplored, suggesting a potential area for future development.

The scholarly work of Kioskli et al. (2023) expands on this by examining the implications of DL in cybersecurity. The integration of DL in cybersecurity indicates a significant advancement in combating evolving cyberthreats. As highlighted by Kioskli et al. (2023), as cyberthreats grow in complexity, the importance of DL in enabling organisations to respond quickly and effectively to potential security breaches becomes increasingly dangerous. However, contrasting these advancements in AI technologies, P5 mentions that despite recognizing the potential of DL models in automating the generation of security protocols, their company continues to rely on traditional methods. For this particular case, there is a gap between the theoretical advancements discussed in the literature and practical implementation in organisational settings. Nonetheless, according to Huyen and Bao (2024) the use of intelligent solutions such as ML and behavioural analytics, illustrates a forward-thinking strategy.

These technologies are capable at analysing and adapting to threats in real-time, recognizing unusual behaviours that may signal a security threat, and taking into account various factors such as user behaviour and network traffic. This proactive approach not only enables organisations to prevent attacks but also minimises potential harm and disruption. Thus, while the literature underscores the sophisticated capabilities of emerging AI technologies like DL in enhancing cybersecurity, interviews with practitioners reveal a more cautious, gradual adoption and integration of these technologies within existing cybersecurity frameworks. This blend of insights from literature and real-world applications paints a comprehensive picture of the ongoing evolution and challenges in the integration of AI into cybersecurity practices.

5.2.2. Integrating Artificial Intelligence into Data Management and Cybersecurity

According to Ansari et al. (2022) the urgent need to secure data has catalysed the expansion of the cybersecurity field, where AI has a great impact. AI's ability in processing and analysing large data sets has significantly improved sectors such as banking, telecommunications, healthcare, entertainment, online retail, automotive, and insurance. These industries utilise AI to develop robust cybersecurity solutions for their information systems, either through standalone AI tools or comprehensive integrated solutions. P1 notes that such recognition has guided ENISA to prioritise the development of AI applications customised for specific European requirements. According to P1, a key strategy of ENISA involves refining AI technologies by training them with diverse datasets that mirror the variety of European market scenarios, ensuring the technologies are directly applicable and relevant to regional needs. Khraisat and Alazab (2021) identify pattern creation as a critical and growing field within AI application in cybersecurity. This process involves collecting a vast array of data from computing infrastructures, network traffic, and publicly available data on known cyberthreats worldwide. The subsequent analysis of this data through sophisticated data analytics tools plays a pivotal role in proactively identifying potential security threats (Ansari et al., 2022; Patel, 2023).

P4, transitioning from being a data analyst to data scientist, offered a practical viewpoint on the internal strategies for managing data within their organisation. For instance, P4 describes the use of a data lake in their organisation, which centralises the storage of both structured and unstructured data, facilitating efficient data management and analysis. This setup supports the application of AI-driven analytics to derive insights that are essential for maintaining data security. Moreover, the company's stringent access protocols, including the use of authentication and authorization techniques, exemplify the integration of AI tools in safeguarding data integrity and confidentiality. This approach is complemented by cryptographic measures as mentioned by P5, where software is secured against unauthorised modifications, thereby reinforcing the overall cybersecurity framework. In line with this is the literature (Ansari et al., 2022), stating that initial AI applications initially utilised signature-based techniques to identify patterns of attacks, significantly enhancing the rapid and effective detection of threats and malware. This approach greatly improved the management of massive data volumes through AI.

Furthermore, the distribution of analytical results within companies, as managed through tools like Power BI, as mentioned by P4, underscores the role of AI in transforming raw data into actionable insights that are securely shared within the organisation. This ensures that data-driven decisions are both informed and protected, aligning with legal standards and operational requirements. This shows that the integration of AI into data management and cybersecurity can enhance the ability to handle and analyse large volumes of data and improve the security measures and protocols within organisations. The ongoing advancements in AI technologies and their application in cybersecurity are crucial in addressing the dynamic challenges faced by organisations across different sectors. As supported by literature (Malatras & Dede, 2020; Pupillo et al., 2021) and practical insights from cybersecurity experts and industry professionals (P1, P4, P5), the strategic application of AI is fundamental in ensuring strong cybersecurity defences, designed to specific organisational needs. This multifaceted approach not only advances technological capabilities but also ensures that data, as a crucial asset, is effectively protected throughout its lifecycle.

5.2.3. Ethical Regulation as a Strategic Advantage in the European Union

In our exploration of the global dynamics of technological innovation, an observation from P5 captures the essence of regional roles: "America innovates, China replicates, and Europe regulates." This statement highlights Europe's distinctive approach to the growing field of AI ;an approach characterised by strict regulatory measures. In agreement with this is P6 and P7, emphasising Europe's proactive stance on AI regulation, particularly through the AIA, categorising AI systems based on risk levels; from low risk, to no risk, to unacceptable risk. This regulatory framework restricts the use of systems considered to have a high risk, effectively shaping the landscape in which AI development occurs within Europe. However, by emphasising compliance with stricter standards and regulatory approach and more stringent development constraints, the EU creates a niche market for European AI products and cutting-edge technologies known for their safety, ethical and technically robust standards (Sharkov et al., 2021). As per Bal and Gill (2020) European policies are increasingly focusing on ethical issues, privacy concerns, and the societal impacts of new technologies, more so than in China or the US. This approach to regulation provides the EU with a strategic advantage in crisis situations where public trust in government becomes crucial. In this way, regulation, while initially seeming like a barrier to innovation, may actually foster a more sustainable and ethical approach to technological development.

5.3 European Union Cybersecurity Frameworks and Landscape

This research explores key insights gleaned from individuals within ENISA and industry roles, shedding light on the complexities of integrating AI with existing cybersecurity frameworks. The results from the study both affirmed the pivotal role of standards organisations like ENISA and NIST in shaping cybersecurity practices and raised questions regarding the presumed ease of compliance with cybersecurity frameworks. This came up in the interviews with both ENISA and FMV participants. This section discusses how the findings align with existing literature and offers recommendations based on these insights.

The data from the interviews, particularly P1, P3, P6 and P7, support the literature (Proença and Borbinha, 2018; McCarthy and Harnett, 2014), stating the importance of organisations who provide guidance related to cybersecurity practices. It emphasises the pivotal role played by ENISA in providing guidance and recommendations for cybersecurity. ENISA's influence in shaping industry compliance highlights the crucial function of such organisations in establishing best practices. Additionally, the findings in feedback with conversation with industry professionals P4 and P5 confirmed the challenges associated with compliance in complex regulatory environments, echoing existing literature that emphasise the difficulties organisations face in navigating legal frameworks and standards.

However, the research also challenges certain assumptions regarding the effectiveness of ENISA guidelines in addressing the complexities of legal requirements. While ENISA guidelines are valued for providing a framework for compliance, the data from the ENISA interviewees suggest that they do not fully encompass the intricacies of legal obligations in

regards to AI integration. This challenges the assumption that strictly following industry standards is sufficient for ensuring comprehensive cybersecurity compliance.

In light of these insights, several recommendations can be made. Firstly, it is imperative for ENISA and similar organisations to enhance the clarity and specificity of their guidelines. Clearer guidelines can better assist organisations in navigating legal frameworks, mitigating the challenges associated with compliance. Secondly, efforts should be made to streamline governance processes involved in implementing legal requirements. Simplifying bureaucratic procedures can facilitate timely compliance and enhance cybersecurity resilience. Lastly, given the increasing importance of AI in cybersecurity, organisations should invest in understanding and integrating AI technologies effectively. This includes developing AI capabilities and leveraging specific datasets to improve cybersecurity practices.

In the ever-evolving landscape of cybersecurity, the integration of AI presents both opportunities and challenges for organisations seeking to bolster their defenses against cyberthreats.

ENISA, plays a pivotal role in shaping cybersecurity practices and providing guidance for information security policy development. The perspectives of individuals within ENISA reveal a concerted effort to understand and define the role of AI in cybersecurity. Despite lacking regulatory power, ENISA's guidelines are highly regarded within the industry, serving as valuable recommendations for achieving compliance with legal frameworks. However, the data also suggest that while ENISA guidelines offer a framework for compliance, they may not fully address the intricacies of legal requirements.

Industry professionals, on the other hand, provide valuable insights into the practical challenges of compliance with legal frameworks and standards. The data highlight the complexities faced by organisations, particularly in value-chain industries like IoT, where navigating legal requirements can be daunting. Compliance with ENISA standards is seen as providing a useful framework for meeting legal obligations effectively. However, the loose nature of some legal requirements presents challenges, necessitating clearer and more specific guidelines to facilitate compliance.

Lengthy bureaucratic procedures can hinder timely compliance and impede efforts to enhance cybersecurity resilience. Efforts to simplify governance processes are crucial for ensuring organisations can adapt quickly to emerging cyberthreats. Moreover, the integration of AI in cybersecurity is recognised as a significant area of focus for both ENISA and industry professionals. While ENISA aims to scale up AI capabilities and improve the European market, industry professionals emphasise the need for investment in understanding and leveraging AI technologies effectively. Clearer guidelines and frameworks for AI integration are essential for maximising its potential in enhancing cybersecurity practices.

While the findings largely align with existing theories regarding the role of standards organisations and the challenges of compliance, they also highlight areas where current approaches may fall short. By addressing these challenges and implementing the

recommended strategies, organisations can better navigate the intersection of AI and cybersecurity, enhancing their overall resilience to cyberthreats. In conclusion, the insights gathered from ENISA and industry perspectives emphasise the importance of clear guidelines, streamlined governance processes, and strategic investment in AI integration for effective cybersecurity. By addressing these challenges and implementing recommended strategies, organisations can navigate the complex intersection of AI and cybersecurity with greater resilience and confidence.

5.4 Implications of the Study

The study shows that teamwork between people and AI is crucial for cybersecurity. Even as AI helps with tasks, human oversight remains vital for quality control. The research also highlights a shortage of skilled workers in cybersecurity, especially in understanding AI. It suggests that training programs should focus more on AI to bridge this gap and that EU policies support the use of AI in cybersecurity but need to adapt to new challenges.

The research uncovers challenges in integrating AI into existing cybersecurity frameworks. Governance processes take time, and there's a need for collaboration between industry and policymakers. ENISA plays a role in developing guidelines, but compliance is not mandatory. Legal frameworks are still evolving, and there's uncertainty about AI certification.

The study also sheds light on the cybersecurity landscape. Public sectors are particularly vulnerable to cyberattacks, but AI affects all sectors. Geopolitical challenges exist, and Europe is adapting by considering open-source projects and policy adjustments. At the same time, ENISA plays a crucial role in working to define its role in AI and cybersecurity. They aim to improve European markets by promoting credible AI models and fostering collaboration between stakeholders. Certification for AI might become a reality in the future, reflecting ongoing efforts to enhance cybersecurity practices. Overall, the study suggests that both people and AI need to work together better to keep our digital world safe.

6. Conclusion

This thesis has explored how the dynamics of human-AI collaboration, and the impact of current EU cybersecurity policies and frameworks influence the effectiveness of cybersecurity measures and contribute to the overall security posture of the EU.

One of the fundamental findings of this study is the complementary relationship between human expertise and AI. The reviewed literature and the interviewees agree that AI should not be viewed as a replacement for human roles but as a powerful enhancive tool that improves human decision-making capabilities within cybersecurity operations. This collaboration ensures that while AI technologies can handle huge amounts of data and perform routine tasks with speed, human professionals maintain control over strategic decision-making. This balance is central not only for optimising security responses but also for ensuring that operations remain adaptable and ethically grounded.

Nevertheless, the integration of AI in cybersecurity is not without its complications. As explored in this study, the current regulatory and guideline frameworks within the EU do not always align perfectly with the fast pace of technological advancement. The findings indicate that while guidelines from bodies like ENISA provide a framework for compliance, they sometimes fall short in fully capturing the legal and practical intricacies of AI integration. This misalignment suggests a need for continuous evolution of policies and guidelines that can keep pace with technological innovations and the shifting landscape of cyberthreats.

Furthermore, the findings within this thesis have highlighted a gap in the current cybersecurity workforce's capabilities to effectively integrate and utilise AI technologies. The demand for professionals who are technically proficient in cybersecurity practices and also skilled in AI is growing. This study argues for improved educational and training programs that can prepare the next generation of cybersecurity professionals to navigate this increasingly complex and fast evolving field. By investing in education, training, and collaborative initiatives, stakeholders can cultivate a skilled workforce capable of navigating the complex intersection of AI and cybersecurity, thereby enhancing resilience against evolving cyberthreats.

Finally, the integration of AI into cybersecurity frameworks within the EU presents a transformative potential to strengthen defences against a constantly changing and evolving array of cyberthreats. However, realising this potential fully requires a collaborative and rigorous effort to maintain the balance between innovation and control, automation and oversight. As AI technologies continue to develop, it will be necessary for policy makers, industry leaders, and academic institutions to collaborate closely to ensure that cybersecurity practices are robust, resilient, and responsive to the needs of this and the future digital society. Accepting these challenges and opportunities with a progressive and adaptable approach will be essential to safeguarding the digital frontiers of the future.

6.1 Areas for Further Research

Future research should prioritise various key areas to advance understanding and effectiveness in this field. Firstly, research should explore how educational programs can adapt to include cybersecurity related and AI-focused curricula. Another critical area is the evaluation of AI's role in threat detection and response, assessing how AI technologies can improve operational efficiency and effectiveness. Furthermore, comparative studies of world-wide AI cybersecurity policies could provide insights into diverse regulatory approaches, informing more effective policies. Finally, longer-in-time studies are needed to assess the long-term impacts of AI integration on cybersecurity effectiveness, providing a comprehensive view of AI’s evolving role in this field. Addressing these research areas will develop our understanding and implementation of technology within broader security frameworks.

7. AI Contribution Statement

Writer 1

In the composition of this Master's Thesis, we utilised AI-based tools for the purposes of refining the content language and conceptual ideas originally generated by us. This collaborative effort ensured that the final submission was articulated as clearly and effectively as possible.

Tools: The AI tool employed was OpenAI's ChatGPT 4.

Degree of Use: ChatGPT's role was confined to text optimisation and concept idea formulation. It assisted in editing drafts by enhancing sentence structure, clarity, and the overall narrative quality of our work. The AI did not contribute to analysis, or code; these were exclusively the product of our collective human effort. ChatGPT acted as a sophisticated writing aid, streamlining our explanations and descriptions without infringing upon the content's originality, which remains our intellectual contribution.

Writer 2

For this thesis, ChatGPT was utilised by providing knowledge on various terms related to the assignment and defining any unknown terms that were found in the literature. It has also helped with the flow of information; being logical and clear. However, the critical analysis, in-depth research, and final structure of the assignment were entirely my own work. ChatGPT's contribution was supplementary, operating as a tool to enhance efficiency and not acting as a primary source of content.

The final submission is a product of my research and understanding, with AI serving only as a supportive tool in the background. The core arguments, specific analysis, and conclusions are drawn by my own effort, ensuring that the majority of the submission reflects my personal contribution. To conclude, ChatGPT was used for defining terms and suggesting synonyms and phrases that might better express my message and providing a basic structure for content. The tool did not contribute to the final writing, in-depth research, or critical analysis. These were carried out independently.

Appendix 1 - ENISA Interview Request Email

Dear ENISA Team,

I hope this message finds you well.

My name is Christos Kyprianou, and I am a Master's student at Lund University, Sweden, specialising in Information Systems. Together with my colleague Mumbi Mwelwa, we are conducting a Master thesis titled "Addressing Cyberthreats: Exploring the Intersection of AI and Cybersecurity Frameworks in the EU".

Our research focuses on exploring the evolving landscape of cybersecurity threats and the role of artificial intelligence in mitigating these risks within the European context. As part of our thesis, we are seeking insights from leading experts in the field, and ENISA's work in cybersecurity is of significant relevance and importance to our study.

We would be immensely grateful if you could spare some time for a short discussion with us. If we get financially supported by our University we could then travel in March/April and meet you in person for academic purposes. Your expertise and perspectives would be invaluable in enriching our research and understanding of the subject.

We assure you that any information provided will be used solely for academic purposes and with the utmost confidentiality. We are flexible with the timing and format of the interview to suit your convenience.

Thank you for considering our request. We look forward to the possibility of engaging with you and learning from your experiences.

Warm Regards,

Christos Kyprianou and Mumbi E. Mwelwa

MSc Information Systems Students

Lund School of Economics and Management (Department of Informatics)

Appendix 2 - Informed Consent Form

Lund University Master's Programme in Information Systems Master's Thesis

Addressing Cyberthreats: Exploring the Intersection of AI and Cybersecurity Frameworks in the EU

Thank you for participating in our Master's thesis, which explores the role of human expertise and with AI technologies in improving cybersecurity frameworks within the EU.

The purpose of this study examines the skills gap, the interplay between human expertise and AI technologies, and the regulatory framework impacting cybersecurity practices. This investigation is driven by the need to understand how these factors collectively influence the effectiveness of cybersecurity measures across the EU.

The interview data will be analysed by the students mentioned below, supervised by the supervisor mentioned below, and the completed thesis will be assessed and graded by an examiner at the end of the course.

We ask for your approval to interview you and use the data for the Master's thesis. Participation in this study is voluntary and you have the option to withdraw from participation at any time without motivating why.

If you agree, the interview will be recorded and subsequently transcribed. All collected data will be protected, securely stored, and will not be disclosed to unauthorised individuals. The transcribed text will be further coded and analysed, and the findings will be presented in an anonymous manner. You may request the transcript to be sent to you until the end of the research.

The results of the study will be presented in the thesis in a manner that protects the confidentiality of participants. Our research adheres to established guidelines on research ethics and applicable laws. Please contact us if you need any additional information.

Christos Kyprianou Email: christos.kyprianou.6218@student.lu.se

Mumbi Eugene Mwelwa Email: mu0243mw-s@student.lu.se

Supervisor: Osama Mansour Email: osama.mansour@ics.lu.se

If you agree to the information provided above, please sign this consent form.

Name: _____ Signature: _____

Date: _____

Appendix 3 - Interview Guide / Questions

Interview Guide for ENISA Experts

Theme	Questions
Enhancing Cybersecurity with Human-AI Collaboration	• What models of human-AI collaboration in threat detection does ENISA advocate for or see as most effective? • Can you elaborate on the synergy between human intelligence and AI in enhancing cybersecurity threat detection?
AI-Technologies in Cybersecurity	• What AI technologies do you find most effective in enhancing threat detection capabilities within cybersecurity frameworks? • ·Are there specific technologies or innovations that you think are vital for improving cybersecurity in the current environment?
AI Integration into Cybersecurity Frameworks	• Can you describe ENISA's current stance or initiatives regarding the integration of AI technologies into cybersecurity frameworks within the EU? • What are the key challenges you've observed in integrating AI into existing cybersecurity frameworks? • How should cybersecurity policies evolve to support the effective integration of AI technologies, particularly for threat detection? • How have recent EU policies influenced the deployment and development of AI technologies in cybersecurity?
Future Work	• What future trends or developments do you foresee in the use of AI for cybersecurity threat detection within the EU?

Interview Guide for Industry Experts

Theme	Questions
AI-Technologies in Cybersecurity	• How is your organisation prepared proactively against any cybersecurity scenarios? • What AI technologies are used in order to combat cyberthreats? • How does your company manage and protect the vast amounts of data generated from its AI-driven processes?
EU Cybersecurity Frameworks	• Could you clarify the role of ENISA in relation to your company? Does ENISA provide regulatory guidelines or other forms of support to your company? • Could you share any best practices from the industry that are particularly important to consider due to the high level of regulation, especially when implementing recommendations?
Future Work	• Based on your experience, what are the emerging trends in AI that could impact cybersecurity in industrial sectors?

Interview Guide for FMV Experts

Theme	Questions
Enhancing Cybersecurity with Human-AI Collaboration	• How can educational institutions and private organisations collaborate to ensure that the workforce is well-equipped to handle emerging AI technologies? • Can you suggest a few ways that human and AI tools can be integrated to detect cyberthreats?
Skills Gap	• How does the current level of cybersecurity expertise in the EU meet the demands posed by the cyber threat landscape? • In light of the skills gap mentioned in the results, what specific skills should cybersecurity training programs focus on to better prepare professionals for AI integration?
AI-Technologies in Cybersecurity	• How would you recommend AI technologies be used in detecting cyberthreats? Any concerns/challenges? • Are there specific technologies or innovations that you think are vital for improving cybersecurity in the current environment?
EU Cybersecurity Frameworks	• How far is Europe in implementing cybersecurity policies to implement AI aspects? • How do you see the integration of advanced AI technologies like machine learning and deep learning evolving in the next five years within EU cybersecurity strategies?

References

Aldawood, H. & Skinner, G. (2020). Analysis and Findings of Social Engineering Industry Experts Explorative Interviews: Perspectives on Measures, Tools, and Solutions, *IEEE Access*, vol. 8, pp.67321–67329. doi:10.1109/ACCESS.2020.2983280.

Alharahsheh, H. H. & Pius, A. (2020). A Review of Key Paradigms: Positivism VS Interpretivism, *Global Academic Journal of Humanities and Social Sciences*, vol. 2, no. 3, pp.39–43. doi: 10.36348/gajhss.2020.v02i03.001.

Alzboon, M.S. *et al.* (2023) 'The Two Sides of AI in Cybersecurity: Opportunities and Challenges', *2023 International Conference on Intelligent Computing and Next Generation Networks (ICNGN), Intelligent Computing and Next Generation Networks（ICNGN), 2023 International Conference on*, pp. 1–9. doi:10.1109/ICNGN59831.2023.10396670.

Ansari, M. F., Dash, B., Sharma, P. & Yathiraju, N. (2022). The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review, *IJARCCE*, vol. 11, no. 9. Available online: https://ssrn.com/abstract=4323317.

Arpaci, I. & Aslan, O. (2023). Development of a Scale to Measure Cybercrime-Awareness on Social Media, *Journal of Computer Information Systems*, vol. 63, no. 3, pp.695–705. doi:10.1080/08874417.2022.2101160.

Baldini, Gianmarco. & European Commission. Joint Research Centre. (2020). Testing and Certification of Automated Vehicles (AV) Including Cybersecurity and Artificial Intelligence Aspects. *Publications Office of the European Union.* doi:10.2760/86907.

Bao, Y., Gong, W. & Yang, K. (2023). A Literature Review of Human–AI Synergy in Decision Making: From the Perspective of Affordance Actualization Theory, *Systems.* 11(9), p. 442. doi:10.3390/systems11090442.

Basholli, F., Mema, B. & Basholli, A. (2024). Training of Information Technology Personnel through Simulations for Protection against Cyber Attacks, *Engineering Applications*, 3(1), pp.45–58, Available Online: https://publish.mersin.edu.tr/index.php/enap.

Brinkmann, S. and Kvale, S. (2015) *InterViews : Learning the Craft of Qualitative Research Interviewing*. 3., [updated] ed. Sage Publications. Available at: https://search-ebscohost-com.ludwig.lub.lu.se/login.aspx?direct=true&AuthType=ip,uid&db=cat07147a&AN=lub.4315115&site=eds-live&scope=site [Accessed: 23 Feb 2024].

Button, M., Shepherd, D., Blackbourn, D., Sugiura, L., Kapend, R. & Wang, V. (2022). Assessing the Seriousness of Cybercrime: The Case of Computer Misuse Crime in the United Kingdom and the Victims' Perspective, *Criminology and Criminal Justice.* [Preprint]. doi:10.1177/17488958221128128.

Campina, A., Rodrigues, C. (2022) Cybercrime and the Council of Europe Budapest Convention: Prevention, Criminalization, and International Cooperation. The Book of Full Papers 7th International Zeugma Conference on Scientific Researches, http://hdl.handle.net/10284/10766 [Accessed 22 Mar 2024].

CapGemini Research Institute (2019) Adapted from "Reinventing Cybersecurity with Artificial Intelligence: The New Frontier in Digital Security", p.7. Retrieved from https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf.

Cheng, H. F., Wang, R., Zhang, Z., O'Connell, F., Gray, T., Harper, F. M. & Zhu, H. (2019). Explaining Decision-Making Algorithms through UI: Strategies to Help Non-Expert Stakeholders, in *Conference on Human Factors in Computing Systems - Proceedings*, 2 May 2019, Association for Computing Machinery. doi:10.1145/3290605.3300789.

Colaric, S. M. (n.d.). Instruction for Web Searching: An Empirical Study. *College and Research Libraries*, 64(2), pp. 111-122–122. doi:10.5860/crl.64.2.111.

Couchoro, M. K., Sodokin, K. & Koriko, M. (2021). Information and Communication Technologies, Artificial Intelligence, and the Fight against Money Laundering in Africa, *Strategic Change*, vol. 30, no. 3, pp.281–291. doi:10.1002/jsc.2410.

Creemers, R. (2022). China's Emerging Data Protection Framework, *Journal of Cybersecurity*, 8(1). [Preprint]. doi:10.1093/cybsec/tyac011.

Davidson, C. (2009). Transcription: Imperatives for Qualitative Research, *International Journal of Qualitative Methods*, 8(2), pp. 35–52. doi:10.1177/160940690900800206.

Dilek, S., Cakır, H. & Aydın, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review, *International Journal of Artificial Intelligence & Applications*, vol. 6, no. 1, pp.21–39. doi:10.5121/ijaia.2015.6102.

Djenna, A., Bouridane, A., Rubab, S. & Marou, I. M. (2023). Artificial Intelligence-Based Malware Detection, Analysis, and Mitigation, *Symmetry*, 15(3), p. 677. doi:10.3390/sym15030677.

Dwivedi, Y.K., Kshetri, N., Hughes, L., Slade, E.L., Jeyaraj, A., Kar, A.K., Baabdullah, A.M., Koohang, A., Raghavan, V., Ahuja, M. and Albanna, H., (2023). "So what if ChatGPT wrote it?" Multidisciplinary perspectives on opportunities, challenges and implications of generative conversational AI for research, practice and policy. *International Journal of Information Management*, 71, p.102642. doi.org/10.1016/j.ijinfomgt.2023.102642.

European Parliament. (2024). *European Parliamentary Research Service* (p. 7). Adapted from: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI%282021%29698792_EN.pdf.

EU Publications, (2017). Harnessing the Economic Benefits of Artificial Intelligence. Digital Transformation Monitor. [pdf] Available at: https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/DTM_Harnessing%20the%20economic%20benefits%20v3.pdf [Accessed 19 April 2024].

European Union Agency for Network and Information Security (ENISA), (2018). ENISA Threat Landscape Report 2018. [pdf] Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 [Accessed 19 March 2024].

European Union Agency for Network and Information Security (ENISA), (2022). Ad-Hoc Working Group Calls on IoT and Smart Infrastructures. [online] Available at: https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/artificial_intelligence/ad-hoc-working-group/adhoc_wg_calls [Accessed 29 April 2024].

European Union Agency for Network and Information Security (ENISA), (2022). ENISA Threat Landscape 2022. [pdf] Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 [Accessed 10 March 2024].

Falowo, O. I., Ozer, M., Li, C. & Abdo, J. B. (2024). Evolving Malware and DDoS Attacks: Decadal Longitudinal Study, *IEEE Access*, vol. 12, pp.39221–39237. doi:10.1109/ACCESS.2024.3376682.

Foddy, W.H. (1993) *Constructing questions for interviews and questionnaires. theory and practice in social research*. Cambridge University Press. Available at: https://search-ebscohost-com.ludwig.lub.lu.se/login.aspx?direct=true&AuthType=ip,uid&db=cat02271a&AN=atoz.ebs848201e&site=eds-live&scope=site. [Accessed 18 Jan 2024]

Frisk, I., Ruoslahti, H. and Tikanmäki, I., 2023. Cybersecurity Through Thesis in Laurea University of Applied Sciences. In Proceedings of the 22nd European Conference on Cyber Warfare and Security. *Academic Conferences International Ltd*. doi:10.34190/eccws.22.1.1447.

Garrido, S., Fano Yela, J., Panigutti, D., Junklewitz, C., Hamon, H., Evas, R., André, T. & Scalzo, A.-A. (n.d.). Analysis of the Preliminary AI Standardisation Work Plan in Support of the AI Act. doi:10.2760/5847.

Ghelani, D. (2023). Securing the Future: Exploring the Convergence of Cybersecurity, Artificial Intelligence, and Advanced Technology, *International Journal of Computer Trends and Technology*, vol. 71, no. 10, pp.39–44. doi.org/10.14445/22312803/IJCTT-V71I10P105. [Accessed 8 Jan 2024].

Hadzovic, S., Mrdovic, S. & Radonjic, M. (2023). A Path Towards an Internet of Things and Artificial Intelligence Regulatory Framework, *IEEE Communications Magazine*, vol. 61, no. 7, pp.90–96. doi**:** 10.1109/MCOM.002.2200373.

Huberman, a. M. & Miles, M. B. (2013). Qualitative Data Analysis, *Qualitative Data Analysis A Methods Sourcebook*, [e-journal] vol. 47, no. Suppl 4, pp.3–16, Available Online: http://www.uk.sagepub.com/books/Book239534?siteId=sage-uk [Accessed 18 May 2024].

ISACA, (2024). Track These 7 Trends for Proactive Cybersecurity in 2024. Available Online: https://www.isaca.org/resources/news-and-trends/industry-news/2023/track-these-7-trends-for-proactive-cybersecurity-in-2024 [Accessed 17 March 2024].

Jada, I. & Mayayise, T. O. (2024). The Impact of Artificial Intelligence on Organisational Cyber Security: An Outcome of a Systematic Literature Review, *Data and Information Management*, vol. 8, no. 2, p.100063 doi:10.1016/j.dim.2023.100063.

Järvelä, S., Nguyen, A. & Hadwin, A. (2023). Human and Artificial Intelligence Collaboration for Socially Shared Regulation in Learning, *British Journal of Educational Technology*, vol. 54, no. 5, pp.1057–1076. doi:10.1111/bjet.13325.

Kabanda, G. (2021). Anchoring AI/Machine Learning on the African Technological Innovation and Investment Table, in *ACM International Conference Proceeding Series*, 26 November 2021, Association for Computing Machinery, pp.18–37 [Accessed 8 Jan 2024].

Kalhoro, S., Rehman, M., Ponnusamy, V. & Shaikh, F. B. (2021). Extracting Key Factors of Cyber Hygiene Behaviour among Software Engineers: A Systematic Literature Review, *IEEE Access.* 9, pp. 99339–99363. doi:10.1109/ACCESS.2021.3097144.

Kaloudi, N. & Jingyue, L. I. (2020). The AI-Based Cyber Threat Landscape: A Survey, *ACM Computing Surveys.* doi:10.1145/3372823.

Khraisat, A. & Alazab, A. (2021). A Critical Review of Intrusion Detection Systems in the Internet of Things: Techniques, Deployment Strategy, Validation Strategy, Attacks, Public Datasets and Challenges, *Cybersecurity*, 4(1), pp. 1–27. doi:10.1186/s42400-021-00077-7.

Kioskli, K., Fotis, T., Nifakos, S. & Mouratidis, H. (2023). The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0, *Applied Sciences (Switzerland), 13(6). doi:10.3390/app13063410.*

Kotuk, Mahir. (2022). The book of Full Papers 7th International Zeugma Conference on Scientific Researches : January 21-23, 2022 Gaziantep, Turkey, IKSAD Publishing House. Available online:https://bdigital.ufp.pt/bitstream/10284/10766/1/Cybercrime%20and%20the%20Council%20of%20Europe%20Budapest%20Conventation%20112-123.pdf [Accessed 17 March 2024].

Lawrence, L. E. M., Echeverria, V., Yang, K., Aleven, V. & Rummel, N. (2024). How Teachers Conceptualise Shared Control with an AI Co-Orchestration Tool: A Multiyear Teacher-Centred Design Process, *British Journal of Educational Technology*, 55(3), pp.823–844. doi:10.1111/bjet.13372.

Lee, J. R. & Holt, T. J. (2020). Assessing the Factors Associated With the Detection of Juvenile Hacking Behaviors, *Frontiers in Psychology*, 11, doi:10.3389/fpsyg.2020.00840.

Luknar, I. & Jovanović, F. (2024). Various Types of Cyber Threats, *Srpska politička misao*, vol. 83, no. 1, pp.161–177. doi: 10.5937/spm83-46059.

Malatji, M., Von Solms, S. & Marnewick, A. (2019). Socio-Technical Systems Cybersecurity Framework, *Information and Computer Security*, 27(2) pp.233–272. doi:10.1108/ICS-03-2018-0031.

Mathew, A (2021) Artificial intelligence for offence and defense-the future of cybersecurity. *Educational Research*, *3*(3), pp.159-163. Available on: https://www.ijmcer.com/wp-content/uploads/2023/07/IJMCER_R0330159163.pdf [Accessed 17 March 2024].

Mijwil, M. M., Aljanabi, M. & ChatGPT. (2023). Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime, *Iraqi Journal for Computer Science and Mathematics*, vol. 4, no. 1, pp.65–70.

Mohammed, I. A. (2016). How Artificial Intelligence Is Changing Cyber Security Landscape and Preventing Cyber Attacks: A Systematic Review, Vol. 4, Available Online: www.ijcrt.org.

Mtair AL-Hawamleh, A. (n.d.). Predictions of Cybersecurity Experts on Future Cyber-Attacks and Related Cybersecurity Measures, *IJACSA) International Journal of Advanced Computer Science and Applications*, 14(2), Available Online: https://www.researchgate.net/profile/Ahmad-Al-Hawamleh/publication/370401571_Predictions_of_Cybersecurity_Experts_on_Future_Cyber-Attacks_and_Related_Cybersecurity_Measures/links/644dc9f5809a5350213a1cd0/Predictions-of-Cybersecurity-Experts-on-Future-Cyber-Attacks-and-Related-Cybersecurity-Measures.pdf [Accessed 3 Jan 2024].

Myers, M.D. (2009) *Qualitative Research in Business & Management*. SAGE. Available at:https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=cat07147a&AN=lub.1893236&site=eds-live&scope=site[Accessed: 19 March 2024].

Nadella, G.S., Gonaygunta, H., & Meduri, K. (2024) Enhancing Cybersecurity with Artificial Intelligence: Predictive Techniques and Challenges in the Age of IoT. *International Journal of Science and Engineering Applications*. 13(4) pp. 30-33, doi:10.7753/IJSEA1304.1007.

National Institute of Standards and Technology (NIST) Cybersecurity Risk Management Framework Applied to Modern Vehicles. (2014). Available Online: www.ntis.gov [Accessed: 19 March 2024].

Patel, H. (2023). The Future of Cybersecurity with Artificial Intelligence (AI) and Machine Learning (ML), [e-journal], Available Online: www.preprints.org.

Petrović, D. & Jovanović, M. (2024). Synergistic Potential of Supercomputing and AI in Shaping Secure Digital Environments, *Journal of Computational Social Dynamics Research Article: Quarterly Journal of Emerging Technologies and Innovations.* Available online: *https://vectoral.org/index.php/QJETI/article/view/69.*

Policy Approaches to Artificial Intelligence Based Technologies in China, European Union and the United States Ravtosh Bal and Indermit Gill. (n.d.).

Prasad, R. & Rohokale, V. (n.d.). Springer Series in Wireless Technology, Available Online: http://www.springer.com/series/14020.

Proença, D. & Borbinha, J. (n.d.). Information Security Management Systems-A Maturity Model Based on ISO/IEC 27001.

Pupillo, L., Fantin, S., Ferreira, A. 1960-, Polito, C. & Centre for European Policy Studies. (n.d.). Artificial Intelligence and Cybersecurity Technology, Governance and Policy Challenges : Final Report of a CEPS Task Force.

Ricci, S., Parker, S., Jerabek, J., Danidou, Y., Chatzopoulou, A., Badonnel, R., Lendak, I. & Janout, V. (2024). Understanding Cybersecurity Education Gaps in Europe, *IEEE Transactions on Education.*

Saunders, M., Lewis, P. & Thornhill, A. (n.d.). Research Methods for Business Students Fifth Edition.

Schmidt, E., Work, R.O., Bajraktari, Y., Catz, S., Horvitz, E.J., Chien, S., Jassy, A., Clyburn, M.L., Louie, G., Darby, C. and Mark, W., (2021). National Security Commission on Artificial Intelligence. Available online: https://reports.nscai.gov/final-report.

Schmittner, C. & Shaaban, A. M. (2023). OVERVIEW OF AI STANDARDIZATION, in *IDIMT 2023: New Challenges for ICT and Management - 31st Interdisciplinary Information Management Talks*, 2023, Trauner Verlag Universitat, pp.143–149.

Sharkov, G., Todorova, C. & Varbanov, P. (2021). Strategies, Policies, and Standards in the EU Towards a Roadmap for Robust and Trustworthy AI Certification, *Information & Security: An International Journal*, vol. 50, pp.11–22.

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I.A. & Xu, M., (2020) A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," in *IEEE Access*, vol. 8, pp. 222310-222354, doi: 10.1109/ACCESS.2020.3041951.

Shoemaker, D. and Conklin, W.A., (2011). *Cybersecurity: The Essential Body of Knowledge*. Delmar Learning.

Sinclair, B. J. (2023). Letting ChatGPT Do Your Science Is Fraudulent (and a Bad Idea), but AI-Generated Text Can Enhance Inclusiveness in Publishing, *Current Research in Insect Science.*

Singh, S., Singh, A. & Goyal, V. (2024). An Analytical View of DoS or DDoS Attacks for Network Architecture, pp.1–27.

Station X (2024) Adapted from “Cyber Security Breach Statistics 2024”, p.1. Retrieved from https://www.stationx.net/cyber-security-breach-statistics/.

Stevens, T. (2020). Knowledge in the Grey Zone: AI and Cybersecurity, *Digital War*, vol. 1, no. 1–3, pp.164–170. doi: 10.1057/s42984-020-00007-w.

Tao, F., Akhtar, M. & Jiayuan, Z. (2021). The Future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey, *EAI Endorsed Transactions on Creative Technologies*, vol. 8, no. 28, p.170285. doi: 10.4108/eai.7-7-2021.170285.

Terry, G., Hayfield, N., Clarke, V. & Braun, V. (n.d.). [Citations: Alpha Order] [Spelling UK Ize] [Recto Running Head: Thematic Analysis] 2 Thematic Analysis.

Thakur, M. (2024). Cyber Security Threats and Counter Measures in Digital Age, *Journal of Applied Science and Education (JASE)*, [e-journal] vol. 04, no. 042, pp.1–20, Available Online: https://doi.org/10.54060/a2zjournals.jase.42http://creativecommons.org/licenses/by/4.0/

Thi Minh Huyen, N. & Quoc Bao, T. (2024). Advancements in AI-Driven Cybersecurity and Comprehensive Threat Detection and Response, *Journal of Intelligent Connectivity and Emerging Technologies*, 9(1), pp.1-12.

Trappe, W. & Straub, J. (2021). Journal of Cybersecurity and Privacy: A New Open Access Journal, *Journal of Cybersecurity and Privacy.* 1(1), pp. 1-3–3. doi: 10.3390/jcp1010001.

Truong, T. C., Diep, Q. B. & Zelinka, I. (2020). Artificial Intelligence in the Cyber Domain: Offense and Defense, *Symmetry*, 12(3). doi: 10.3390/sym12030410.

Vadiyala, V.R., (2019). Innovative Frameworks for Next-Generation Cybersecurity: Enhancing Digital Protection Strategies. *Technology & Management Review*, *4*, pp.8-22. Available online: https://www.researchgate.net/profile/Vishal-Reddy-Vadiyala/publication/378309875_Innovative_Frameworks_for_Next-Generation_Cybersecurity_Enhancing_Digital_Protection_Strategies/links/65d39a8101325d465211d4f2/Innovative-Frameworks-for-Next-Generation-Cybersecurity-Enhancing-Digital-Protection-Strategies.pdf.

Van De Ven, A. H. & Johnson, P. E. (2006). Knowledge for Theory and Practice, *Source: The Academy of Management Review*, 31, Available Online: https://www.jstor.org/stable/20159252.

Wilson, C. (2013.). Interview Techniques for UX Practitioners: A User-Centered Design Method. Morgan Kaufmann. Available at: https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,uid&db=cat07147a&AN=lub.6551073&site=eds-live&scope=site [Available Online: 9 Jan 2024].

Xu, S., Xia, Y. & Shen, H. L. (2020). Analysis of Malware-Induced Cyber Attacks in Cyber-Physical Power Systems, *IEEE Transactions on Circuits and Systems II: Express Briefs*, 67(12), pp.3482–3486. doi: 10.1109/TCSII.2020.2999875.

Zeadally, S., Adi, E., Baig, Z., & Khan, I., (2020). Harnessing Artificial Intelligence Capabilities to Improve Cybersecurity. IEEE Access, 8, pp. 23817-23837. doi.org/10.1109/ACCESS.2020.2968045.