Beyond Reacting: Integrating Strategic Foresight for Proactive Cybersecurity in Critical Infrastructure

Delal Karabulut

Dissertation written under the supervision of Professor Duarte Cardoso Ferreira

Dissertation submitted in partial fulfilment of requirements for the MSc in Management with Specialization in Strategy, Entrepreneurship & Impact, at the Universidade Católica Portuguesa, 05. January 2025.

Abstract

Title: Beyond Reacting: Integrating Strategic Foresight for Proactive Cybersecurity in Critical Infrastructure

Author: Delal Karabulut

This thesis investigates how strategic foresight can strengthen cybersecurity practices in critical infrastructure sectors against AI-driven threats. While existing research has explored cybersecurity in critical infrastructure, there remains limited understanding of how strategic foresight can be effectively implemented to counter emerging AI-driven threats. Through qualitative research methods, the study combines a comprehensive literature review with semi-structured interviews featuring cybersecurity experts from diverse industries to examine vulnerabilities and evaluate proactive security strategies.

The research reveals three key findings: First, Collective Intelligence systems prove essential for enhancing information sharing and threat detection across organizations. Second, Autonomous AI technologies emerge as crucial tools for adapting to and mitigating emerging cybersecurity challenges. Third, IT consulting firms play a vital role in facilitating the transition toward foresight-based security measures.

The study encountered several limitations, including restricted access to current and comprehensive literature and the rapidly evolving nature of AI and cybersecurity technologies, which may impact the longevity of the presented insights. Furthermore, selecting interview participants who could represent the full spectrum of sector stakeholders proved challenging.

This research makes significant contributions to cybersecurity, strategic planning, and IT consulting fields by providing actionable insights for strengthening critical infrastructure resilience. The findings establish a foundation for future research and practical applications, emphasizing the necessity for security practices to continuously evolve alongside rapid technological advancement.

Keywords: Strategic Foresight, Cybersecurity, Critical Infrastructure (CI), Artificial Intelligence (AI), IT Consulting

Resumo

Título: Além da Reação: Integrando Antecipação Estratégica para uma Cibersegurança Proativa em Infraestruturas Críticas

Autor: Delal Karabulut

Esta tese investiga como a antecipação estratégica pode fortalecer as práticas de cibersegurança em setores de infraestrutura crítica contra ameaças impulsionadas por inteligência artificial (IA). Embora pesquisas anteriores tenham explorado a cibersegurança em infraestrutura crítica, ainda há uma compreensão limitada sobre como implementar a antecipação estratégica de forma eficaz para combater ameaças emergentes de IA. O estudo utiliza métodos qualitativos, combinando uma revisão abrangente da literatura com entrevistas semiestruturadas realizadas com especialistas em cibersegurança de diversas indústrias para analisar vulnerabilidades e estratégias proativas.

A pesquisa apresenta três descobertas principais: Primeiro, sistemas de inteligência coletiva são essenciais para melhorar o compartilhamento de informações e a detecção de ameaças entre organizações. Segundo, tecnologias de IA autônoma emergem como ferramentas cruciais para enfrentar desafios emergentes. Terceiro, empresas de consultoria em TI desempenham um papel vital na transição para medidas de segurança baseadas em antecipação.

As limitações incluem acesso restrito à literatura atualizada e a rápida evolução das tecnologias de IA e cibersegurança, o que pode afetar a validade dos insights apresentados. Além disso, selecionar participantes que representassem todo o espectro de partes interessadas foi desafiador.

Esta pesquisa contribui para a cibersegurança, planejamento estratégico e consultoria em TI, oferecendo insights para fortalecer a resiliência de infraestruturas críticas e fundamentar futuras pesquisas e aplicações práticas.

Palavras-chave: Antecipação Estratégica, Cibersegurança, Infraestrutura Crítica (IC), Inteligência Artificial (IA), Consultoria em TI

Table of Contents

List of Figures

List of Tables

1.0 Introduction

Nowadays, in the evolving landscape of global cybersecurity threats, critical infrastructure sectors are increasingly targeted by sophisticated AI-driven attacks. These sectors are particularly vulnerable due to their interdependencies, where successful attacks on their IT security can trigger cascading effects with serious impacts (De Felice et al., 2022). Furthermore, these sectors face increased challenges due to outdated security systems and limited capabilities in proactive cybersecurity, making them susceptible to exploitation (Ige et al., 2024). As our digital world and cyber threats continuously evolve, the adoption of strategic foresight in security systems becomes essential for anticipating and mitigating potential attacks, necessitating a shift from traditional reactive security measures to proactive strategies.

Recent research underlines the critical role of strategic foresight in shaping cybersecurity strategies within critical infrastructure sectors. Unlike traditional methods, foresight-based strategies enable effective responses to dynamically evolving threats and are increasingly recognized as vital for critical infrastructure, where cyberattacks can cause wide-ranging systemic disruptions (Kuraku et al., 2023). Experts increasingly emphasize that strategic foresight integration is crucial for better threat prediction and improved resilience.

The integration of strategic foresight in cybersecurity extends beyond technological upgrades, requiring significant shifts in organizational culture and processes. Therefore, to implement modern, foresight-based solutions effectively, a comprehensive approach that includes all cybersecurity stakeholders is essential, allowing the identification of strengths and synergies across multiple industries, firms, and individuals (Kuraku et al., 2023; BCG, 2024).

While AI advancement benefits potential attackers, it also presents opportunities for the defender side when implemented responsibly. AI-driven defense mechanisms are becoming crucial, particularly as attacks on critical infrastructure continue to escalate. According to Check Point (2024), from January to August 2024, the utilities sector, which encompasses critical infrastructure, ranked as the fifth most targeted by cyberattacks, with organizations experiencing an average of 1,514 attacks per week—a 37% increase from the previous year.

This thesis aims to provide a comprehensive understanding of the relationship between security system vulnerabilities in critical infrastructure and approaches for proactive solutions. The analysis offers recommendations for implementing foresight-based solutions to better anticipate

and prepare for rapidly evolving AI-driven threats, while addressing implementation barriers. To achieve this, the thesis addresses the following research question:

> To what extent does integrating strategic foresight enhance current cybersecurity measures in critical infrastructure sectors to prepare for and anticipate rapidly evolving AI-driven threats, and what role do IT consulting firms play in this transformation?

The thesis is structured as follows: After the introduction, a comprehensive literature review examines cybersecurity measures, gaps, and vulnerabilities within critical infrastructure, particularly in the context of rising AI-driven threats. The review then investigates how strategic foresight can be integrated into existing cybersecurity frameworks to approach the development of proactive solutions, including an analysis of AI's potential to strengthen cybersecurity measures. The literature review concludes by examining the role of IT consulting firms in the transition from reactive to proactive cybersecurity approaches. Following this, the methodology section outlines the research approach, leading to a presentation of the qualitative findings. The thesis then discusses these results and their implications for the field. Finally, after the conclusion, it addresses the study's limitations and provides directions for future research.

2.0 Literature Review

2.1 Critical Infrastructure Sectors

Critical infrastructure protection has become increasingly vital in our interconnected digital world. This section examines the fundamental sectors of critical infrastructure, their inherent vulnerabilities, and the emerging role of artificial intelligence (AI) in both threatening and safeguarding these essential systems. By exploring these aspects, we gain crucial insights into the challenges and complexities of protecting the infrastructure that underpins our society.

Critical infrastructure (CI) refers to the essential systems and assets vital to national security, economic stability, public safety, and health. These sectors which include energy, water, transportation, telecommunications, healthcare and financial services are forming the backbone of our modern society. The importance of these sectors lies not just in individual functionality, but also in their complex interdependencies. For example, telecommunications enable real-time

monitoring of energy grids, while healthcare facilities depend on consistent power supplies, which creates a fragile ecosystem of interconnected services (De Felice et al., 2022).

As digital technologies like the Internet of Things (IoT) and cloud computing transform these sectors, they enhance efficiency and simultaneously introduce new vulnerabilities. Each sector faces unique cybersecurity challenges. The energy sector is especially exposed by its aging infrastructure, which was originally designed without modern cybersecurity considerations and therefore, lacking capabilities to adapt to AI-driven cyber attacks. Similarly, the system within the telecommunication sector remains vulnerable to both external cyberattacks and internal system failures. Taking into account their critical nature, protecting these infrastructures has become a national priority (De Felice et al., 2022; Ige et al., 2024)

Furthermore, the previously mentioned sectors are considered "lifeline sectors" due to their fundamental role in supporting broader societal functions. Any disruption in one of them can trigger cascading effects and potentially causes widespread damage. This interconnectedness simultaneously increases their operational complexity and makes them main targets for sophisticated cyberattacks aimed at national security disruption (De Felice et al., 2022).

2.1.1 Vulnerabilities in Critical Infrastructure

The growing dependence on digital technology and services in critical infrastructure reveals serious cybersecurity vulnerabilities. While many critical infrastructure systems focus and even prioritize reliability and continuous service, they often fall short in defending against more advanced attacks (Riggs et al., 2024). A major vulnerability lies in their dependence on outdated technologies that are not suited to handle modern AI-driven cyber threats. For example, Supervisory Control and Data Acquisition (SCADA) systems used in the energy and water sectors have significant security gaps due to their outdated communication protocols (George, Baskar, & Srikaanth, 2024).

Furthermore, the potential attack surface of our CI is significantly increased by the growing use of IoT devices in AI. As these devices are poorly secured in most cases, they offer attackers simplified entry points and opportunities to infiltrate larger networks and cause damage. This is because, once the attackers have penetrated, they can move laterally and disrupt operations or gain access to sensitive data (Riggs et al., 2024). A notable example to illustrate this risk is again the healthcare sector, which is currently experiencing a huge increase in ransomware

attacks. These attacks specifically target vulnerable and poorly protected medical devices and systems. It is important to note that such attacks not only compromise patient privacy, but also pose a significant threat to lives by disrupting important medical procedures (Canorea, 2024).

The statistics speak for themselves: yet in 2022, healthcare facilities were exposed to an average of 1,463 attacks per week - an increase of 74% on the previous year - underlining the urgent need for improved cybersecurity defences (Canorea, 2024).

Additionally, the physical distribution of CI assets further complicates security efforts. Critical facilities like energy plants and water treatment centers are often located in remote or dispersed locations, making continuous monitoring challenging. This limited visibility creates opportunities for attackers to exploit vulnerabilities undetected. For example, the Colonial Pipeline attack, where cybercriminals exploited weaknesses in the energy sector and disrupted fuel supplies across the U.S, is demonstrating how sophisticated attackers can leverage such vulnerabilities in the system to disrupt vital services (Riggs et al., 2024).

Finally, human error still remains a significant vulnerability in CI cybersecurity. Attacks frequently arise from preventable issues like phishing, weak passwords or insufficient cybersecurity training. These seemingly minor mistakes can have enourmous consequences when they provide access to systems which are controlling critical infrastructure operations (Stewart, 2024).

2.1.2 Role of AI in Exploiting these Vulnerabilities

The rise of artificial intelligence has changed how cyber attacks are conducted against critical infrastructure. This section explores how AI-powered attacks work, examines real cases where they have caused significant damage, and looks at the growing risks as AI technology continues to advance at a rapid pace.

Artificial intelligence plays a double role in the realm of cybersecurity, acting both as a protective tool and as a way for attackers to launch more advanced attacks. Those AI-driven cyber threats present significant dangers to critical infrastructure, as they can rapidly learn, adapt, and exploit system vulnerabilities with little human oversight (Minhaj, 2023). One of the main advantages is the ability to automate and scale attacks, allowing for the simultaneous targeting of multiple interconnected systems. This is especially relevant for sectors like

telecommunications and energy, where interconnected systems give attackers more chances to infiltrate and cause disruption (Stewart, 2024)

Next to that, machine learning algorithms provide attackers with serious tools to quickly and precisely identify system vulnerabilities. By analyzing extensive datasets, these algorithms can detect subtle patterns that traditional techniques may overlook and with that revealing potential points of exploitation. Some AI-enhanced malware can even evolve in real-time, adapting to its surroundings to bypass current cybersecurity measures (Minhaj, 2023).

Furthermore, recent events have highlighted the impacts of AI attacks on critical infrastructure. For example, AI-driven Distributed Denial of Service (DDoS) attacks have overwhelmed telecommunications networks, causing services to become inoperable. Additionally, machine learning allows for more precise attacks on energy systems by predicting the best times to cause maximized disruptions (Stewart, 2024). The adaptable nature of these attacks makes them hard to defend against, as traditional cybersecurity measures may not be enough to handle the dynamic strategies used by AI-driven threats (Minhaj, 2023).

These emerging trends highlight the urgent need for organizations to incorporate AI into their cybersecurity strategies. By shifting to advanced foresight and proactive approaches, organizations might be improved in predicting and addressing the risks associated with AI-driven cyberattacks before they occur (Minhaj, 2023).

2.2 AI-Driven Threats

Artificial intelligence (AI) has significantly transformed the field of cybersecurity, especially through developed techniques such as deep learning and adversarial AI. AI can enhance attack precision and sophistication in cyber attacks, allowing attackers to manipulate and exploit vulnerabilities more efficiently and impactful (Minhaj, 2023).

For example, deep learning algorithms enable the rapid analysis of network vulnerabilities and can optimize the timing and direction of attacks. It basically learns and improves in real-time how to find holes and uses that to create targeted breaches that are difficult to detect and counteract. Furthermore, there is adversarial AI, which has become increasingly concerning within cybersecurity. It is a method where attackers use algorithms to generate "adversarial" inputs that fool even advanced detection systems (Minhaj, 2023; Yamin et al., 2021).

Yamin et al. (2021) points out how adversarial models can bring down even advanced machine learning (ML) defenses by leveraging minor input modifications, which allows attacks to escape from traditional security measures in critical sectors such as the healthcare and broader infrastructure.

These approaches have fundamentally shifted the nature and level of cyber risks. As AI-driven automation enables the execution of large-scale, continuous attacks which is creating vulnerabilities within organizations that lack advanced defenses (AbnormalSecurity,2024).

Sangfor Technologies (2024) further points to the slightly unknown danger of AI-driven automation's role in "hacking-as-a-service," making it easily accessible for individuals with low technical expertise to launch or to say, to order, AI-enhanced cyberattacks on critical infrastructure.

Fig. 1 illustrates an example of a carefully calculated noise which is added to a normal chest CT examination. As a result, the software will categorize the apparently normal examination as one with a (nonexistent) pulmonary mass highly suspicious for lung cancer. With that, causing misclassification with potentially significant consequences for the patient (Sorin et al.,2023).

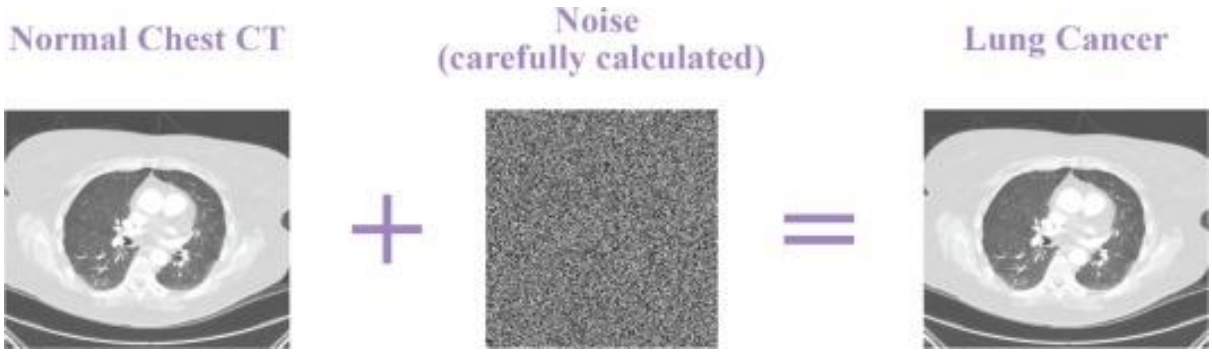

Figure 1. A Simplified Example of Adversarial Attack Generation (Sorin et al., 2023)

As already pointed out, the landscape of cyber threats is being transformed by AI and is challenging our current security defenses – another concerning observed development is deepfake technology - the ability to create highly realistic audio and video impersonations. These are often used to fake authority and other important figures, in order to trick people into revealing critical information. Those deepfake attacks have become a major concern with over 66 per cent of cybersecurity organizations reporting such attacks only in 2022 (Sangfor Technologies, 2024).

The list of threats continues with polymorphic malware, this one can modify its own code to go past antivirus software. We can also observe, that AI is revolutionizing social engineering attacks. This means that it can develop highly personalized and convincing phishing emails that are almost indistinguishable from legitimate and original messages. These AI-powered attacks have brought cyber attacks on a completely new level not only with developed attacking skills but also by reducing attack costs by up to 95% while simultaneously improving success rates through more precise targeting (Sangfor Technologies, 2024).

Finally, there are some other notable AI-driven developments, such as automated brute force attacks and voice cloning technology. These new threats are specifically targeting our security fundamentals like password systems and voice authentication (Sangfor Technologies, 2024). It is clear that attackers, who gain access to those security fundamentals, can have a highly impactful damage on our critical infrastructure - this whole development is highlighting why we should not underestimate the need to develop more adaptable and foresight-based cybersecurity strategies.

2.2.1 Notable AI-Driven Cyberattacks on Critical Infrastructure

The development of AI-driven cyberattacks has rapidly transformed the threat landscape for our critical infrastructure, revealing unmatched vulnerabilities in essential services like energy, water, and telecommunications. Some of those modern attacks demonstrate how AI enables cybercriminals to identify and exploit system weaknesses with improved skills. One notable example involved Nippon Telegraph and Telephone (NTT), where attackers exploited vulnerabilities on public-facing websites to gain access to the internal systems of companies. This attack illustrated how attackers utilize AI tools to identify weaknesses and pass traditional defenses, which leads to a domino effect that impacts interconnected infrastructure systems (Istari Global, 2024).

Another major incident took place at the Oldsmar Water Treatment Plant in Florida, where attackers gained remote access to the control system for the water supply and manipulated chemical levels, including sodium hydroxide. Although the breach was detected and reversed in time, it highlighted the tangible and direct physical threats that AI-driven cyberattacks can have on public safety. The ability of the attackers to remotely access the system shows the risks with AI amplifying harm in cyber-physical infrastructure (Istari Global, 2024).

The Colonial Pipeline attack in the energy sector is another critical example. A group known as DarkSide used AI-based tools to infiltrate and deploy ransomware, which disabled fuel distribution systems across the U.S. Eastern Seaboard. By leveraging AI to enhance the adaptability of the ransomware, the attackers successfully passed through security measures and demanded a large ransom. This incident showed not only the capabilities of AI to increase the complexity of attacks but also to avoid being detected while disrupting vital supply chains (Istari Global, 2024).

It let be said, that the previous mentioned cases again call for the need of strategic foresight in cybersecurity to be more capable of preparing and to some extent anticipating the new levels of such attacks.

2.2.2 Emerging Risks Due to Rapid AI Evolution

The development of new risks is a process of constant growth due to the rapid evolution of AI and traditional defenses which are struggling to keep up with the pace of adapting threats. Abnormal Security (2024) highlights the danger of greater autonomy and predictive power gained by advanced AI models, which allows them to conduct complex attacks with little human input. This makes it even more challenging for traditional and reactive cybersecurity systems, as these are usually static and cannot adjust quickly or effectively to counter such dynamic AI-driven threats.

Furthermore, Sangfor Technologies (2024) points out that the fast pace of AI advancements has led to a situation where even robust cybersecurity defenses are constantly reacting to new forms of AI exploitation, instead of preventing them. For example, the rise of generative adversarial networks (GANs) has made it easier to create realistic phishing content, which makes it hard for conventional detection systems to tell real from fake. Moreover, as AI continues to progress, it is expected that attackers will use these tools for more specific attacks on sectors to take advantage of unique vulnerabilities within critical infrastructure (Yamin et al., 2021).

In consideration of the rapid AI development, there is a growing risk that new tools will keep outpacing defense capabilities and their potential for harm could increase. Therefore, the need for proactive strategies that can address not only current but also future AI-driven cyber threats is urgent in every aspect of modern cyber security (Malik et al., 2024).

Figure 2 below illustrates how multi-diverse and damaging these AI-driven cyber attacks have become over the years and how some of the previously mentioned techniques are used for attacks on industries (Kour et al., 2024).

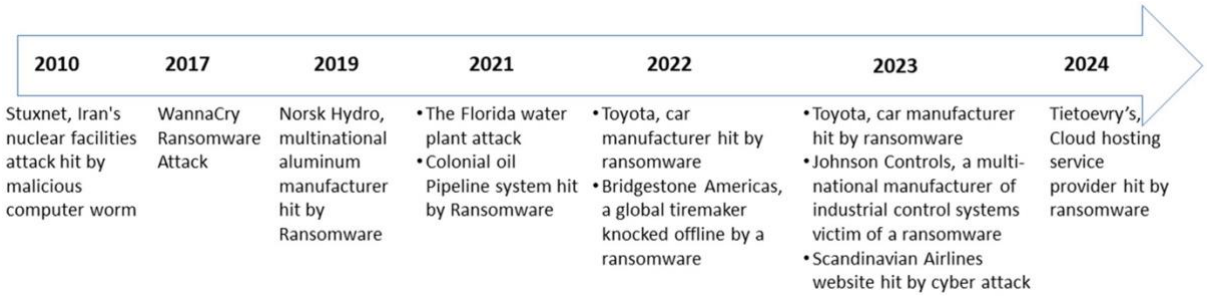

Figure 2 : Timeline of some of the occurrences of cyberattacks in industries. (Kour et al., 2024)

2.3 Shortcomings of Current Cybersecurity within Critical Infrastructure

While traditional cybersecurity measures focus on responding to attacks after they happen, this approach is becoming increasingly inadequate in today's world of AI-powered threats. This section examines the limitations of reactive cybersecurity strategies and makes the case for a more forward-thinking approach that can anticipate and prevent attacks before they occur.

Current cybersecurity strategies for critical infrastructure mostly rely on reactive approaches, addressing cyber incidents only after they occur. Although these post-incident responses remain important, they consistently fail to address the complexity and adaptability of modern cyber threats. This vulnerability becomes particularly concerning when confronting AI-driven attacks, as many organizations lack mechanisms for preemptive risk detection and mitigation (Ozcan et al., 2022; Gueye et al., 2024).

Reactive cybersecurity without foresight strategies has a key limitation most visibly against advanced attack methods like AI-enhanced social engineering and polymorphic malware. Polymorphic malware dynamically modifies its code during each attack and therefore, easily circumvents traditional signature-based detection systems (Malik et al., 2024). Similarly, AI-powered social engineering uses deep learning to create highly personalized phishing schemes, which is increasing the likelihood of user compromise (Gourisetti et al., 2024; Kour et al., 2024). So these reactive strategies which are mainly focused on post-incident responses, could

be in this case unable to anticipate or quickly adapt to evolving attack methods, leaving our critical infrastructure exposed to modern threats.

Furthermore, the fragmentation of cybersecurity protocols across interconnected sectors compounds these challenges. Critical infrastructure like healthcare, finance, energy and telecommunications, operates as a tangled and interdependent ecosystem (Kour et al., 2024).

However, organizations often implement cybersecurity measures in isolation, which is limiting comprehensive threat detection and response capabilities – this counts as a main gap and barrier for IT security firms to integrate foresight in those firms and prepare their systems for AI attacks. Therefore, this siloed approach creates systemic vulnerabilities, where a breach in one sector can potentially cascade and amplify damages across multiple systems (Canorea, 2024; Ozcan et al., 2022).

Although detection and recovery efforts are necessary, they are not sufficient to meet the cybersecurity demands of critical infrastructure. An overemphasis on recovery overlooks the importance of proactive and forward-looking strategies that are capable of preempting potential threats. This limitation is especially concerning when it comes to AI-driven attacks, which significantly reduce the response time for our security systems and could increase the damage to critical services (Kour et al., 2024).

2.3.1 Calls for Proactive and Foresight-Based Approaches

In consideration of the limitations of reactive measures, cybersecurity experts increasingly advocate for proactive and foresight-based strategies. These strategies highlight the importance of anticipating and addressing threats before they occur, focusing on building resilience rather than relying only on recovery. This shift is particularly important given the growing sophistication of AI-driven threats, which allow attackers to quickly adapt and automate their techniques at a pace which traditional and outdated cyber security measures cannot cope with. (Fischer et al., 2022).

Therefore, proactive cybersecurity strategies can have the ability to cope with that sophistication. It can leverage advanced tools like predictive analytics, behavioral analysis, and AI-powered threat intelligence. By detecting vulnerabilities early, these approaches allow organizations to address potential weaknesses before they can be exploited. In contrast to traditional models, these strategies can effectively respond to threats evolving in real-time, a

crucial capability for critical infrastructure, where cyberattacks can lead to significant systemic disruptions. Experts consistently highlight the importance of strategic foresight and early-warning systems in anticipating potential threats and enhancing overall resilience (Kuraku et al., 2023).

Furthermore, the integration of proactive and foresight-based approaches into cybersecurity frameworks is not only effective in addressing known threats but also essential for adapting to new attack vectors as they emerge. By this, firms could also conduct improved vulnerability assessments and find unknown entry points which could be exploited by AI-driven attacks. This transition is highly important, as AI capabilities continue to grow as well and attackers are likely to utilize these tools for more sophisticated methods, making foresight-driven strategies essential for maintaining a forward-thinking cyber security. By cultivating a mindset of continuous adaptation and proactive risk management, cybersecurity stakeholders can build more agile defenses to ensure effective protection against this evolving landscape of AI-driven attacks (Fischer et al., 2022; Kuraku et al., 2023).

2.4 Strategic Foresight Techniques as a Cybersecurity Tool

The following section explores how strategic foresight techniques can be integrated and enhanced to meet the challenges of AI-driven cyber threats. Moving from traditional cybersecurity tools to more proactive approaches, we examine how strategic foresight methods can be implemented and transformed to anticipate and counter AI attacks. Particularly significant is the potential of using AI itself as a defensive tool - essentially fighting AI with AI - which could transform how we protect critical infrastructure from cyber threats. This analysis sets the foundation for bridging the gap between theoretical approaches and practical implementation in cybersecurity.

Strategic foresight offers a proactive approach to anticipating AI-driven cyber threats. Traditional and reactive measures in cyber security which include, scenario planning, trend analysis, and expert consultation, have long served to detect potential risks across various domains. However, due to developments of the cybersecurity landscape by AI, these conventional security methods struggle to keep the pace of AI-driven threats that are rapidly evolving in its impact and complexity (Fischer et al., 2022).

The idea of integrating strategic foresight in cybersecurity, especially in our critical infrastructure, has shown promise.

Current approaches often fall short when dealing with AI-driven attacks due to their strong differentiation from traditional threats, in their ability to learn and adapt to reactive security measures (Raban & Hauptmann, 2018; Salami et al., 2024). Conventional scenario planning, which relies on predictable attacker behaviors, becomes insufficient when facing AI systems that are able to autonomously adjust their strategies in real-time. This limitation highlights that traditional techniques, focused on historical and current data, cannot address the innovative nature of AI-threats in which attackers can identify unknown entry points (Salami et al., 2024)

Furthermore, AI-driven attacks employ an advanced level of the earlier mentioned machine learning models, that can adapt and refine their strategies as they encounter new defenses. This ability to learn autonomously without human intervention, demands more advanced foresight models for proactive security systems. For example, environmental scanning must expand beyond just monitoring AI technologies - it also needs to track patterns in AI research that could signal potential malicious applications and also scan for unknown entry points which could be exploited (Onwubiko & Ouazzane, 2021; Salami et al., 2024). While this shift toward "AI-aware" foresight is promising, it faces significant barriers to overcome in current frameworks that struggle to fully address the dynamic nature of AI-driven threats (Salami et al., 2024).

2.4.1 Adapting Foresight Techniques for the Specific Challenges of AI-Driven Threats

Traditional cyber security tools, showing clear limitations as these measures were not built to handle autonomous and adaptable threats. Therefore, the self-learning and adaptive capabilities of AI-driven cyber threats introducing now unmatched uncertainty to cyber security in critical infrastructure. While conventional risk assessments rely on recognized attack patterns, AI-driven threats can significantly vary from these patterns in using their learning capabilities to bypass known defenses (Weng & Wu, 2024)

One promising adaptation to tackle this modern issue, is the integration of AI-driven attack simulations into scenario planning. This enhanced method, known as "AI-enhanced scenario planning," generates more realistic threat models by accounting for the speed and adaptability which are unique to AI-driven attacks. These simulations can reveal potential vulnerabilities in existing defenses and guide the development of proactive countermeasures (ENISA, 2023; Akhtar, 2021).

Furthermore, environmental scanning which is a vital tool in cyber security, needs to evolve as well to match AI-specific developments. An ‘’AI-sensitive’’ scanning approach could monitor not only technological advances but also potential dual-use technologies of AI research, such

as developments in natural language processing or image recognition that could be remodeled for attacks. This broader approach could enable improved anticipation of emerging AI-driven threats (Balantrapu, 2024)

The incorporation of machine learning into foresight techniques offers advanced capabilities for analyzing large datasets to detect weak signals of potential threats. By examining data across sectors, these enhanced foresight methods can reveal patterns that point to emerging types of AI-driven attacks, like automated vulnerability exploitation or adaptive malware that might escape traditional analysis (George et al., 2024)

This integration of AI-driven analytics into strategic foresight encourages continuous and real-time assessment of cybersecurity frameworks. It fosters a shift from static to dynamic foresight approaches. While strategic foresight remains crucial for proactive cybersecurity, AI-driven threats pose novel challenges that require significant adaptation of traditional methods. The evolution toward "AI-sensitive" foresight techniques, including enhanced scenario planning and environmental scanning, could provide the tools needed to address these complex and new risks. However, the effectiveness of these adaptations remains an active area of research critical to protecting infrastructure against increasingly advanced AI-driven attacks (George et al., 2024; Weng & Wu, 2024).

2.4.2 AI vs AI: Leveraging AI for Advanced Foresight-based Cybersecurity

With the rise of AI-driven cyber threats, employing AI as a defense tool in cybersecurity has become a focal point. AI can process large amounts of data quickly, recognize complex patterns, and adapt in ways that traditional cybersecurity cannot. However, by using AI not only to defend against but also to anticipate these threats adds another level of complexity and innovation. This approach involves leveraging AI for "strategic foresight" and with that, predicting future threats and understanding how they could evolve, especially when facing other AI-driven attacks (Schwarz et al., 2024; Weng & Wu, 2024).

Furthermore, such AI-driven foresight tools could also analyze and predict patterns in the behavior of malicious AI systems. For example, machine learning algorithms can be trained to recognize the tactics and patterns of adversarial AI, allowing defenders to forecast how future attacks might emerge (Schwarz et al., 2024). By studying these patterns, cybersecurity teams could prepare defenses for attacks before they happen and coming closer to shifting from reactive responses to proactive strategies (Weng & Wu, 2024).

Another aspect of AI-based foresight is its ability to simulate potential attack scenarios- like a scenario planning tool enhanced by AI. Such a tool, powered by AI can create realistic models of AI-driven threats and offering insight into vulnerabilities within critical infrastructure systems (Vegesna, 2023). These simulations could help organizations to explore "what-if" scenarios and evaluate the effectiveness of different defense systems. With such predictive insights preparedness may be enhanced but the effectiveness of these tools remains an ongoing area of research and development (Iyer, 2023).

Despite the potential benefits, leveraging AI for proactive cybersecurity is far from a perfect solution. Anticipating AI-driven threats is a constantly evolving challenge, as malicious AI systems continue to improve and adapt as well. As noted by Boston Consulting Group (2024), using AI to outsmart other AI requires advanced, up-to-date models that can keep pace with the latest techniques used by cybercriminals – a leveraging tool that provides AI defend systems with real-time data and with real scenarios. Furthermore, AI needs to be implemented with highest safety, as there is the risk of false positives, where AI might misidentify activities as threats, highlighting the need for a balanced, cautious approach (BCG, 2024).

Finally, while AI offers promising possibilities for enhancing cyber security with strategic foresight, the field is still developing. Current advancements indicate that AI could become a valuable tool in predicting and preparing for AI-driven cyber threats, yet these methods require more refinement and testing to be fully effective and feasible against advanced AI-powered attacks (BCG, 2024; Schwarz et al., 2024).

2.5 Role of IT Consulting firms in Bridging Theory and Practice

As the gap between cybersecurity theory and practical implementation grows, IT consulting firms are emerging as crucial bridge-builders in protecting critical infrastructure. This section explores how these firms are uniquely positioned to combine technical expertise with strategic planning, helping organizations in CI adapt to the challenges of AI-driven cyber threats while developing more integrated and collaborative security approaches across different sectors.

Critical infrastructure's increasing vulnerability to AI-driven cyber threats presents both challenges and opportunities for IT consulting firms. These organizations are uniquely positioned to help in protecting our interconnected infrastructure systems like energy grids, healthcare networks, and financial institutions. The interdependency of these systems means

that a successful attack in one sector could trigger serious effects across others which is making holistic security approaches essential (SmartTechnologies, 2024; Fischer et al., 2022).

Furthermore, IT consulting firms bring a valuable combination of technical expertise and strategic thinking to this complex landscape. While they usually have helped organizations defend against conventional cyber threats, the emergence of AI-driven attacks presents new exploration areas. These firms have the potential to leverage the interconnected nature of critical infrastructure to develop more robust and coordinated defense strategies that benefit multiple sectors simultaneously (Courtney, 2024).

Additionally, the role of IT consultants goes beyond providing technical solutions. They work closely with organizations to identify vulnerabilities in order to shape response strategies and build security awareness among employees. Especially in critical infrastructure this comprehensive approach is crucial, as a single successful attack could impact public safety and economic stability. As organizations grapple with the transition from traditional cybersecurity to methods that can counter AI-driven risks, IT consultants' expertise in both technology and strategic planning becomes increasingly valuable (Boston Consulting Group, 2024).

2.5.1 Bridging Fields of Technical Expertise and Strategic Insight

IT consulting firms are best positioned to bridge the current gap between pure technical cybersecurity expertise, strategic planning and consulting. By bringing together IT specialists, ethical hackers and strategy consultants, these firms are able to create more holistic and effective approaches to address AI-driven threats (Dinkova, 2024; Boston Consulting Group, 2024).

Given the apparent lack of synergy between traditional security practices and strategic foresight strategies, this bridging role seems especially important. IT consultants could explore ways to further leverage the practical expertise of ethical hackers with strategic planning techniques to develop more effective defences against AI-driven attacks. For example, consultants could use the collaboration with ethical hackers to test foresight-based security models against real-world attack simulations in order to help validate and refining their strategic approaches. Such synergies could result in transformed security frameworks that integrate hands-on experience with innovative and forward-thinking strategies (BridgeIT, 2024; Al-Hawamleh, 2023).

Furthermore, IT consulting firms might play a crucial role in helping organizations to develop more integrated approaches to cybersecurity. Rather than using security as a purely technical challenge, consultants could explore ways to embed strategic foresight into their clients' organizational culture and daily operations to foster a long-term impact on preparing firms against AI. This could involve, for example, developing new methodologies that combine technical security measures with strategic planning to help organizations prepare for both current and emerging AI-driven threats (Schwarz et al., 2024).

The interdependent nature of critical infrastructure also provides an opportunity for IT consultants to further develop collaborative security approaches. By working with various sectors, consultants could assist in developing coordinated defense strategies that leverage these interconnected systems. This could involve to create a shared threat detection network, standardized response protocols or collaborative foresight exercises that benefit multiple sectors simultaneously and could bring our critical infrastructure security closer to preparing and anticipating for emerging AI-driven threats (Boston Consulting Group, 2024; Yigit et al., 2024).

3.0 Methodology

3.1 Research Design

This thesis examines how strategic foresight can be integrated into cybersecurity practices for critical infrastructures to better prepare for and anticipate AI-driven threats.

The research methodology combines an extensive literature review of academic journals, consultancy reports, and industry publications with semi-structured interviews. Semi-structured interviews were chosen because they offer both structure and flexibility, making them ideal for gathering detailed insights about evolving cybersecurity challenges (Brinkmann, 2013). This interview format supports the thesis's holistic approach by capturing diverse expert perspectives across multiple domains. Each interview participant brings unique expertise and experience, contributing valuable insights into potential cybersecurity solutions.The research uses a qualitative approach to understand the experiences and strategic thinking of cybersecurity and consulting professionals. This methodology is particularly suited for examining the complex realities and challenges that come along with exploratory approaches (Kallio et al., 2016).

Using thematic analysis allows for the identification of important patterns that quantitative methods might miss, providing detailed contextual understanding of the data (Braun & Clarke, 2006).

3.2 Data Collection

Semi-structured interviews served as the primary data collection method, enabling detailed discussions about the complex relationship between cybersecurity and critical infrastructure. This method combined structured exploration of key themes with the flexibility for participants to share deeper insights. Open-ended questions were particularly valuable for exploring complex topics where responses could not be predicted in advance (Harrell & Bradley, 2009).

The study included 11 interviews in total, conducted via Zoom or in written form, over a four-week period, with participants across different locations. The interviewees represented diverse professional backgrounds in critical infrastructure and cybersecurity and are coded from A-K:

- 3 ethical hackers from IT consulting firms with clients in healthcare, telecommunication, and finance sectors (A,B,C)
- 4 IT consultants from IT consulting firms serving telecommunications and energy sectors (D, E, F, G)
- 2 strategy consultants from telecommunication and food sectors (H,I)
- 2 IT specialists from healthcare and finance sectors (J,K)

This variety ensured a rich breadth of perspectives from different segments of the industry, enhancing the study's holistic approach to identify solutions.

Interview participants were recruited through private network and LinkedIn. Separate questionnaires were developed for strategy consultants, IT consultants, and IT specialists/ethical hackers to address their specific expertise. Each questionnaire followed a structured progression: identifying vulnerabilities and gaps of traditional reactive cyber security within critical infrastructure, exploring potential approaches for strategic foresight integration as proactive cyber security, to prepare for and anticipate for AI-driven threats, and the role of IT consulting firms.

Interview durations ranged from 25 to 70 minutes, with two interviews conducted in German and the remainder in English based on participant preferences. All participants were guaranteed

anonymity to encourage open discussion. While most interviews were conducted via video call, two were adapted to written format to accommodate time and technological constraints.

The interviews yielded approximately 7 hours of recorded audio, which was transcribed using Restream software. These transcriptions provided the foundation for thematic analysis, supporting a thorough examination of how strategic foresight could be integrated into cybersecurity practices for critical infrastructure.

3.3 Evaluation of the interviews

The recorded interviews were transcribed and converted from text files to Word documents for analysis. German interviews were translated to English to ensure consistency across the analysis process.

The study used Thematic Analysis following Braun and Clarke's (2006) methodology to analyze the collected data. This widely recognized qualitative method offers both flexibility and methodological rigor, making it particularly suitable for examining the complex relationships between strategic foresight, cybersecurity, and IT consulting practices.

The analysis followed two stages. First, an inductive approach identified themes emerging directly from the interview data, capturing participants' experiences and insights. Second, a deductive approach connected these findings, to some extent with the theoretical frameworks established in the literature review, focusing specifically on how strategic foresight could strengthen cybersecurity in critical infrastructure against AI-driven threats.

A coding framework was developed to organize the data into themes that aligned with the literature review categories. The interview analysis revealed both expected and unexpected insights about strategic foresight in cybersecurity. While many findings aligned with the categories identified in the literature review, new themes emerged that offered additional perspectives. The analysis revealed an additional category, labeled 'Barriers to implementing Foresight-based Cybersecurity' (B), which captured important insights that fell outside the initial categorization framework.This emergence of a new category highlights the dynamic nature of qualitative research and underscores the importance of maintaining an adaptable approach to data analysis. These unexpected themes were documented and incorporated in the thematic analysis to ensure a comprehensive coverage of all the insights gained from the interviews.

Furthermore, the categories of "Vulnerabilities in critical infrastructure" and "Gaps in cyber security within critical infrastructure" were combined into a single category titled "Gaps and Vulnerabilities in Critical Infrastructure." This integration reflects their conceptual overlap and the interconnected nature of these issues as revealed through the interviews. This approach enhances the clarity and depth of the analysis, allowing for a more holistic discussion of the security challenges faced in critical infrastructure.

The following Table 1 presents these categories, their codings and descriptions, providing the structure for the findings and discussion sections. Statements from the interviews were then analyzed, coded and classified within the specific category.

Category	#	Description
Gaps & Vulnerabilities in Critical Infrastructure Cybersecurity	GV	Statements that describe gaps & vulnerabilities in traditional cybersecurity systems within critical infrastructure firms
Strategic Foresight in Cybersecurity	SF	All statements about the shift from traditional reactive security approaches to proactive practices: Strategic foresight integration for advanced cybersecurity solutions aimed at preparing for and anticipating AI-driven threats
Role of IT Consulting in Cybersecurity Transformation	IC	Statements on how IT consulting firms could facilitate the integration of advanced cybersecurity measures and strategic foresight within critical infrastructures: IT consulting as a bridge between current practices and desired advancements
Barriers for Implementing Foresight-based Cybersecurity	B	This category focuses on the challenges and obstacles faced in shifting towards foresight-based cybersecurity strategies and recommendations to overcome barriers

Table 1: Categories of interview statements

4.0 Results

The following chapter shows the results from the analysis of the interviews and the classified statements assigned to their categories.

The tables below will show excerpts of the categorized statements from the interviews. The complete summary results and all classified statements can be found in Appendix C.

Table 2 below shows all statements from the coded interviewees (ID) about gaps and vulnerabilities in critical infrastructure cybersecurity coded as category (GV).

Gaps and Vulnerabilites In Critical Infrastructure Cybersecurity		
#	ID	
GV1	A	so the main issue here, it's reactive. It waits for the attacker, to make an action, and later on, it react to that…reactive approach is the biggest drawback.
GV4	G	If you have proactive approaches, you can at least limit the amount of stuff that's happening at the same time. Because you filter a lot of from the beginning before it's even happening.
GV11	J	What makes them particularly risky is their reliance on outdated protocols, which AI-driven attacks can exploit.
GV13	I	A lack of unawareness, to really tackle this topic and understand foresight's strategic value…if you are unaware… it's also quite difficult to access quality data to do the required trend analysis and scenario planning to do the anticipation.
GV14	I	insufficient integration of foresight into security strategies

Table 2: Interview statements excerpt – GV

The next Table 3 illustrates all statements made about strategic foresight integration in cyber security, in order to approach proactive solutions. Coded as category (SF).

Strategic Foresight in Cybersecurity		
#	ID	
SF2	B	it would be effective if we all can share our data and build the big dataset and use machine learning algorithms to train it on this data.
SF6	I	establish a foresight team within the critical infrastructure organizations that are, overseeing all the progress and the process also in the transformation…crucial to conduct regular scenario planning and threat modeling, for the possible AI

		risks…collaboration is key in this kind of scenarios. So, I would also suggest to build up collaborative networks
SF14	E	Self healing. So these are systems that can not only detect, but fix themselves by themselves. It's very futuristic…This is like, an approach of, I would say, autonomous AI.

Table 3: Interview statements excerpt – SF

Table 4 below shows all statements regarding the role of IT consulting firms in integrating strategic foresight within cyber security measures and its role in bridging theory and practice. Coded as category (IC).

Role of IT Consulting in Cybersecurity Transformation		
#	ID	
IC1	A	And this can be a good, solid foundation for, AI threat detection and AI, to work against AI driven threats.. And, this should help in, like, building, let's say, collective intelligence… the IT consulting firm could be a base for this collective intelligence approach or solution.
IC5	I	maybe use the consultant expertise to train, critical infrastructure firms in foresight too, like trends, like analysis and scenario planning.
IC7	F	centralized platform. You can share your threat intelligence, across the sectors, and collaborate together and use the learnings of other companies, use their data, use their intelligence to anticipate attacks that, might happen and also to learn how to to mitigate the risk for that… that would be actually a big step for anticipating, because if somewhere happens something and we are, like, connected, we can anticipate it before it even hurts us….So that you like sharing real time data.

Table 4: Interview statements excerpt – IC

The last one is the category about barriers for implementing foresight-based solutions in cyber security. Here, all statements are included about barriers and challenges to overcome for the implementation of anticipatory and proactive solutions in critical infrastructure firms. Coded as category (B).

Barriers for Implementing Foresight-based Cybersecurity		
#	ID	
B1	I	Furthermore, physical and digital assets are having increased vulnerabilities. And, what many clients also struggle with is to find the resources that are required to handle those challenges.
B2	K	Data security, Human error, Finding qualified specialists.
B14	A	the problem again about enough data set, enough training data.

Table 5: Interview statements excerpt - B

5.0 Discussion

This research explores the complex relationship between gaps and vulnerabilities in critical infrastructure cybersecurity, strategic foresight solutions, and implementation barriers in the context of AI-driven threats. The findings reveal an interconnected dynamic where potential solutions to prepare for and anticipate AI-driven threats can address certain gaps and vulnerabilities while simultaneously facing implementation barriers. This creates a continuous cycle of development and adaptation, demonstrating why a holistic approach is essential for identifying viable solutions because of the strong correlation between weaknesses, solutions, and barriers to implementation.

To facilitate understanding and provide a clear overview, Table 6 below summarizes the key insights from the chapters of the discussion section. It presents the general topics, the corresponding insights, and the identified interviewees associated with each topic.

General Topic	Relevant Insight	Identified Interviewee
5.1 Current State of Gaps and Vulnerabilities in Critical Infrastructure Sectors (CI)	**Reactive Nature of Current Security:** reactive systems seen as major threats, unable to handle AI-driven threats and limited against AI attack variablitiy	A,B,G,J
	Outdated Systems and Technologies: old systems are less capable of coping with modern AI threats, requiring updates and modernization	A,D,E,G,J
	Human Error: human factors are significant vulnerabilities, with errors often paving the way for breaches	F,K
	Unwareness Gap: lack of awareness about full infrastructure capabilities and threats, needs better strategic oversight	A,I
5.2 Strategic Foresight-based Solutions	**General:** emphasis on proactive approaches to cyber threats, focusing on real-time intelligence and AI integration	A,B,F,G,I,J
	Collective Intelligence: the need for a secure, real-time data exchange among cybersecurity stakeholders to develop an ecosystem of information flow that improves threat anticipation and strategic foresight	A,B,F,G,H,I, J
	Autonomous AI: essential for reducing human intervention in real-time threat detection and response, enabling more dynamic and efficient anticipation of AI-driven threats	A,B,E
	AI-driven Scenario Planning: Utilizing AI to develop and enhance scenario planning techniques, providing a foresight-based framework for predicting and preparing for potential security threats before they manifest	A,D,I,K

5.3 Barriers to Implementing Foresight-based Solutions	**Data Issue** (sharing and gathering, trust, integrity and legal issues) and **Resource Limitation (cost, time and labor)** are identified as most significant barriers.	A,B,D,E,F,I,K
5.4 Role of IT Consulting and key recommendations	**IT consulting firms** are uniquely positioned to bridge the gap between theoretical solutions and practical implementations – shift from reactive to proactive foresight-based security in (CI) **Key Recommendations:** Collaboration between cybersecurity stakeholders, academia and government to foster foresight culture, develop new technologies and overcome barriers like resources and data.	A,B,D,E,F,G,I,J, K

Table 6: Discussion Overview

5.1 Current State of Gaps and Vulnerabilities

The research identifies several critical gaps and vulnerabilities in current cybersecurity approaches within critical infrastructure. A primary concern emerging from the interviews is the predominantly reactive nature of existing security measures.

Interviewees A, B, G, and J describe reactive systems in cybersecurity of firms in critical infrastructure as the biggest vulnerability and threat for exploitation by AI attacks. As interviewee A emphasizes, "The main issue here is that it's reactive. It waits for the attacker to make an action and later on, it reacts to that" (GV1). This reactive approach significantly hampers the ability to prevent attacks proactively, particularly in critical infrastructure environments where the consequences of breaches can be severe.

This problem is further complicated by the probabilistic nature of AI-driven attacks, as highlighted by interviewee B: "The biggest problem is the noise that AI can generate... AI models are probabilistic. They won't generate the same results every time" (GV2). This variability makes threat detection increasingly challenging and underscores the limitations of reactive security measures.

The reactive vulnerability is often described in current literature. Sangfor Technologies (2024) points out that the fast pace of AI advancements has led to a situation where even robust cybersecurity defenses, if reactive, are constantly reacting to new forms of AI exploitation, instead of preventing them. Moreover, Malik et al. (2024) add that these new tools will not only keep outpacing defense capabilities but their potential for harm could also increase. Therefore, the need for proactive strategies that can address future AI-driven cyber threats is urgent for our modern cybersecurity.

Another significant vulnerability lies in the prevalence of outdated systems and technologies. Interviewees A, D, E, G, and J identifying legacy systems and outdated protocols as major security concerns. As Interviewee A says, "IoT devices that they are relying on are old technologies or data protocols" (GV6). Interviewee G adds that legacy systems in firms they are working with are not updated, and the danger is that it takes less time for AI-driven attacks than for humans to find gaps in all these old systems (GV7). Interviewee J confirms that reliance on outdated systems makes it particularly risky and easier for AI-driven attacks to exploit those systems(GV11).

This aligns with the literature of George, Baskar, & Srikaanth's (2024) findings regarding vulnerable SCADA systems in energy and water sectors. However, the interviews revealed a deeper complexity to this issue, highlighting how AI-driven attacks can exploit these legacy vulnerabilities, especially in connection with reactive systems, and underline the interconnected nature of vulnerabilities and possible solutions. Therefore, a holistic approach is needed to explore strategic foresight solutions.

Another significant vulnerability in critical infrastructure systems described in both literature and interviews is human error. Interviewees F and K say that human error is still responsible for successful AI-driven attacks which could have been prevented with proactive systems. Interviewee F describes it as "the biggest vulnerability is the humans behind the systems" and notes that humans are the most vulnerable part because even if you have "the biggest and nicest security, which you can't really attack, you still have some kind of human interaction behind it where the human can still allow, run this as an administrator and then the security just goes blank" (GV16). From the literature, Stewart (2024) describes human error as a significant vulnerability in CI cybersecurity, noting that attacks like phishing or weak password setting could be prevented as they seem minor but can have enormous consequences.

An interesting gap in current critical infrastructure systems was gathered through the interviews and extended the scope of gaps and vulnerabilities from the literature – the unawareness gap in companies. Interviewee A and I noting this gap as a very impactful vulnerability but noted that it is not given enough attention in critical infrastructure firms and current research in cybersecurity. Interviewee A says: "big companies, sometimes they are not aware of the whole infrastructure...and their environment" (GV12). Interviewee I, as a strategy consultant, adds an important strategic viewpoint to that issue, stating that the lack of awareness is a topic to tackle and emphasizes the importance of understanding the strategic value of foresight integration in cybersecurity. He continues: "Another problem is that, if you're unaware, you're not really...hit the starting point that is required. And besides that, it's also quite difficult to access quality data to do the required trend analysis and scenario planning to do the anticipation" (GV13). Both state that unawareness either in their own security systems or from a strategic foresight perspective hinders cybersecurity in developing proactive approaches. Interviewee I continues in saying that there is within the unawareness gap a foresight lack and describes it as "insufficient integration of Foresight into security strategies" (GV14). Furthermore, he adds another valuable strategic perspective on this gap and describes a threat for our critical infrastructure firms, which was neither mentioned in the literature nor in any of the other interviews - reputational and long-term damage. Interviewee I describes the threat through a lack of foresight as follows: "And this could really lead to reputational damage. If you're operating in the segment of critical infrastructure, these kinds of attacks that are putting you in danger really could, cause reputational damage for you. This would have a long-term effect on your company" (GV15). This statement extends the vectors of how cyber attackers can amplify their impact of damage on firms in our critical infrastructure and how important it is to integrate strategic foresight in cybersecurity.

5.2 Strategic Foresight Solutions and Their Dual Nature

The research identifies several promising strategic approaches to address these gaps vulnerabilities primarily centered around two key approaches for solutions: Collective Intelligence and Autonomous AI development. These two approaches aim for our current cybersecurity in critical infrastructure to account for gaps and vulnerabilities. They also serve as exploratory approaches to overcome some barriers in integrating strategic foresight and developing proactive cybersecurity measures to prepare and anticipate for AI-driven threats. Besides the two mentioned main solution approaches there are two other approaches to discuss which aim to account for some of the previously discussed gaps and vulnerabilities in critical

infrastructure security. These solutions are partly used in cybersecurity strategies but in this thesis, it will be discussed to leverage those approaches with AI usage as discussed in the literature in section 2.4.2 AI vs AI. The solutions are called: AI Environmental Scanning and AI Scenario Planning. In the literature, these approaches were also mentioned. ENISA (2023) and Akhtar (2021) described AI in scenario planning as valuable to generate more realistic threat models and Balantrapu (2024) described AI Environmental Scanning as being able to enable improved anticipation of emerging AI-driven threats. However, the interviews revealed more depth in those approaches and linked them to strategic foresight implementation in cybersecurity. Environmental Scanning, or also called Vulnerability Analysis, is a common tool in strategic cybersecurity but using AI to leverage this tool is still a developing topic. Interviewees A, I, and J mention the use of AI for transforming Environmental Scanning. Interviewee I says that "AI algorithms are super helpful for that, to I identify the potential vulnerabilities" (SF19). Furthermore, A and J describe an interesting approach in not only using AI Environmental Scanning and AI Scenario Planning separately but rather to combine them and synergize the impact they have combined. Interviewee A describes the combination of AI usage in environmental scanning to enhance simultaneously scenario planning as follows: "we can use AI to help us understand, our attack surface and environment...huge firms, they are not actually aware of the whole infrastructure. And, if it can detect something hidden or something was not, tested or used for, then it can build an attack scenario for that...based on that, we can plan our strategic, security controls and proactive solutions" (SF17). Additionally, A adds the following: "it can plan you some attack scenarios that might occur or might happen based on what you have" (SF18).

With that he points not only the synergy between those approaches out but also how it can improve integration of foresight strategies for proactive cybersecurity and touches solutions for anticipating AI threats. Furthermore, he showcases that this kind of AI usage can account for the previously described “Unawareness Gap” by using AI to scan the environment for vulnerabilities which the firms do not even be aware of. This was a valuable statement on how to fill a gap in critical infrastructure security systems. Interviewee J also mentions the combination of both approaches but goes further in-depth by saying to use them as a predictive tool. He elaborates as follows: "AI can transform cybersecurity by enabling us to perform environmental scanning to detect previously unknown entry points and vulnerabilities within the system. AI-driven scenario planning can also simulate a range of attack strategies, allowing

us to prepare defenses against possible future threats. The key is to use AI not just defensively but as a predictive tool that can adapt and learn from continuous data inputs" (SF20).

These approaches are a good base for exploring solutions to anticipate AI threats but they are not enough to really prepare for and anticipate AI attacks as they are limited in their ability to work in real-time and with real data. Therefore, the interviews revealing two interesting approaches which were not covered in the literature and are aimed to overcome the limitations of the previous and current measures and strategies in cybersecurity: Collective Intelligence and Autonomous AI. Interviewees (A, B, F, G, I, J) all describing the best approach for exploring a solution to anticipate AI-driven threats – a Collective Intelligence tool. Interviewee A describes it as follows: "you collect data and experience and knowledge from different companies and sectors in the IT security. In real time and real scenarios. That's the important thing. So they are real. They are, alive, and they are up to date. That's very important" (SF1). He underlines the importance of real-time and real scenarios in preparing and anticipating for AI-driven threats by having an eco-system of information between all cyber security stakeholders. Interviewee B says that "it would be effective if we all can share our data and build the big dataset and use machine learning algorithms to train it on this data" (SF2), with that he added the ability to advance strategic foresight planning in cybersecurity as it allows us to use this collective data to train machine learning for anticipating possible threats. More in detail, this could be an approach to overcome the data barrier of having a big enough data set, which is essential to implement foresight-based solutions like AI Scenario planing and other approaches aimed at anticipating AI-driven threats. Interviewee G describes it as a "centralized platform where you can share data or information" (SF3) and adds that this would even allow "To learn from it and anticipate new threats which could come" (SF4). Furthermore, Interviewee I gives an interesting strategic advice on the development of such a collective intelligence. He says that firms need to "establish a foresight team within the critical infrastructure organizations that are, overseeing all the progress and the process also in the transformation to proactive cybersecurity" he continues with the importance "to conduct regular scenario planning and threat modeling, for the possible AI risks...collaboration is key in this kind of scenarios. So, I would also suggest building up collaborative networks" (SF6). Interviewee J also says that “future strategies should focus on enhancing collaborative efforts across different sectors to share threat intelligence and response strategies" (SF9) and highlights as well the leverage of collective intelligence in integrating foresight strategies in cybersecurity. Furthermore, Interviewee F describes this collective intelligence as a "defense wall" and elaborates further

that if we once have such a "collective knowledge", that “you collect the data of all firms and data about the infrastructure, you can really, use this data to train an AI on the Defender side to know how to best attack yourself... Especially when you combine it with a lot of other firms so that you have, like, a big collective data set, which you then can train an AI for" (SF7). Finally Interviewee F summarizes the common goal of the other interviewees with that approach: "if someone is a victim. Then you can at least anticipate the coming threat for the others and cut the connection…" (SF8) with that said, he points on a solution approach which could allow firms to semi-anticipate AI-driven attacks by collaborating and reporting attacks.

The second approach, gathered in the interviews, for an anticipatory solution is the development of Autonomous AI. It represents another promising solution pathway, especially for addressing human error vulnerabilities and enhancing response times. Interviewees A, B, and E mentioning the development of Autonomous AI as a huge step for approaching proactive solutions aimed at anticipating AI-driven threats. They all described it in different ways but confirmed to refer at the same concept. Interviewee A describes the usage of this development for automated reaction which overcomes the previously discussed human error gap, as "we have short reaction time to anticipate it if it's in one department" (SF10) and with autonomous AI this shortage could be solved and therefore again, be able to semi-anticipate threats. He further continues that this autonomous AI could be used to "be more flexible when there's a new update including security patches. It should be able to easily just, get the new updates… of the new security patches" (SF12) in order to better prepare for AI threats by constantly updating itself. Another interesting point is made by Interviewee B as follows: "We need to find the way how the model can found actually the lack of knowledge in itself. If we will find a way to do so, the model actually can say that: I don't have actually knowledge about this one. That will be a huge step in the ways that we can actually use this for automation alone" (SF13) Interviewee E refers to autonomous AI as a "self-healing system" that can not only detect, but fix themselves independently. E refers to that as “very futuristic” and as an "approach of… autonomous AI" (SF14). This approach was discussed as a main barrier which hinders us currently from better preparing and anticipating for AI-driven threats, as attackers can use autonomous AI freely but for defenders there are too many risks in automated AI as Interviewee A describes as follows: "If it was misimplemented or someone took advantage of it, it can work against the firm" (B27) and therefore, autonomous AI is still a developing approach but if developed safely all three (A, B, and E) mentioning that it could be a solution to prepare for AI-driven threats.

5.3 Barriers for Implementing Foresight-Based Solutions

This section was completely formed by the interviews as the literature did not cover barriers but the interviewees were seeing a highly important point in discussing barriers.

The implementation of proactive solutions faces significant barriers to overcome. For example, in the case of Collective Intelligence barriers are, particularly in data sharing and trust. As interviewee F observes, "fragmentation of information... there's no communication, some company has a breach and they don't wanna talk about it, then nobody can learn from it" (B18). This highlights the need for careful balance between information sharing and security concerns. Interviewee A further describes the trust issue as a barrier for implementing a solution approach like Collective Intelligence as follows: "you can take a dataset from company 1 and based on their experience and knowledge base, they say, threat x is not an actual threat, and company 2 says it is an actual threat. So now your whole process is not is not working correctly. Like this, you will have contraction, and it will cause issues…" and continues with saying that this issue could be solved "…with good data scientists" (B15). Interviewee B adds that there is a threat coming along with the trust issue as if firms "give data to another big dataset, then we we have the issue with the integrity of your data. So your data was used by another company, and it could be data of your clients…you don't know if it's not from your company, then you're not sure if, the another company don't gonna try to poison your dataset" (B17).

Furthermore, resources were mentioned as a serious barrier. Interviewees B, D, E, I, K identifying resources like time, cost, and labor as the main barrier. Interviewee D describes it as follows: "these false positive events that are a big issue because they cost operational time. So imagine you get ten or fifteen notifications every hour that you've just suffered an attack. But it's just not right. It's just a false signal, a false early warning signal… And the question here is how to differentiate between requests from the right users and those from attackers" (B3). To overcome this barrier Interviewee I mentiones the previously discussed solution of Collective Intelligence as follows: "collaborating with, the academia or industry partners to co-develop these, foresight methodologies could be really helpful to, to speed up the whole process…share costs and resources" (B4). Furthermore, Interviewee B extends that point in combining it with the other discussed solution approach of Autonomous AI as follows: ", much work to filter the results… I think we need a tool that not only track this, but also we can rely on in analyzing these results. Because right now, it's, mostly people. We rely on the analysis because, we don't have the bulletproof system that will return the acceptable feedback, like, the

acceptable percent of, correct, feedback" (B5). Here, Interviewee B mentions how autonomous AI could facilitate data processing and overcome resource barriers.

5.4 Final Recommendations to Overcome Barriers and the Role of IT Consulting Firms

A unique contribution of this research is the identification of IT consulting firms as potential facilitators in implementing these solutions. The interviews reveal that these firms can serve as a bridge between theoretical solutions and practical implementation, particularly in developing and maintaining Collective Intelligence systems. Interviewee I emphasizes this potential: "use the strengths of IT consulting....combining the technical know-how with strategic foresight, that would help the critical infrastructure firms to develop a robust security framework" (IC6). This represents an advancement beyond the literature, which has primarily focused on technical solutions without adequately addressing implementation challenges. In addition, Interviewee B describes IT consulting firms as "a good, solid foundation for, AI threat detection and AI, to work against AI-driven threats" and with that IT firms "should help in, building collective intelligence… the IT consulting firm could be a base for this collective intelligence approach" (IC1). He further mentiones the synergy of IT specialists and consulting proficiency is a constant growth factor in IT consulting firms which is a unique base in developing anticipatory solutions (IC2). Furthermore, Interviewee I adds a strategic viewpoint how IT consulting firms can foster a strategic foresight culture to tackle the unawareness gap, in saying "maybe use the consultant expertise to train, critical infrastructure firms in foresight too, like trends, like analysis and scenario planning" (IC5). Interviewee I then continues in saying that IT consulting firms could serve as a "centralized platform" to share threat intelligence, across the sectors, and collaborate together by using learnings and data of other companies in order to finally anticipate attacks that might happen and to learn how to mitigate risks for that and that this would be actually a big step for anticipating, "because if somewhere happens something and we are, connected, we can anticipate it before it even hurts us….So that you like sharing real-time data" (IC7). With this statement I describes IT consulting firms unique position as a solid base for implementing a futuristic and anticipatory approach like Collective Intelligence. This aligns to some extent with the literature as BCG (2024) describes the role of IT consultants to go beyond providing technical solutions and rather as organizations grapple with the transition from traditional cybersecurity to methods that can counter AI-driven risks and defines IT consultants' expertise in both technology and strategic planning as becoming increasingly valuable. Furthermore, Courtney (2024) confirms that IT consulting firms bring a valuable combination of technical expertise and strategic thinking to this complex landscape of anticipatory

cybersecurity. However, the interviews added much more depth in the role of IT consulting firms in developing proactive solutions for modern AI-driven threats.

Furthermore, this study explores some final future implications and recommendations to overcome barriers for implementing the previously discussed anticipatory solution approaches, resulting from the interviews. Based on these findings, several recommendations emerge:

1. Development of Segmented Implementation Approaches: As suggested by interviewee A (B26), implementing security measures in isolated segments can provide "semi-anticipation" capabilities while managing risks and could overcome the trust barriers for implementing Collective Intelligence. Interviewee A explains it as follows: “by segmentation, I mean, like, isolation between departments, between physical resources “ this has the aim to motivate firms to collaborate by giving security for firms data ind infrastructure. This security A defines as follows: "If I have 2 or 3 departments inside my institution, each one should have their own network or their own storage. So if one compromise, the other one does not…if there is an attack, they cannot reach the whole firm, just probably a specific department…They cannot, do literal movement and attack the whole.” (B26) – this would serve as a semi anticipation system in case of a malicious attack on the Collective Intelligence platform.

2. Establishment of Trusted Information Sharing Frameworks: Creating structured platforms for sharing security information while maintaining organizational privacy and security. This could overcome the trust issue and help establish a Collective Intelligence platform. Here, IT consulting firms could serve as a "centralized platform" to use data of firms but not letting it flow through other competing firms. (IC7).

3. Partial Dependent Collective Intelligence: Interviewee A recommended a Partial Collective Intelligence to overcome the barriers for implementing, he describes it as follows: "collective intelligence platforms that a company would use, if they get compromised, they can be a nightmare for the whole world. They can't just allow, malicious threat, and they say it's allowed and it can, if I totally depend on them, that's a very important point also. " Therefore A suggests to not fully depend on the collective intelligence but depend on them partially, and also depend on internal people. He described it as an additional "internal intelligence… I should also be working internally and doing my own research online and having my own, offline collective intelligence. " (B29)

To sum up the discussion and filter the combined results from the interviews and literature, interesting approaches to develop foresight-based cybersecurity and to come closer in preparing for and anticipating AI-driven threats in critical infrastructure, stakeholders could consider the following: an autonomous AI system capable of learning and adoption. It could use real-time data from a collective intelligence platform which promotes secure collaboration and an eco-system of information flow among experts in cyber security, IT and Strategy Consulting and firms in critical infrastructure – while simultaneously offering independent offline channels for every participant. It needs to be designed with strong privacy protections and be able to operate under various regulatory environments.

5.5 Implications

Theoretical Implications

This thesis contributes to the understanding of strategic foresight in cybersecurity within critical infrastructure sectors by examining the complex relationship between technological innovation and strategic management. The research extends current theoretical frameworks by demonstrating how AI-driven strategies effectively address vulnerabilities within critical systems. Furthermore, it provides a more differentiated understanding of the challenges and potential solutions in implementing strategic foresight in cybersecurity. Building on previous research that identified similar gaps and solutions, this study offers detailed insights into implementation barriers and examines how IT consulting firms could serve as intermediaries between theoretical frameworks and practical applications. The study calls for an interdisciplinary approach that integrats IT, strategic management, and cybersecurity. Such an approach is a crucial step for developing advanced models that address rapidly evolving cyber threats and the technological capabilities to counter them. Furthermore, this study contributes to the discourse on ethical AI use in cybersecurity by underlining the importance for stringent guidelines and regulatory frameworks for responsible AI deployment.

Practical Implications

The findings provide actionable insights for critical infrastructure organizations seeking to integrate strategic foresight into their cybersecurity practices. A key recommendation is the investing in and developing of Collective Intelligence systems that could enable real-time data sharing and threat anticipation. Furthermore, organizations should also prioritize training and development of IT staff, focusing on skills that encourage and develop the proactive use of AI

technologies in cybersecurity tasks. Leadership in critical infrastructure companies should foster a proactive security culture that encourages continuous learning and adaptation to new threats. Active involvement from top management is crucial to cultivating organizational readiness and resilience against sophisticated AI-driven cyber threats.

6.0 Conclusion

This thesis aimed to explore the integration of strategic foresight into traditional cybersecurity practices within critical infrastructure firms, with the purpose of enhancing preparedness and anticipation against AI-driven threats. The research was based on an extensive and holistic literature review and complemented by conducting semi-structured interviews with diverse cybersecurity stakeholders from different industries. The findings provided deep insights into existing gaps and vulnerabilities, strategic solution approaches, and the implementation barriers within this dynamic field. Furthermore, the results show that approaching strategic foresight solutions for modern AI-driven threats is a process of continuous research and development. It requires collaboration among diverse stakeholders in critical infrastructure cybersecurity.

The findings highlight the dual importance of robust data management and adaptive cybersecurity technologies in addressing evolving threats. Strategic foresight requires a combination of technological capabilities and human expertise, emphasizing the vital role of continuous development and cultivating forward-thinking mindsets among cybersecurity specialists.

Effective collaboration between stakeholders in critical infrastructure proves essential for implementing foresight strategies successfully. This collaboration approach could enable organizations to make use of collective intelligence and shared experiences, strengthening their ability to anticipate and respond to threats.

This thesis contributes to the field by providing insights and understanding of how strategic foresight can be integrated into cybersecurity frameworks in order to mitigate risks associated with modern AI-driven threats. Through these advanced strategic approaches, critical infrastructure organizations could shift more effectively from a reactive to a proactive security approach. This would allow firms to not only defend but adapt to and anticipate future threats

and build long-term resilience against both present and future threats in our increasingly digital world.

6.1 Limitations

This thesis encountered several constraints during both the literature selection and methodology phases in selecting interview partners.

Due to the recent emergence and rapid development of this research field, sourcing comprehensive and up-to-date academic literature proved challenging. The selection was based on articles, journals, and reports, which were not always comprehensive, as this field remains in active development.

The participant selection process for interviews was also limited by multiple factors and specific requirements. The need for individuals who possessed the combination of critical infrastructure expertise, cybersecurity knowledge, and AI understanding. While the perspective of strategy consultants were crucial for examining strategic foresight, finding professionals with both strategic and IT security expertise proved very challenging. Furthermore, adapting to availability limitations of my interview partners was an additional constraint. Practical constraints also impacted data collection, with two potential participants withdrawing completely and two others switching to a written format due to scheduling conflicts.

In general, the constant development of AI and technology in cybersecurity presented an overall limitation for this study and therefore both the literature review and interview findings represent rather a current glimpse in this exploratory field.

6.2 Further Research

This study provides a foundational exploration, by a systematic and holistic review of recent literature and qualitative research on the integration of strategic foresight in current cyber security measures within critical infrastructure. Due to the rapidly evolving nature of this field, there are multiple vectors for future research to use and extend the insights which were developed here.

Future research could benefit, for example, from incorporating quantitative methods on a larger scale, alongside these qualitative insights to extend the research. It could either validate or

challenge the findings here and with that providing an improved or more robust framework for a better understanding of how strategic foresight-based solutions can be integrated into cybersecurity to prepare for modern threats. This could be done by exploring discussed approaches in this thesis, like Collective Intelligence and Autonomous AI development, in different contexts or sectors. Additionally, comparative studies across geographical regions or industries could reveal unique challenges and solutions which could enhance the applicability and relevance of the strategic foresight approach within cybersecurity.

Finally, in consideration of the constant development of AI technologies, future research should constantly update the frameworks and different strategies discussed in this thesis to keep them relevant and effective against future cyber threats.

To further develop this integrated approach of cybersecurity and strategic foresight, a collaboration between academia, industry and government institutions could advance this approach and drive innovation and resilience in critical infrastructure sectors.

References

Abnormal Security. (2024). How AI-enabled cyberattacks work, why they're increasing, and how to stop them. Retrieved from: https://abnormalsecurity.com/glossary/ai-enabled-cyberattacks

Anandita Iyer, A. & Umadevi, K.S. (2023). Role of AI and Its Impact on the Development of Cyber Security Applications. *Springer*. https://doi.org/10.1007/978-981-99-2115-7_2

Akhtar, M. (2021). The future of Artificial Intelligence in Cybersecurity: A Comprehensive Survey. *EAI. http://dx.doi.org/10.4108/eai.7-7-2021.170285*

Balantrapu, S. (2024). AI for Predictive Cyber Threat Intelligence. *International Journal of Management Education for Sustainable Development.* Retrieved from: https://www.ijsdcs.com/index.php/IJMESD/article/view/590/228

BCG. (2018). ARTIFICAL IUNTELLIGENCE IS A THREAT TO CYBER SECURITY. IT'S ALSO A SOLUTION. Retrieved from: *http://boston-consulting-group-brightspot.s3.amazonaws.com/img-src/BCG-Artificial-Intelligence-Is-a-Threat-to-Cyber-Security-Its-Also-a-Solution-Nov-2018_tcm9-207468.pdf*

BCG. (2024). What Leaders in Cyber Security Get Right. Retrieved from: https://www.bcg.com/publications/2024/what-cybersecurity-leaders-get-right

BCG. (2024). Closing The Gap In The Cyber Security Talent Shortage. Retrieved from: https://www.bcg.com/publications/2024/cybersecurity-talent-shortage-close-the-gap

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101. http://dx.doi.org/10.1191/1478088706qp063oa

Brinkmann, S. (2013). Qualitative interviewing. *Oxford University Press.* https://psycnet.apa.org/doi/10.1093/acprof:osobl/9780199861392.001.0001

Canorea, E. (2024). Protecting critical infrastructure from cyber-attacks. *PlainConcepts*. Retrieved from https://www.plainconcepts.com/protecting-critical-infrastructure-cyberattacks/

CheckPoint. (2024). AI: The New Frontier in Safeguarding Critical Infrastructure. Retrieved from: https://blog.checkpoint.com/artificial-intelligence/ai-the-new-frontier-in-safeguarding-critical-

infrastructure/#:~:text=According%20to%20Check%20Point%20Research,emphasizing%20the%20need%20for%20AI%2D

De Felice, F., Petrillo, A., Monfreda, S., & Romano, E. (2022). Critical infrastructures overview: Past, present, and future. *Sustainability, 14*(4), 2233. https://doi.org/10.3390/su14042233

ENISA (2023). Identifying Emerging Cyber Security Threats and Challenges For 2030. Retrieved from: https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030

Fischer, B., Meissner, D., Nyuur, R., & Sarpong, D. (2022). Guest Editorial: Cyber-Attacks, Strategic Cyber-Foresight, and Security. *IEEE Transactions on Engineering Management*, 69(6), pp. 3660-3663. https://doi.org/10.1109/TEM.2022.3204165

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber threats to critical infrastructure: Assessing vulnerabilities across key sectors. *Journal of Infrastructure Research, 11*(3). Retrieved from https://puiij.com/index.php/research/article/view/118

Gourisetti, S. N. G., Mylavarapu, S., & Robertson, S. (2024). The role of AI in advanced cybersecurity threats: Emerging vulnerabilities and implications. *Journal of Cyber Security Technology, 11*(2), 95-117. https://doi.org/10.1080/12345678.2024.1123456

Gueye, M., Iqbal, A., & Wang, Y., Mushtaq, R., Petra, M. (2024). Addressing the gaps in cybersecurity for critical infrastructure: A proactive framework. *electronics, 18*(4), 335-353. https://doi.org/10.1016/j.ijcip.2024.101234

Harrell, M. C., & Bradley, M. A. (2009). Data Collection Methods. Semi-Structured Interviews and Focus Groups. *RAND*. Retrieved from: https://www.researchgate.net/publication/235018870_Data_Collection_Methods_Semi-Structured_Interviews_and_Focus_Groups

Hassan Minhaj, S. M. U. (2023). Study of artificial intelligence in cybersecurity and the emerging threat of AI-driven cyber attacks and challenges. *SSRN Electronic Journal.* Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4652028

Ige, A., Kupa, E., & Ilori,O. (2024). Analyzing defense strategies against cyber risks in the energy sector: Enhancing the security of renewable energy sources. *IJSRA*. https://doi.org/10.30574/ijsra.2024.12.1.1186

Istari Global. (2024). Analysis of top 11 cyber attacks on critical infrastructure. Retrieved from: https://istari-global.com/insights/spotlight/analysis-of-top-11-cyber-attacks-on-critical-infrastructure/#:~:text=Nippon%20Telegraph%20%26%20Telephone%20(NTT)%3A

Kallio, H., Pietilä, A.-M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide. *Journal of Advanced Nursing*, 72(12), 2954-2965.

Kour, S., Singh, K., & Rana, P. (2024). Polymorphic malware and AI-driven social engineering: Implications for cybersecurity. *Journal of Information Security, 20*(1), 34-56. https://doi.org/10.1016/j.jinfosec.2024.111234

Kumar, S., Gupta, U., Singh, A., & Singh, A. (2023). Artificial Intelligence: Revolutionizing Cyber Security in the Digital Era. *Journal of Computer, Mechanical and Management.* Retrived from: https://jcmm.co.in/index.php/jcmm/article/view/64/45

Kuraku, T., Nakamoto, H., & Suzuki, R. (2023). Foresight-driven cybersecurity: Building resilient critical infrastructure against AI-driven threats. *Technology in Society, 62,* 101758. https://doi.org/10.1016/j.techsoc.2023.101758

Malik, Z., Singh, R., & Baig, Z. (2024). Challenges in defending critical infrastructure against AI-enabled malware. *International Journal of Computer Science and Information Security, 14*(2), 182-193. https://doi.org/10.1007/s10115-024-01077-4

Ojo, B., Ogborigbo, J., Okafor, M. (2024) Innovative solutions for critical infrastructure resilience against cyber- physical attacks. *World Journal of Advanced Research and Reviews. https://doi.org/10.30574/wjarr.2024.22.3.1921*

Onwubiko, C. & Ouazzane, K. (2021). Multidimensional Cybersecurity Framework for Strategic Foresight. *Intl. Journal on Cyber Situational Awareness*, 6(1), pp. 46-77.

Ozcan, A., Demir, M., & Gürsoy, M. (2022). Interconnected vulnerabilities in critical infrastructure: Challenges for reactive cybersecurity measures. *Critical Infrastructure Journal, 9*(3), 189-202. https://doi.org/10.1016/j.cij.2022.102311

Raban, Y., & Hauptman, A. (2018). Foresight of cyber security threat drivers and affecting technologies. *foresight*, *20*(4), 353-363.

Riggs, H., Tufail, S., Parvez, I., Tariq, M., & Amir, A. (2024). Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure. *Sensors, 23*(8), 4060. https://doi.org/10.3390/s23084060

Salami, A., Igwenagu, U., Esambe, M., Olaniyi, O., & Oladoyinbu, O. (2024). Beyond Conventional Threat Defense: Implementing Advanced Threat Modeling Techniques, Risk Modeling Frameworks and Contingency Planning in the Healthcare Sector for Enhanced Data Security. *SSRN. https://dx.doi.org/10.2139/ssrn.4809837*

Sangfor Technologies. (2024). Defining AI hacking: The rise of AI cyber attacks. Retrieved from https://www.sangfor.com/blog/cybersecurity/defining-ai-hacking-rise-ai-cyber-attacks

Schwarz, K., Schwarz, F., Brandis,K., Creutzburg, R. (2024). AI-Based Cybersecurity Management Consulting – A New Disruptive Technology For the Future. *Electronic Imaging*. https://doi.org/10.2352/EI.2024.36.3.MOBMU-325

Sledjeski,C. (2023). PRINCIPLES FOR REDUCING AI CYBER RISK IN CRITICAL INFRASTRUCTURE: A PRIORITIZATION APPROACHJ. *Mitre.* Retrived from: https://www.mitre.org/sites/default/files/2023-10/PR-23-3086%20Principles-for%20Reducing-AI-Cyber-Risk-in-Critical-Infrastructure.pdf

Sorin, V., Soffer, S., Glicksberg, B., Barash, Y., Konen, E., & Klang, E. (2023). Adversarial attacks in radiology – A systematic review. *European Journal Of Radiology.* Retrieved from: https://www.ejradiology.com/article/S0720-048X(23)00399-6/fulltext

Stewart, J. (2024). Critical infrastructure systems are vulnerable to a new kind of cyberattack. *Georgia Institute of Technology.* Retrieved

from: https://coe.gatech.edu/news/2024/02/critical-infrastructure-systems-are-vulnerable-new-kind-cyberattack

Vegesna, D. (2023). Enhancing Cyber Resilience by Integrating AI-Driven Threat Detection and Mitigation Strategies.*Transactions on Latest Trends in Artificial Intelligence, 4*(4). Retrieved from: https://ijsdcs.com/index.php/TLAI/article/view/396/140

Weng, Y., Wu, Y. (2024). Leveraging Artificial Intelligence to Enhance Data Security and Combat Cyber Attacks. *Journal of Artifical Intelligence General Science. https://doi.org/10.60087/jaigs.v5i1.211*

Yamin, M. M., Ullah, M., Habib, U., & Katt, B. (2021). Weaponized AI for cyber attacks. *Journal of Information Security and Applications, 61*. https://doi.org/10.1016/j.jisa.2021.102926

Appendices

Appendix A: Interview Guide - IT Specialist, IT Consulter and Ethical Hacker

Introduction and Consent:

- Introduction: Introduce myself and my academic affiliation.
- Purpose of Research: Briefly explain the research's goal to explore strategic foresight integration into cybersecurity within critical infrastructure.
- Research Objectives: Outline objectives, focusing on identifying vulnerabilities, strategic solution approaches, and the role of IT consulting.
- Importance of Participation: Emphasize how their expertise is crucial to gaining practical insights into the implementation and challenges of strategic foresight in cybersecurity.
- Interview Structure: Inform about the structure and estimated duration of the interview.
- Consent for Recording: Request consent to record the interview for accuracy in data collection.
- Anonymity and Confidentiality: Assure confidentiality and explain the use of anonymized data in research outputs.

Company and Interviewee Background:

- Role and Experience: "Could you describe your current role and your experience in cybersecurity?"
- Connection to Critical Infrastructure: "How does your work relate to critical infrastructure cybersecurity?"
- Experience with AI in Cybersecurity: "What experience do you have with AI technologies in the context of cybersecurity?"

Main interview questions for guidance

1. Vulnerabilities and Gaps in Cybersecurity

- "What are the most pressing cybersecurity vulnerabilities in critical infrastructure that you encounter in your work?"
- "How do these vulnerabilities affect the firm's resilience against AI-driven threats?"
- "Why are these gaps specifically more endangered from rapidly growing AI-driven Attacks? "

2. Strategic Foresight Integration

- "Can you discuss any existing strategic foresight practices within your organization or observed in the industry?"
- To what extent can the integration of strategic foresight advance cyber security to prepare for and anticipate AI driven threats?
- "What are the benefits and challenges of integrating strategic foresight into cybersecurity practices?"
- "How do AI technologies feature in your strategic foresight planning?"
- "How could AI in defending, bring us a step closer to be prepared or to some extent anticipate AI-Driven attacks? "

3. Role of IT Consulting

- "How would you describe the role of IT consulting in leveraging the integration of strategic foresight within traditional cyber security?"
- "What role does IT consulting play in shaping cybersecurity strategies within critical infrastructure?"
- "How do consultants contribute to bridging gaps between strategic planning and practical cybersecurity implementation?"
- "Do you think IT consulting can facilitate the development of approaches for anticipating AI-driven threats?"

4. Future Directions and Personal Recommendation

- "Looking forward, what areas within cybersecurity and strategic foresight do you think require more in-depth research?"
- "What technologies or future research we need to better anticipate AI driven threats ?"
- "Can you suggest any innovative practices or technologies that might enhance the strategic foresight approach in cybersecurity?"
- "If you could develop the perfect tool for preparing for and anticipating AI-driven cyber attacks – How would it look like? What future technologies would be needed, what gaps & limitations must be filled? "

Closing

- Final Thoughts: "Is there anything else you would like to add that we haven't covered but you feel is important to this research topic?"
- Thank You and Next Steps: Express gratitude for their time and insights, explain the next steps, and offer to share findings once the research is completed.

Appendix B: Interview Guide - Strategy Consultant

Introduction and Consent:

- Introduction: Introduce myself and my academic affiliation.
- Purpose of Research: Briefly explain the research's goal to explore strategic foresight integration into cybersecurity within critical infrastructure.
- Research Objectives: Outline objectives, focusing on identifying vulnerabilities, strategic solution approaches, and the role of IT consulting.
- Importance of Participation: Emphasize how their expertise is crucial to gaining practical insights into the implementation and challenges of strategic foresight in cybersecurity.
- Interview Structure: Inform about the structure and estimated duration of the interview.
- Consent for Recording: Request consent to record the interview for accuracy in data collection.
- Anonymity and Confidentiality: Assure confidentiality and explain the use of anonymized data in research outputs.

Company and Interviewee Background:

- Role and Experience: "Could you describe your current role and your experience in terms of strategic foresight and planning?"
- Connection to Critical Infrastructure: "How does your work relate to critical infrastructure cybersecurity?"
- Experience with AI in Cybersecurity: "What experience do you have with AI technologies in the context of strategic planning and/or cybersecurity?"

General Role and Perspectives

1. How do you define the role of strategic foresight in supporting organizations to navigate complex and rapidly changing environments?
2. What do you see as the main challenges organizations face when integrating foresight and long-term planning into their operational strategies?

Strategic Foresight and Planning

1. What are the key elements of effective strategic foresight and scenario planning in industries with high uncertainty, such as critical infrastructure?
2. In your opinion, what techniques or methodologies are most effective for anticipating "unknown unknowns"? Can you share an example of where these methods worked well?
3. How do you recommend organizations balance short-term operational demands with the need for long-term strategic foresight?

Implementing Foresight in IT Consulting Contexts

1. What strategies or techniques would you suggest to help IT consulting firms integrate strategic foresight into their client services?
2. How should IT consultants and strategy consultants collaborate to develop robust plans for addressing complex challenges like AI-driven threats or other emerging risks?
3. In your view, what role does organizational culture play in successfully implementing foresight practices in IT consulting and critical infrastructure sectors?

Working with IT Consultants

9. How do you perceive the collaboration between strategy consultants and IT specialists/consultants? What are the key success factors in such partnerships?
10. What are some common challenges or gaps you have observed when aligning strategic foresight with technical expertise? How can these be addressed?
11. From a strategic perspective, how can IT consulting firms better align their services with broader organizational goals, particularly in sectors like critical infrastructure?

Future Trends and Preparedness

12. Looking forward, how do you think advancements in AI and other technologies will shape the future of strategic foresight? Do you think we could use AI ourselves to use against AI-driven Cyber Attacks? Do you know about possible future developments and technologies?
13. What advice would you give organizations in critical infrastructure sectors to future-proof their strategies and remain resilient against unpredictable challenges?
14. Are there any emerging strategic foresight tools or frameworks that you believe will become essential in the coming years?

Closing Reflections

15. What do you think is the single most critical factor for organizations to succeed in integrating strategic foresight into their planning processes?
16. Is there anything else you'd like to share about the role of strategy consultants in shaping foresight and planning within critical sectors?
17. Where do you see our current limitations – in Cyber Security, in strategic foresight, current technologies etc. – what hinders us to find a better solution to anticipate AI – driven threats?

Appendix C: Interview Results With Categories

Gaps and Vulnerabilites in Critical Infrastructure Cybersecurity		
#	ID	
GV1	A	so the main issue here, it's reactive. It waits for the attacker, to make an action, and later on, it react to that…reactive approach is the biggest drawback.
GV2	B	the biggest problem is, the noise that, AI can generate…AI models are probabilistic. They won't generate every time the same results. So, for, every attack, we will have, different, patterns…crucial challenge to detect it.
GV3	G	if you have reactive systems when a lot of stuff happens at the same time, it could very easily be overwhelming. We need to figure out what happens and what to do .But if a lot of events happen at the same time, it could take a very long time to actually figure out what happened and what is the right way to to mitigate this.
GV4	G	If you have proactive approaches, you can at least limit the amount of stuff that's happening at the same time. Because you filter a lot of from the beginning before it's even happening.
GV5	B	The reactive nature of these systems is also a major concern because they often can't counteract threats until after they have occurred, leaving us continuesly a step behind attackers.
GV6	A	IoT devices that they are reliance on old technologies or data protocols.
GV7	G	Legacy Systems…to keep them up to date… less time for AI than for human to find all these, old systems.
GV8	G	legacy systems…old databeses being used..and not secure anymore
GV9	D	API's and Iot devices.

GV10	E	you find yourself dealing with very outdated resources or very old technologies…and budget challenges.
GV11	J	What makes them particularly risky is their reliance on outdated protocols, which AI-driven attacks can exploit
GV12	A	big companies, sometimes they are not aware of the whole infrastructure...and their environment.
GV13	I	a lack of unawareness, to really tackle this topic and understand foresight's strategic value and how important it would be, especially in the current market surrounding for your company and, really strive towards doing this transformation. Another problem is that, if you're unaware, you're not really hit the starting point that is required and besides that, it's also quite difficult to access quality data to do the required trend analysis and scenario planning to do the anticipation
GV14	I	insufficient integration of Foresight into security strategies.
GV15	I	And this could really lead to reputational damage. If you're operating in the, segment of critical infrastructure, these kind of attacks that are putting you in danger really could, cause reputational damage for you. This this would have a long term effect on your company.
GV16	F	biggest vulnerability is the humans behind the systems. Because humans are the most vulnerable part….for example, you have the biggest and nicest security, which you can't really attack, you still have some kind of human interaction behind it where the human can still allow, like, run this as an administrator and then the security just goes blank.

Strategic Foresight in Cybersecurity		
#	ID	
SF1	A	you collect data and experience and knowledge from different, companies and sectors in the IT security. In real time and real scenarios. That's the important thing. So they are real.They are, alive, and they are up to date. That's, that's very important
SF2	B	it would be effective if we all can share our data and build the big dataset and use machine learning algorithms to train it on this data.
SF3	G	centralized, platforms where you can share data or share information.
SF4	G	To learn from it and anticipate new threats which could come
SF5	I	what would…highly help is that that if public and private sectors would collaborate more, also, like, helping each other out with providing, information and data and also learning from each other.
SF6	I	establish a foresight team within the critical infrastructure organizations that are, overseeing all the progress and the process also in the transformation. Also, what is crucial is, to conduct regular scenario planning and threat modeling, for the possible AI risks. And as previously said, collaboration is key in this kind of scenarios. So, I would also suggest to build up collaborative networks.
SF7	F	It's like a defense wall…this collective knowledge….when you have such a base and you collect the data of all firms and data about the infrastructure, you can really use this data to train an AI on the Defender side to know how to best attack yourself... Especially when you combine it with a lot of other firms so that you have, like, a big collective data set, which you then can train an AI for..And then use this for pen testing or, running scans on the system.
SF8	F	if someone is a victim. Then you can at least anticipate the coming threat for the others and cut the connection or something.
SF9	J	Future strategies should focus on enhancing collaborative efforts across different sectors to share threat intelligence and response strategies

SF10	A	we have short reaction time to anticipate it if it's in one department
SF11	A	AI driven tools should be there to, anomaly detection and intrusion detection. Like, if someone, trying to gain unauthorized access in my, infrastructure, as well as it should take action, like, should respond in time.
SF12	A	It should be more flexible when there's a new update including security patches. It should be able to easily just, get the new updates… of the new security patches.
SF13	B	We need to find the way how the model can found actually the lack of knowledge in in itself…That's, gonna be a huge step and, it will be a huge step in the ways that we can actually use this for for for automation alone.
SF14	E	Self healing.So these are systems that can not only detect, but fix themselves by themselves. It's very futuristic….This is like, an approach of, I would say, autonomous AI.
SF15	F	you can close the most traditional kind of threats with proactive cyber security. Because when you close these traditional gaps, you give attackers less playground to really hack you or come into your system. So it's it's really about how can I go or how can I limit the playground for attacks.
SF16	I	maybe use the consultant expertise to train, critical infrastructure firms in foresight too, like trends, like analysis and scenario planning.
SF17	A	we can use AI to help us understand, our attack surface, like our, environment with that…huge firms, they don't they are not actually aware of the whole infrastructure. And if it can detect something hidden or something was not, tested or used for, and it can detect, then it can build a scenario attack scenario for that…And then based on that, we can plan our strategic, security controls and proactive solutions.

SF18	A	from my perspective using AI just to build better vision or better understanding of my environment and my what do I have in my infrastructure. And later on, I use also AI to give me a good planning… it can plan you some attack scenarios that might occur or might happen based on what you have.
SF19	I	Also AI algorithms, are are super helpful for that, to I identify the potential vulnerabilities
SF20	J	AI can transform cybersecurity by enabling us to perform environmental scanning to detect previously unknown entry points and vulnerabilities within the system. AI-driven scenario planning can also simulate a range of attack strategies, allowing us to prepare defenses against possible future threats. The key is to use AI not just defensively but as a predictive tool that can adapt and learn from continuous data inputs.
SF21	F	So a proactive approach, in my opinion, would be to take the knowledge of existing things and try to attack a system, or just in general, pen test it to to see where you can still improve your, security system … you can just say to AI: write me code for overflowing the memory, How do I, do it? And then it would take, an attack that would take, for example, before, like, half a day or a day. would be much faster. Or even automated if you have a super good AI for attacking.
SF22	B	AI actually can find new vulnerabilities.

Role of IT Consulting in Cyber Security Transformation		
#	ID	
IC1	A	And this can be a good, solid foundation for, AI threat detection and AI, to work against AI driven threats.. And, this should help in, like, building, let's say, collective intelligence… the IT consulting firm could be a base for this collective intelligence approach or solution.
IC2	A	this concept of IT consulting leverages the ethical hacker. As an ethical hacker, you're not working alone for yourself in your department. You

		have always this, synergy and constant growth factor in an IT consulting firm.
IC3	A	not only on the working level, but also on the research level. The outcome from research should always have impact on internal procedures and companies and therefore improve the internal process…companies should always adapt to new technologies outside. They should always look, around and on the Internet and hear from researchers here and there about any new approaches or any new, outcome from research
IC4	G	AI and AI security are threats…it's a very new field… And it's, like, always evolving, and there's always coming out new stuff, new information, new data that maybe some people don't see. Like, for example, I don't get the insight, that the pen testers get.
IC5	I	maybe use the consultant expertise to train, critical infrastructure firms in foresight too, like trends, like analysis and scenario planning.
IC6	I	use the strengths of IT consulting….combining the technical know how with strategic foresight, that would help the critical infrastructure firms to develop a robust security framework
IC7	F	centralized platform. You can share your threat intelligence, across the sectors, and collaborate together and use the learnings of other companies, use their data, use their intelligence to, anticipate, attacks that, might happen and also to learn how to to mitigate the risk for that… that would be actually a big step for anticipating, because if somewhere happens something and we are, like, connected, we can anticipate it before it even hurts us….So that you like sharing real time data.
IC8	J	IT consulting firms play a pivotal role in cybersecurity, particularly because they merge deep technical know-how with strategic insights. This blend is something internal IT teams often miss.

Barriers for Implementing Proactive Cybersecurity		
#	ID	
B1	I	Furthermore, physical and digital assets are having increased vulnerabilities. And, what many clients also struggle with is to find the resources that are required to handle those challenges.
B2	K	Data security, Human error, Finding qualified specialists.
B3	D	these false positive events that are a big issue, because they also cost operational time. So imagine you get ten or fifteen notifications every hour that you've just suffered an attack. But it's just not right. It's just a false signal, a false early warning signal…
B4	I	collaborating with, the academia or industry partners to codevelop these, foresight methodologies could be really helpful to speed up the whole process…share costs and resources.
B5	B	much work to filter the results we need a tool that not only track this, but also we can rely on in analyzing this results… we don't have the bulletproof system that will return the acceptable feedback, like, the acceptable percent of, correct, feedback
B6	B	… And the question here is how to differentiate between requests from the right users and those from attackers.
B7	E	developing and running, AI based simulations, can be resource intensive. It needs a lot of resource, and, then it can be inaccessible for, small organization
B8	K	Shortage of specialists: There is a significant shortage of specialists with the necessary knowledge of AI and cyber security. Companies, and IT service providers in particular, face a particular challenge here
B9	A	difficult for Critical Infrastructure firms them to get new upgrades…Costly and, permissions

B10	A	AI being in hands of the attackers, it can help them to better understand the outdated technologies and the protocols of CI firms…plus to that, with tools being, AI driven or AI in the background being used, it can have more and more precise payloads and precise attacks. Nowadays, let's say detection systems, especially in these areas in these infrastructures, they can go and detect normal attacks or like human, based attacks. But with AI, it will be more precise and more accurate…AI has probably the whole surface to attac
B11	G	So they're just vulnerabilities in the system that are still needed, but at the same time, there's nobody that's really, taking the responsibility of, migrating them because it's so much work, too much money.
B12	I	from one of my previous projects is, the high recovery costs that are that are coming along
B13	A	the problem again about enough data set, enough training data.
B14	A	It depends on the source…where are you getting these datasets from? It's very important and there should be a trustworthy relationship between you and the source of these datasets. And these datasets, again, if you are talking about the datasets and machine learning, they should be scanned. They should be monitored. They should be, secured.
B15	A	you can take a dataset from company 1 And based on their experience, based on their knowledge base, they say, threat x is not an actual threat, and company 2 says it is an actual threat. So now your whole process is not working correctly. Like this, you will have contraction, and it will cause issues. But with good data scientists, it can be solved.
B16	B	the difficulties here is that we actually don't know how the attack model was trained and what data it was used. That's why it's pretty difficult to replicate your own model that you can use in this simulations and to test it and to see how how this model will try to bridge the system… the biggest problem is the data set.
B17	B	just give your data to another big dataset, then we have the issue with the integrity of your data. So your data was used by another company, and it could be data of your clients…you don't know if it's not from your

		company, then you're not sure if, the another company don't gonna try to poison your dataset.
B18	F	fragmentation of information..there's no communication, some company has a breach and they don't wanna talk about it, then nobody can learn from it. And especially if you have, new or emerging, threats like AI, there's not a lot of information out there..So we learn new on a day by day basis. Today, something new happens that could help us prevent the next breach. And I think that's currently a big limitation that there's not enough information sharing.
B19	F	Lack of real-time data processing.
B20	F	when we make it open source, well, then the hackers could also use it. So it must be on some kind of proprietary level. That we limit who can access this data, but still have it kind of collective for all firms or all critical infrastructure.
B21	F	data is a big barrier and that we could overcome it with a collective set of data.
B22	F	it's important to talk about it, to talk where your vulnerabilities were or how you got hacked. Otherwise, you won't help other firms to close these gaps. So transparency and not shaming other or think shamefully about your own threats is really important.
B23	E	machine learning depends on high quality data because you have models that you need to train on data.
B24	E	developing and running, AI based simulations, can be resource intensive. It needs a lot of resource, and, then it can be inaccessible for, small organization.
B25	J	research into machine learning models that can predict and neutralize new threats in real-time. Current limitations are often related to data privacy concerns and the computational power needed to run these advanced models. Overcoming these will be crucial for advancing our defensive capabilities.
B26	A	Segmentation. And by segmentation, I mean, isolation between departments, between, physical resources. So that's very important and

		should be taken …Into cybersecurity terms.. Isolation. If I have 2 or 3 departments inside my, institution, so each one should have, for example, their own network or their own, storage. So if one compromise, the other one does not…if there is an attack, they cannot reach the whole firm, just probably a specific department…They cannot, do literal movement and attack the whole, content… it is a semi anticipation of an attack.
B27	A	If it was misimplemented or someone took advantage of it, it can works against the firm.
B28	B	we're missing, like, good filter technology.
B29	A	collective intelligence platforms that, for example, a company would use, if they get compromised, they can be a nightmare for the whole world. They can't just allow, malicious threat, and they say it's allowed and it can, if I totally depend on them, that's very important point also. I should not be fully dependent on them. I should depend on them partially, but also depend on my internal people. Like, my internal, intelligence… I should also be working internally and doing my own research online and having my own, offline collective intelligence.

Appendix D: Links for transcripts

WeTransfer Link:
https://we.tl/t-x6c2rwmU8c

Dropbox Link:
https://www.dropbox.com/scl/fo/7371df903tds502qvo041/AC3QxMUchtZTOVcpKy2izN0?rlkey=w0pw6ux6a3d70ukw7j9oxv181&st=k50y6ygx&dl=0