UiA University of Agder

Master

To Deceive or not Deceive: Unveiling The Adoption Determinants Of Defensive Cyber Deception in Norwegian Organizations

DAN BOJOVIĆ
JARL TENGESDAL LYGRE

SUPERVISOR
Wael Soliman

University of Agder, 2023
Faculty of Social Science
Department of Information Systems

Obligatorisk gruppeerklæring

Den enkelte student er selv ansvarlig for å sette seg inn i hva som er lovlige hjelpemidler, retningslinjer for bruk av disse og regler om kildebruk. Erklæringen skal bevisstgjøre studentene på deres ansvar og hvilke konsekvenser fusk kan medføre. Manglende erklæring fritar ikke studentene fra sitt ansvar.

1.	Vi erklærer herved at vår besvarelse er vårt eget arbeid, og at vi ikke har brukt andre kilder eller har mottatt annen hjelp enn det som er nevnt i besvarelsen.	Ja
2.	**Vi erklærer videre at denne besvarelsen:** • Ikke har vært brukt til annen eksamen ved annen avdeling/universitet/høgskole innenlands eller utenlands. • Ikke refererer til andres arbeid uten at det er oppgitt. • Ikke refererer til eget tidligere arbeid uten at det er oppgitt. • Har alle referansene oppgitt i litteraturlisten. • Ikke er en kopi, duplikat eller avskrift av andres arbeid eller besvarelse.	Ja
3.	Vi er kjent med at brudd på ovennevnte er å betrakte som fusk og kan medføre annullering av eksamen og utestengelse fra universiteter og høgskoler i Norge, jf. Universitets- og høgskoleloven §§4-7 og 4-8 og Forskrift om eksamen §§ 31.	Ja
4.	Vi er kjent med at alle innleverte oppgaver kan bli plagiatkontrollert.	Ja
5.	Vi er kjent med at Universitetet i Agder vil behandle alle saker hvor det forligger mistanke om fusk etter høgskolens retningslinjer for behandling av saker om fusk.	Ja
6.	Vi har satt oss inn i regler og retningslinjer i bruk av kilder og referanser på biblioteket sine nettsider.	Ja
7.	Vi har i flertall blitt enige om at innsatsen innad i gruppen er merkbart forskjellig og ønsker dermed å vurderes individuelt. Ordinært vurderes alle deltakere i prosjektet samlet.	Nei

Publiseringsavtale

Fullmakt til elektronisk publisering av oppgaven Forfatter(ne) har opphavsrett til oppgaven. Det betyr blant annet enerett til å gjøre verket tilgjengelig for allmennheten (Åndsverkloven. §2).
Oppgaver som er unntatt offentlighet eller taushetsbelagt/konfidensiell vil ikke bli publisert.

Vi gir herved Universitetet i Agder en vederlagsfri rett til å gjøre oppgaven tilgjengelig for elektronisk publisering:	Ja
Er oppgaven båndlagt (konfidensiell)?	Nei
Er oppgaven unntatt offentlighet?	Nei

Acknowledgements

Firstly, we would like to thank our supervisor Wael Soliman for his support throughout the thesis. Giving us valuable insights into our research topic, how we should approach it, how we should structure our thesis and help us stay on track during the thesis. You have been of great help during these months, thank you very much!

Secondly, we would like to give a thanks to our interview participants. The participants took time out of their busy daily schedules to participate in our interviews and share their knowledge with us. We greatly appreciate the help!

Lastly, we would like to thank our families for their support during this master's period. The thesis could not have been completed without your love and support, for that we are very grateful.

Jarl T. Lygre Dan Bojovic

Abstract

Due to the prevailing threat landscape in Norway, it is imperative for organizations to safeguard their infrastructures against cyber threats. One of the technologies that is advantageous against these threats is defensive cyber deception, which is an approach in cyber security that aims to be proactive, to interact with the attackers, trick them, deceive them and use this to the defenders advantage. This type of technology can help organizations defend against sophisticated threat actors that are able to avoid more traditional defensive mechanisms, such as Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS). In order to aid the adoption of defensive cyber deception in Norway, we asked the question: "What affects the adoption of defensive cyber deception in organizations in Norway?". To answer this question, we utilized the Technology, Organization, and Environment (TOE) Framework to identity what factors affect an organization's adoption of defensive cyber deception. Through our use of the framework, we identified eighteen different factors which affect an organization's adoption of defensive cyber deception. These factors are the product of the empirical data analysis from eight different semi-structured interview with individuals from six different organizations in Norway. The main theoretical implications of our research is the introduction of a TOE model for defensive cyber deception, focusing specifically on organizations in Norway as well as contributing with a maturity estimate model for defensive cyber deception. For the practical implications of our research, we have identified seven different benefits that defensive cyber deception provides. We are also contributing to raising the awareness of defensive cyber deception in Norwegian research and we hope that our TOE model can aid organizations that are considering adopting the technology. We hope that these implications and contributions can act as a spark for both the adoption of defensive cyber deception in organizations as well as the start of a new wave for the cyber security researchers within Norway.

Keywords: Cyber Security, Defensive Cyber Deception, TOE Framework, Adoption

Contents

List of Figures

List of Tables

Chapter 1

Introduction

The threat landscape for 2023 in Norway has been changed dramatically from the prior years. Due to the war between Ukraine and Russia, Norway has become Europe's lead exporter of gas, and the sabotage of the Nord-Stream pipeline and sightings of drones at Norwegian oil and energy installations has shown that cyber security is becoming more and more important (NSM, 2023). According to NSM (2023), they have seen a tripling of cyber attacks against Norwegian organizations from 2019-2021, where the three most common types of attacks were denial of service attacks, phishing attacks and mapping activity from the threat actors.

In 2022 it took an average of 207 days to identify a breach, this means that an attacker could dwell within your systems for 207 days, and the average time to contain a breach was 70 days in 2022. In other words, if a breach happened, it could take up to 277 days to successfully contain a data breach (Ponemon-Institute, 2022). For context, if an attacker breached your defenses on 1st January, it would take on average until 4th October to identify and contain the breach, which is an unacceptable amount of time (Ponemon-Institute, 2022). Additionally, the average cost of a data breach in Scandinavia in 2022 was $2.08M (Ponemon-Institute, 2022). Most of the time, organizations rely on traditional detection and prevention capabilities, such as Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), which can easily be avoided by skilled attackers (Islam and Al-Shaer, 2020).

Defensive cyber deception is a promising approach (Islam and Al-Shaer, 2020; Islam, Dutta, et al., 2021; Sajid et al., 2020) that provides defenders with early detection, which again detects an in-network threat and gives defenders faster response and reduces the dwell time of an attacker, and the cost of a breach significantly (Steingartner et al., 2021). The research conducted by K. Ferguson-Walter et al. (2018) yielded findings regarding the effectiveness and outcomes of defensive cyber deception, revealing that decoys impeded attacker forward progress, reduced attacker success, wasted attacker resources, and increased detectability (K. J. Ferguson-Walter et al., 2023).

1.1 Rationale and motivation

The exponential growth in the number of connected devices has significantly increased the attack surface of cyber systems, making them more vulnerable to cyber security breaches (Huang et al., 2022). Traditional defense-in-depth mechanisms, such as anti-virus, IDS, and firewalls (Heckman et al., 2015; Steingartner et al., 2021), that adopt a reactive or prevention-only posture, have been rendered inadequate (Heckman et al., 2015; Huang et al., 2022; Steingartner et al., 2021) to combat the sophisticated Advanced Persistent Threats (APTs) that are currently threatening system operations (Heckman et al., 2015). This is true even for the best cyber security architectures (Steingartner et al., 2021). Furthermore, these reactive defenses are complex, prone to false positives, and often fail to detect and

prevent attacks, leading to analyst alert fatigue (Steingartner et al., 2021). Attackers are spending a considerable amount of time inside the network, perpetuating the persistence cycle of privilege escalation, internal reconnaissance, lateral movement, and maintaining a presence (Steingartner et al., 2021), as the concept of a perimeter is no longer applicable. As a result, organizations are seeking new tools and programs for early detection of such attacks (Steingartner et al., 2021). To address these contemporary challenges, alternative active defense mechanisms, such as defensive cyber deception, have been proposed as a viable approach to protect computer systems by actively hindering and deceiving attackers (Heckman et al., 2015). The simplicity, ease of use, and ability to complement existing cyber security controls (Steingartner et al., 2021) make cyber deception an attractive option. Moreover, cyber deception offers the added benefit of shifting the asymmetry in favor of defenders, which is not achievable with traditional reactive defenses (Steingartner et al., 2021). Deceptive defense mechanisms involve actively deploying deceptive entities to disrupt and derail attacks (Steingartner et al., 2021) while collecting, recording, and reporting on underlying threats through the deliberate exposure of deceptive information (Li et al., 2021). Additionally, cyber deception camouflages target assets (Li et al., 2021), providing internal visibility into the activities of the threat actors while denying them accurate intelligence through misinformation and misdirection (Steingartner et al., 2021). Researchers design and deploy deceptive entities to actively defend and deter APTs without requiring prior knowledge of attacks (Steingartner et al., 2021).

Furthermore, existing literature on defensive cyber deception primarily focus on enhancing or improving its effectiveness, while neglecting the exploration of the factors influencing its adoption. This research gap highlights the lack of comprehension regarding the factors that hinder or promote the adoption of defensive cyber deception. Despite the demonstrated effectiveness and positive outcomes of employing defensive cyber deception, it has not yet been extensively adopted (Mohan et al., 2022). Based on this, we present our research question: "What affects the adoption of defensive cyber deception in organizations in Norway?" as a way to bring more attention to the potential benefits/advantages defensive cyber deception can provide organizations. We also want to find out what factors affect the adoption, so that organizations can more easily see if they are ready, or mature enough to adopt it.

1.2 Research Approach

As we are researching what affects organization's adoption of defensive cyber deception, we are going for a qualitative approach. We are using semi-structured interviews as our method of data collection, as we believe that the insights from cyber security professionals within the organizations hold the key to understanding the factors influencing adoption. To support our thesis, we have done a systematic literature review, where we have gathered research articles regarding the use of defensive cyber deception. We have also gathered supporting literature for the thesis, such as papers on deception theory, maturity models and adoption frameworks. We conducted 8 different interview with 6 organizations between March and April 2023, resulting in the empirical data you, the reader, will see further down in the thesis. The interviews consisted of us, the researches, asking predefined questions to the interview participants and improvising questions if we started deviating towards a topic we thought could enrich our empirical data. In around mid February 2023, we decided to use the TOE framework as our theoretical lens for the analyzing of the data we had collected through our semi-structured interviews. The literature review and the gathered empirical data was our theoretical and empirical bedrock for when we tried to answer our research question through our theoretical lens.

1.3 Structure of the thesis

Chapter 1 - Introduction: Gives a brief introduction to the threat landscape Norway is in today, the rationale and motivation behind our research and a introduction of how we have done our research.

Chapter 2 - Background and Related Work: Goes through the literature found during our systematic literature review as well as the supporting literature.

Chapter 3 - Theoretical Lens: Introduces our theoretical lens of choice and argues for why it was chosen.

Chapter 4 - Research Approach: Explains our process throughout the research approach and why we chose to have for example a qualitative approach over a quantitative approach, the ethical considerations for our thesis and so on. It also briefly discusses our maturity estimate model.

Chapter 5 - Results: Here we go through the analyzed empirical data from our data collection as well as present our maturity estimate model and TOE model for defensive cyber deception.

Chapter 6 - Discussion: We discuss the findings presented in the previous chapter and discuss our thesis's theoretical and practical implications as well as the limitations and possibilities for future research.

Chapter 7 - Conclusion: Here we provide a conclusion and closing remarks to our thesis.

Chapter 2

Background and Related Work

In this chapter of the thesis, we present our literature review, discussing our choice of methodology which includes literature identification, screening, quality assessment, data extraction and data analysis. We then discuss the findings and insights we gathered through the review.

2.1 Literature Review

In this section, we will be going through the methodology that we have used for our literature review, as well as presenting the literature that was discovered through this methodology.

2.1.1 Methodology

Systematic literature reviews (SLR) are a means of identifying, evaluating and interpreting all available research relevant to a particular research question, or topic area, or phenomenon of interest (Kitchenham, 2004). One of the reasons one should conduct a systematic literature review is to identify gaps in the existing literature, in order to better understand what areas are lacking in the literature (Kitchenham, 2004).

We have based our literature review process on five main pillars: Identification, Screening, Quality Assessment, Data Extraction and Data analysis. The data analysis here should not be confused with the one in the Research Approach chapter of our thesis. We extracted these five pillars from a paper written by Xiao and Watson (2019) on how to conduct a systematic literature review. It is important to note that this literature review procedure is only done on the "main" literature in our thesis, the literature regarding defensive cyber deception. The rest of the literature, such as the literature regarding deception theory or theoretical frameworks are not included in for example the identification section of this chapter.

2.1.2 Literature Identification

The identification of the literature was done through these "rules" listed as points below:

- The literature has to written in English or Norwegian
- The literature should be released earliest in 2018 and latest in 2023
- The literature should only be gathered through various journals and electric libraries (WebofScience, ProQuest, etc) or snowballed from these journals/libraries
- The literature should be found using our predefined key words regarding the research topic
- The literature should be peer-reviewed

- Literature with several citations from other relevant articles will be prioritized

The literature being in English or Norwegian is mainly due to our, the researches, ability to read and understand the literature. The reasoning for mainly gathering literature between 2018 and 2023 is to ensure that we gather research that is new and relevant. However, there is a lot of research that still is relevant even though it is older than 2018, so we opted to prioritize newer papers, but not completely exclude the older ones. We used the search words "Cyber Deception" and "Defensive Cyber Deception" in our first search for literature through WebofScience, and identified 333 articles based on their title, which we believed could be relevant to our review and thesis.

Identified Literature

Our 12 literature sources used for our data on defensive cyber deception can be found in Table C.1 in Appendix C.

2.1.3 Screening for Inclusion & Quality Assessment

We decided to merge screening and quality assessment, as we felt like these were quite similar and both were mentioned in our flowchart of the literature review, which can be seen in Figure 2.1. After we had identified the first 333 articles through our literature identification, we began the screening for inclusion. As seen in the figure, we first screened the literature based on the abstract, leaving us with 56 papers. After skimming through these 56 articles, 26 were found eligible to use in our thesis. We then snowballed using these 26 papers and found 9 more, leaving us at 35 papers found. Then after the quality assessment, which included a thorough read through of the papers by both researches, we decided on the final 13 papers that we are using as the base for our literature review on defensive cyber deception. As mentioned previously, these 13 papers are only about defensive cyber deception and we have other literature that act as supportive literature which did not go through this screening process.

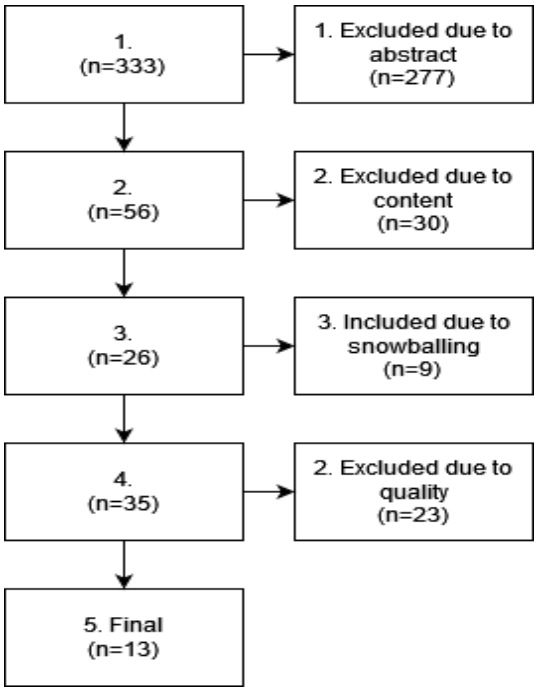

Figure 2.1: Literature review procedure

2.1.4 Data Extraction & Analysis

The data we extracted from the papers were: The name of the paper, authors, the general theme, the year it was published, and the data we deemed relevant to our study on defensive cyber deception. This data could be anything from frameworks, techniques or quotes that we felt would strengthen our literature review. The data we extracted was analyzed in NVIVO, using coding as our tool of choice. The extraction of data was done separately by the two researches, but there was clear discussion and communication on what should be a part of the literature findings section and what should be excluded from it.

2.2 Literature findings

This section aims to present a comprehensive overview of the literature on the topic of cyber deception. The literature review will commence with an examination of the theory of deception, exploring the historical use of deception in the Old Testament to modern-day tactics. Subsequently, we will delve into the fundamental principles of deception in cyber security.

We will delve into the ways in which attackers have utilized cyber deception to manipulate and deceive defenders, highlighting the dangers of these malicious techniques. The literature review will then shift its focus towards defensive cyber deception, outlining the fundamental principles of deception in cyber security. Specifically, we will examine various methods employed in the field of OT/IT, including SCADA/Cyber-physical deception, network deception, and malware deception. We will also explore the benefits that defensive cyber deception provides.

Overall, the literature review aims to provide a comprehensive understanding of the theory and practice of cyber deception, examining its use in both offensive and defensive contexts. By analyzing the existing literature, we hope to give the reader a comprehensible understanding of what cyber deception is and how organizations can utilize it for their own benefits.

The Figure 2.2 is a road-map that illustrates the literature findings for cyber deception. The theoretical lens is also included in the road-map, with a dedicated chapter subsequent to the literature findings:

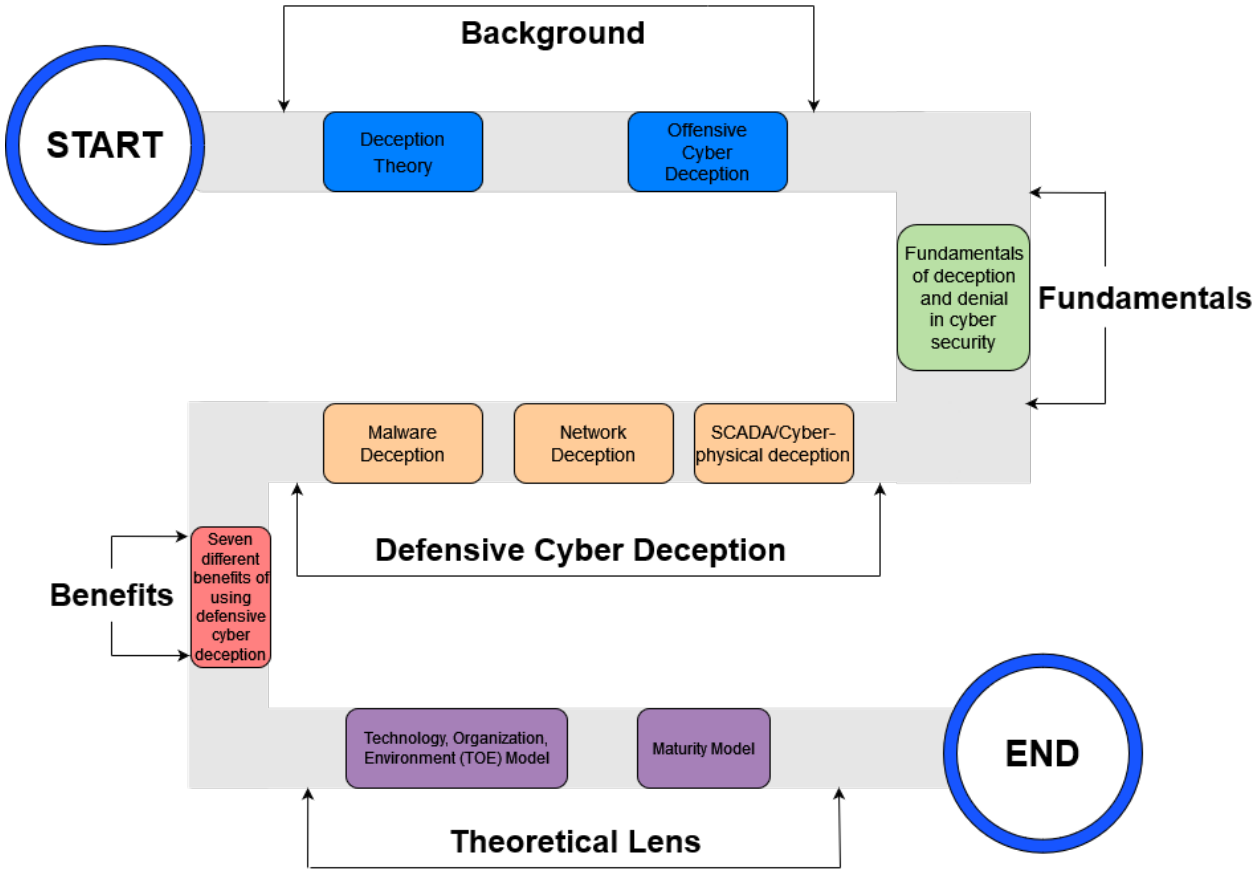

Figure 2.2: Literature findings road-map

2.2.1 Deception Theory

Deception can be found within more things than one would think, even animals and plants use deception to their advantage (Searcy and Nowicki, 2010; Amotz Zahavi and Avishag Zahavi, 1999), and written records on deception against humans can be found as far back in the Old Testament when Eve was tricked by the snake in the Garden Of Eden (Rue et al., 1994).

In their book, Rowe and Rrushi (2016) present their spectrum of deception which includes white lies, self-deception, humorous lies and much more. This shows just how broad the spectrum of deception is and how much it affects us in our daily lives. In the same book, they state the purpose of deception is to cause the deceived to subsequently act on those false beliefs to benefit the deceiver.

If we also take a look at how Buller and Burgoon (1996) defines deception: "A message knowingly transmitted by a sender to foster a false belief or conclusion by the receiver." It correlates well to what we have learned about defensive cyber deception throughout our research. The theory of deception is the same, however the means to achieve and utilize the deception differs.

We can understand deception as something very broad, in our case, deception is made up of two actors, the deceiver and the deceived. Our perception of deception is quite similar to how Cranford et al. (2021) view it. They state that deception typically involves one agent that is presenting truthful or false information to gain an advantage over an opponent. What is special in our case is that it does not matter if the attacker knows it is being deceived,

as long as the deceptive techniques are plenty and well thought out, the defender should be able to get an advantage in their interaction. This is quite similar to how deception is used in warfare.

An example of deception in warfare comes from the popular Strategist Sun Tzu's Art of War, in which Tzu states "All warfare is based on deception." Tzu also mentions deceiving enemy spies openly, making them deliver untrue reports directly to the enemy. There is also a more modern example of deception presented by Steingartner et al. (2021), where the authors propose a more modern way to utilize deception in warfare, which is defensive cyber deception. Defensive cyber deception will be discussed in greater detail later in the chapter.

2.2.2 Fundamentals of deception and denial in cyber security

Before diving into the practicality of cyber deception, we will first introduce the fundamentals of deception in cyber security. In the book "*Cyber Denial, Deception, and Counter Deception*" by Heckman et al. (2015), the authors introduce a traditional framework known as the Deception & Denial (D&D) methods matrix, which provides a basis for describing the fundamental concepts of D&D in the physical world. The underlying objects of these D&D methods, as depicted in Figure 2.3, include both facts and fictions that are either revealed through deception methods or concealed through denial methods (Heckman et al., 2015). These facts and fictions may be either information or physical entities. The term *non-essential friendly information* (NEFI) refers to the fact that the deceiver chooses to reveal to the target. *Essential elements of friendly information* (EEFI), also known as dissimulation, are the factual information that the defender's cyber-D&D team must protect, while the *essential elements of deception information* (EEDI), also known as simulation, are the key fictions that the defender's cyber-D&D team must reveal to the target of the deception. Finally, the fictions that the deceiver must keep hidden from the target are referred to as *non-disclosable deception information* (NDDI) (Heckman et al., 2015).

Traditional denial and deception (D&D) techniques can be adapted to the domain of cyber security, although some adaptation of these techniques may be required in order to translate them from the physical to the virtual world. To further elaborate on the cyber-D&D methods matrix, Figure 2.3 presents a set of high-level cyber-D&D techniques, which are a combination of two or more tactics, and are organized based on whether they involve facts or fictions and whether they are revealed through deception methods or concealed through denial methods (Heckman et al., 2015).

	D&D methods (Traditional)			**D&D methods (Cyber Security)**	
Deception Objects	**Deception:** Mislead (M)-type methods revealing	**Denial:** Ambiguity (A)-type methods conecealing	**Deception Objects**	**Deception:** Mislead (M)-type methods revealing	**Denial:** Ambiguity (A)-type methods conecealing
Facts	*Reveal Facts: NEFI* • Reveal true information on the target • Reveal true physical entities, events, or processes to the target	*Conceal Facts: EEFI* • Conceal true information from the target • Conceal true physical entities, event, or processes from the target	*Facts*	*Reveal Facts: NEFI* • Publish true network information • Allow disclosure of real files • Reveal misleading compromise details • Selectively remediate intrusion	*Conceal Facts: EEFI* • Deny access to system resources • Hide software using stealth methods • Reroute network traffic • Silently intercept network traffic
Fictions	*Reveal Fictions: EEDI* • Reveal to the target information known to be untrue • Reveal to the target physical entities, events, or processes known to be untrue	*Conceal Fictions: NDDI* • Conceal to the target information known to be untrue • Conceal to the target physical entities, events, or processes known to be untrue	*Fictions*	*Reveal Fictions: EEDI* • Misrepresent intent of software • Modify network traffic • Expose fictional systems Allow disclosure of fictional information	*Conceal Fictions: NDDI* • Hide simulated information on honeypots • Keep deceptive security operations a secret • Allow partial enumeration of fictional files

Figure 2.3: Translated D&D methods matrix to traditional (left) & cyber security (right) adapted from (Heckman et al., 2015)

The following section presents an organized discussion of the four quadrants of the D&D methods matrix, elaborating on each of the high-level cyber-D&D techniques outlined in Figure 2.3. Each subsection provides insights into the potential implementation of D&D techniques in the domain of cyber security, with a specific focus on the application of these techniques in incident response scenarios within the context of a deception operation.

Reveal Facts (NEFI)

Revealing factual information to potential adversaries can serve as an effective mechanism for detecting malicious actors. According to Bennett and Waltz (2007), by selectively **publishing limited amounts of true information** about their network, personnel, and mission, defenders can attract the attention of malicious actors or reduce their sensitivity to defensive network surveillance. As an example, defender deception tactics may encompass revealing employee attendance at forthcoming conferences through the company blog or public mailing list. This may prompt malicious actors to modify their tactics, for instance by sending a seemingly follow-up message to an employee with regards to a session at the conference. The resulting information can then be used to differentiate targeted spear phishing attempts from untargeted malicious email (Heckman et al., 2015). Phishing will be explained in more detail later in the chapter.

Defenders can create a simulated environment such as a virtual honeypot, which offer baits in hope that the adversary will mistake honeypots for regular hosts/servers that will trigger an alarm if interacted with (Chiang, Venkatesan, et al., 2018). Honeypots entice malicious actors to intrude and potentially expose their tactics and objectives. The deception environment is designed to appear as a genuine network by **disclosing real**, non-sensitive documents, or previously released information, in order to create a sense of authenticity (Heckman et al., 2015).

Defenders can demonstrate their deception capabilities **by revealing them** in a manner that causes their adversary to question the validity of information obtained from previous intrusions. This can be achieved through building a virtual honeypot environment that closely resembles the actual environment of the organization, including accurate configurations of usernames, email accounts, software registration, and server names. If discovered, the duplicated data may cause malicious actors to doubt the authenticity of both previous and future intrusion data, and make them cautious when engaging with seemingly compromised systems. Sophisticated defenders often integrate deception capability signatures into their production networks, creating further skepticism in the event of a real compromise (Heckman et al., 2015).

The defenders must consider various dimensions of the impact of deception tactics. For instance, the dissemination of information regarding a network intrusion can harm an organization's reputation and credibility. However, by effectively **emphasizing the organization's robust security measures**, this apparent vulnerability can serve as a deterrent for future intrusion attempts. The dissemination of information regarding an intrusion such as "unverified claims of network compromise are being investigated as a matter of routine by teams of internal security specialists" conveys a sense of urgency to the intruders' operations. A successful deception operation can prompt the adversary to reveal their operational methods and support, such as their implants, tools for compromise and enumeration, and command and control (C2) hop points, which they may have kept hidden if they believed they had more time. This tactic is more effective when the planners have a deep understanding of the adversary's open-source intelligence collection capabilities (Heckman et al., 2015).

In alignment with the above-mentioned approach, the use of **overt yet incomplete remediation actions** can stimulate an accelerated pace of operations for intruders. The network defenders typically employ incident response strategies, which involve the isolation and purification of contaminated machines in a systematic manner. However, after the initial contamination, security personnel could choose to remove only a portion of the intruder's access while retaining some aspects intact, in order to enable the malicious actors to observe the remediation activities. This tactic serves to encourage the adversary to reveal additional tactics, techniques, and procedures (TTPs) in their attempts to re-establish their presence in the post-remediation environment (Heckman et al., 2015).

Conceal Facts (EEFI) - Dissimulation
The implementation of proactive defense technologies is rooted in the redirection of adversarial traffic. Techniques such as "sink-holing," which involves routing known malicious DNS requests to non-existent Internet Protocol (IP) addresses or internal sensors, form the foundation of this approach (Heckman et al., 2015). More advanced strategies, such as the use of Software Defined Networking (SDN) to direct adversarial traffic to honeypot systems, are also included in the scope of network deception techniques, which will be explored later in the chapter. Additionally, defenders may choose to deter malicious actors by performing system shutdown or log-off actions, using contrived reasons, as a means of disabling malicious access and revealing false information, instead of concealing actual facts (Heckman et al., 2015).

Reveal Fictions (EEDI) - Simulation

The primary purpose of a honeypot is to be vulnerable to compromise, defenders can use honeypots to deceive attempted intruders by presenting a wholly fake system. Honeypots fall into two categories: low-interaction honeypots that passively respond to malicious actors and high-interaction honeypots that require care and feeding for best results. Low-interaction honeypots are shallow simulations of systems that respond plausibly to attempted compromise. (Heckman et al., 2015).

Benefits of low-interaction honeypots include flexible deployment and the ability to gather information on malicious actors without the risk of compromising real systems. These honeypots have proven effective against relatively unsophisticated actors who rely on automated exploitation scripts but does not necessarily possess the technical ability to discover the deceptive environment. Integrating low-interaction honeypots into production networks by re-allocating unused IP space gives an organization visibility into attempts to map and exploit hosts on their internal network (Heckman et al., 2015).

In contrast, high-interaction honeypots offer a deeper level of simulation than the minimally implemented services intended to thwart automated tools. These honeypots seek to deceive a live adversary by presenting a range of services and vulnerable machines. Successful deployment enables network defenders to collect data on how malicious actors behave in the latter phases of an intrusion (Heckman et al., 2015).

High-interaction honeypots require regular monitoring by network defenders, who should add artifacts over time to take advantage of changing adversary interests. Typically, defenders create plausible documents, emails, and user activity prior to launching a high-interaction honeypot. These so-called honeytoken documents need not be fully backstopped, but should be interesting to the adversary in question. Tracking honeytokens allows an organization to discover leaks or adversary distribution methods. As an example, if a malicious actor steals a fake list of email addresses during a deception operation, those emails may be subject to bulk public disclosure or be re-used to send phishing messages to the fake users. Tools such as pastycake or Google Alerts can monitor popular distribution sites to detect public

exposure of the "stolen" documents, and organizations can perform additional monitoring on the "stolen" email accounts (Heckman et al., 2015).

The creation of fictional information, or honeytokens, such as fake user accounts, requires the defending organization to add them to its phone directory, email system, and employee domain. Organizations must treat any attempt to interact with these accounts as very suspicious, and investigate them immediately. On a production network, these accounts can be added to groups without dangerous privileges and have logon scripts that prevent abuse. As a proactive measure, organizations can use decoy email addresses for high-value targets such as executives or system administrators. Email addresses disclosed to external parties can be monitored for phishing attempts without affecting internal communications (Heckman et al., 2015).

Conceal Fictions (NDDI)

Deceptive tactics have become a popular approach for network defenders to mitigate cyber security threats. One such technique involves the planting of fictional but inaccessible documents that can entice malicious actors without risking disclosure. For example, defenders may create a document, disguised as a planned business acquisition, containing a random collection of bytes presented as an encrypted file, which can attract both external attackers and malicious insiders who have already breached perimeter security. Discoverable metadata about the file can also enhance its perceived value, such as indicating that it was authored by executives or well-known engineers (Heckman et al., 2015).

In addition, defenders may craft documents in highly technical or domain-specific language, which can prompt a malicious actor to upload them to their server, providing valuable information on their collection requirements and infrastructure. To prove the compromise of intellectual property, defenders can implant watermarks in these files (Heckman et al., 2015).

For proprietors of secured and protected credit card databases, including a sizable percentage of fictional "fluorescent" identities and account numbers that are designed to report any attempted use as fraud, can help prevent unauthorized access. This method can also summon security for physical transactions, honor transactions for cyber transactions while reporting the use, and install covert tracking and beaconing software on the attacker's machine via a clickable purchase link. These fictitious accounts are concealed and protected and only work against the attacker if obtained illegally (Heckman et al., 2015).

To effectively conceal the deception, defenders configure honeypots to return tampered values in response to system commands such as "uptime" or "systeminfo," enhancing plausibility and concealing the deceptive nature of the environment. To create a fake honeypot, defenders construct a real system that appears to have the known characteristics of a honeypot system (Rowe, 2007), and systems can appear as poorly concealed pieces of low-interaction emulation software when queried in certain ways (Heckman et al., 2015).

With the fundamentals out of the way, we will now introduce how attackers use deception to reach their goals and how the research of cyber deception may be used as a defensive tool in OT/IT systems.

2.2.3 Offensive Cyber Deception

The most commonly known offensive cyber deception used by attackers is phishing, which falls under the term social engineering, which describes a class of computer hacking that targets the user of the system rather than the hardware or software. It is a proven and viable

vector that includes techniques like phishing, pharming, and persuasion (Skarda et al., 2008). Attackers that conduct a phishing attack use psychological manipulation of individuals into disclosing information (Alkhalil et al., 2021). Phishing makes up for 33% of all cyber attacks against organizations and remains the leading infection vector, identified in 41% of incidents as of 2023 (IBM, 2023). Phishing attacks is a tactic that often relies on enticing users to click on hyperlinks within emails or downloading files attached to the fraudulent email. The main objective of this technique is to redirect users to fraudulent websites that aim to collect confidential data, including banking credentials and login details, or to install malware onto the user's device. However, compromising a legitimate website, for example, through the embedding of malware, or tampering with the Domain Name System (DNS) that maps domain names to their corresponding IP addresses, is considerably more challenging than creating a new fake website. As a result, most phishing attacks lure users to click on hyperlinks that direct them to the attacker's URL (Butavicius et al., 2022).

2.2.4 Defensive Cyber Deception

SCADA/Cyber-physical Deception

The networked critical infrastructures (NCIs) such as power grids and Supervisory Control and Data Acquisition (SCADA) are crucial for the functioning of modern society. However, they are also highly vulnerable to cyber attacks, which can have devastating consequences. Traditional cyber security measures, such as firewalls and intrusion detection systems, are not always effective against sophisticated attackers (Ajmal et al., 2021; Cifranic et al., 2020). An approach to combat sophisticated attacks on NCIs, such as SCADA and Intelligent Electronic Devices (IEDs), has been studied by several researchers by placing deception mechanisms within the production network (Ajmal et al., 2021; Cifranic et al., 2020; Mashima, 2022).

In the article by Cifranic et al. (2020), the authors argue that cyber deception can be a more effective approach to defending NCIs, and hence propose a cyber deception framework called "Decepti-SCADA" that can be used to actively defend NCIs against cyber attacks. The two main components of the Decepti-SCADA framework are the Decepti-Box and ELKSUR and is illustrated in Figure 2.4.

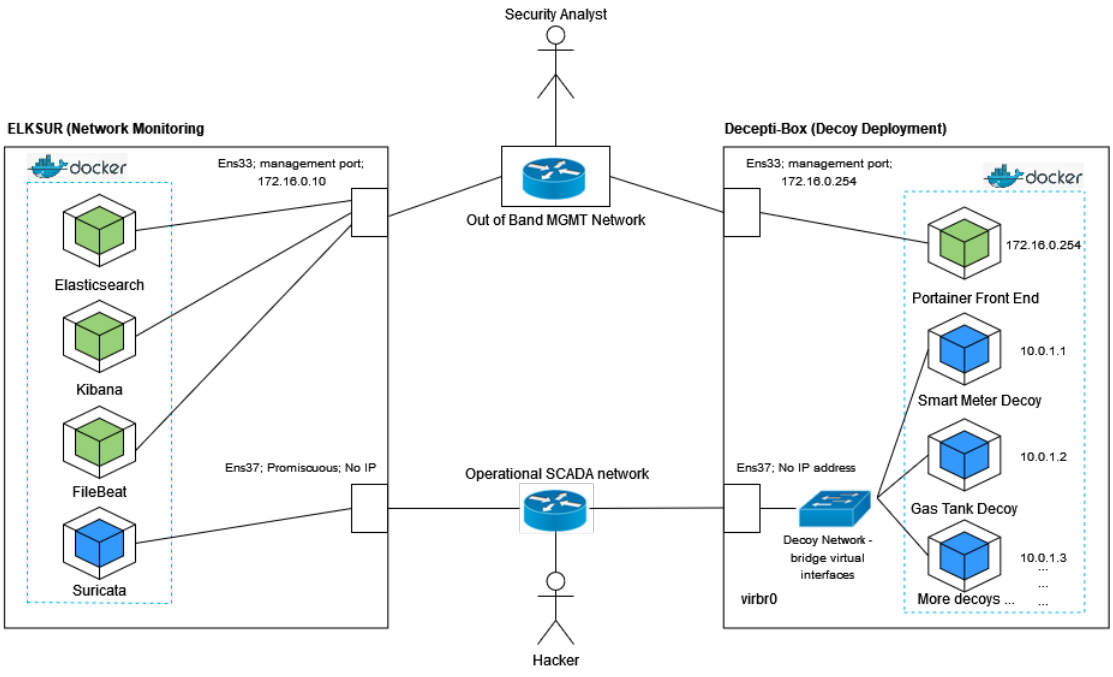

Figure 2.4: Decepti-SCADA framework adapted from Cifranic et al. (2020)

The Decepti-Box is a specialized hardware component implemented in the Decepti-SCADA system to facilitate cyber deception in critical infrastructure. Its purpose is to mimic the behavior of genuine control system devices, with the aim of luring attackers towards a decoy network, while keeping the actual network secure (Cifranic et al., 2020). This approach was also studied by Ajmal et al. (2021), but instead of using the Decepti-SCADA, they utilized decoy farms which mimicked Programmable Logic Controllers (PLCs) in conjunction with threat hunting intelligence for dynamic purposes. Decepti-SCADA also has the capability of identifying and alerting cyber security personnel on any attacks directed at the decoy network (Ajmal et al., 2021). The device comprises of a Raspberry Pi computer, as well as diverse modules, including network and serial communication modules, which allow it to connect with the industrial control system components (Ajmal et al., 2021). The Decepti-Box is configured and managed via the ELKSUR. ELKSUR consists of four main components, which are:

1. Kibana: A front-end web Graphical User Interface (GUI) that serves as the user-facing component that provides access to the interactions between the deployed decoys and the network. It allows analysts to monitor and evaluate potential intrusions by assessing whether an attacker is interacting with a SCADA Decoy.

2. Suricata: A network-based intrusion detection system (IDS) used in this context is an open-source software that records alerts based on predefined signatures, specifically those related to interactions with decoys. The log file is called fast.log

3. Filebeat: A host-based agent used to relay Suricata fast.log logs to Elasticsearch

4. Elasticsearch: A search engine that is utilized to gather and index received data, and is used to receive parsed fast.log data, which is then visualized through Kibana for comprehensive analytics and visualization of the collected data.

(Cifranic et al., 2020)

Smart power grid systems have also become a desirable target of cyber attacks. The power grid infrastructure is considered the backbone of other critical infrastructures, thereby making it a prime target for attackers, including state-sponsored hackers and cyber terrorists, who aim to undermine the availability and stability of power grid operations (Mashima, 2022). Despite significant efforts by industry and academia to improve cyber security for critical infrastructure, several real-world incidents have occurred in the past decade, some of which have nearly resulted in significant disasters such as the destruction of nuclear plants, while others have caused widespread power outages (Mashima, 2022). Multiple cyber security solutions have been proposed by both academia and industry to safeguard critical infrastructure, such as the power grid. The International Electrotechnical Commission (IEC) has introduced IEC 62351, IEC 61850 and IEC 60870-5-104 standards to outline security specifications for communication protocols. Additionally, cyber security technologies have been proposed, ranging from intrusion detection systems to remote attestation (Mashima, 2022). However, Tan et al. (2019) notes that no single solution is perfect, and it is beneficial to use multiple complementary cyber security solutions for a defense in depth approach. Deception technologies, using decoy devices and networks, are gaining attention as an additional layer of defense (Mashima, 2022).

DecIED is a practical and scalable in-network based deception technique designed for the defense of IEC 61850-compliant smart grid systems, and is illustrated in Figure 2.5. By using decoy systems, DecIED can implement a large number of deception/decoy devices that mimic the behavior of real IEDs and other SCADA devices (Yang et al., 2020). This technique aims to lure attackers into a "deception zone" by pretending to be a real IEC 61850 compliant IED that deploys decoy devices and data within the substation network.

The decoys consist of fake controllers, HMIs (Human Machine Interfaces), and PLCs that mimic the behavior of legitimate devices. DecIED detects and records attacker activity when they interact with decoys and generates alerts that can be used to identify and respond to the attack. In addition, DecIED includes a management console that enables administrators to configure and monitor the deployment of decoys and view and analyze attack data. This approach offers a way to detect and respond to attacks without negatively impacting the normal and legitimate operation of real IEDs and other SCADA devices (Mashima, 2022).

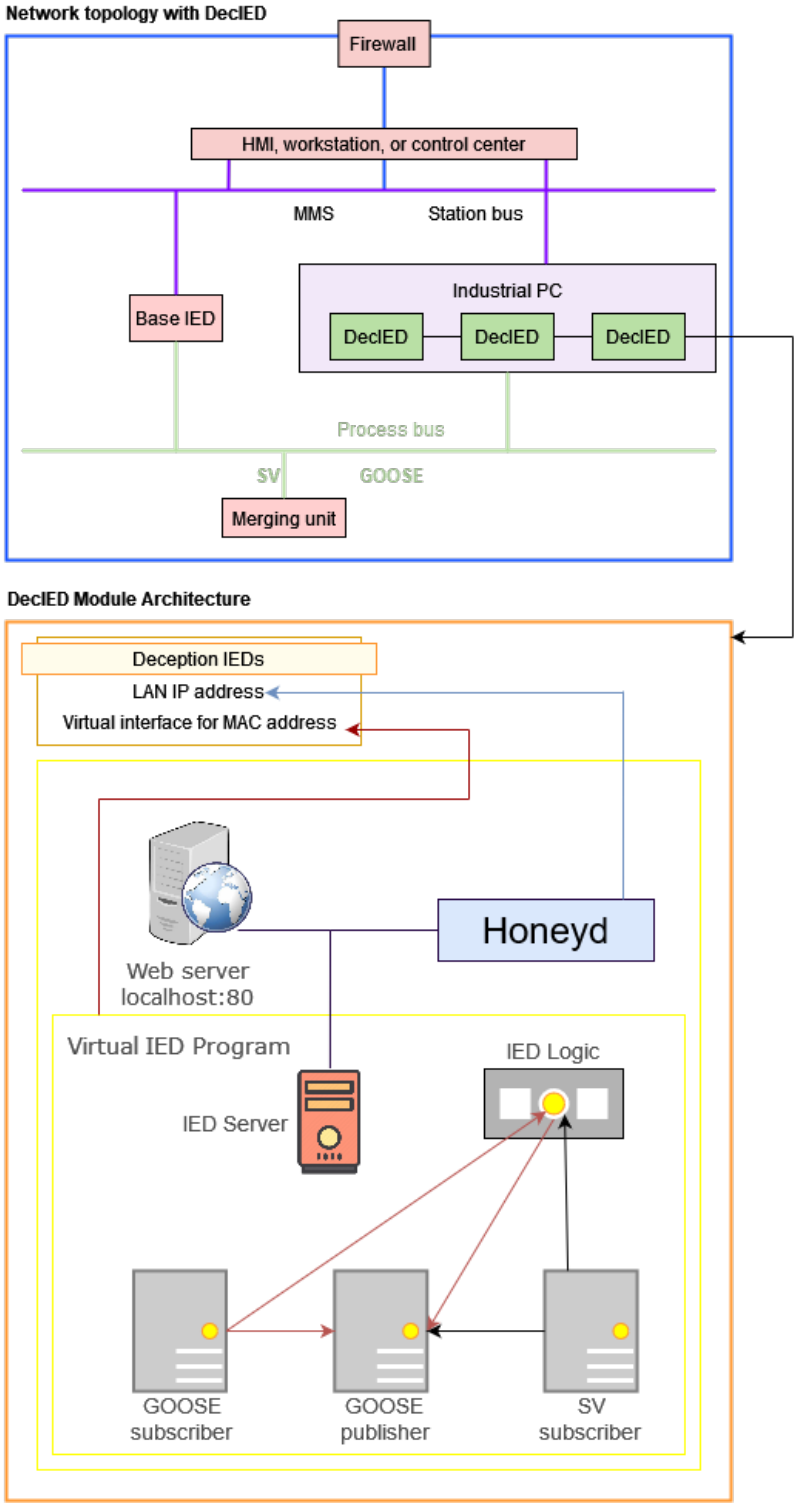

Figure 2.5: DecIED architecture adapted from Yang et al. (2020)

Network Deception

The concept of a perimeter as we know it is inadequate and the battle against cyber-crime has moved inside the network (Steingartner et al., 2021). Attackers spend the most time inside the network in the persistence cycle of privilege escalation, internal reconnaissance, lateral movement, and maintaining a presence (Steingartner et al., 2021), and deception excels at providing internal visibility to such activities while denying accurate intelligence to the threat actor through misinformation and misdirection (Steingartner et al., 2021), hence network deception has been a popular research topic.

SDN has been a popular research area to enable deception within the network. The article by Chiang, Gottlieb, et al. (2016) introduces an Adaptive Cyber Deception System (ACyDS) that leverages SDN technologies to enable cyber deception in an enterprise network setting that allows defenders to dynamically manipulate network traffic and create virtual network topologies that mimic the real network. In the present network design, the network forwarding is generally based on destination IP addresses and is only bound to a handful of routing protocols, restraining the packet forwarding decisions. Chiang, Gottlieb, et al. (2016) argues that SDN devices can be used as a centralized controller for network forwarding, which removes the restrains from normal routing protocols used today, which again allows more flexible, scalable, and dynamic network infrastructure. This is because in an SDN environment, network devices (such as switches and routers) are programmable, and the forwarding decisions are made by a controller that has a global view of the network topology, which makes is possible to change the destination IP on-the-fly. In other words, SDN separates the network control plane from the network forwarding plane in order to simplify the functions of the networking forwarding plane and allow the control plane to "program" forwarding plane functions as desired (Chiang, Gottlieb, et al., 2016). OpenFlow is a communication protocol that enables the communication between the SDN controllers and the SDN switches, and is widely supported by the SDN community. OpenFlow defines messages sent between SDN controllers and SDN switches, and expected behaviors of recipient upon receiving messages (Chiang, Gottlieb, et al., 2016). In ACyDS, there is no need to deploy many static honeypots, as all suspicious access to nodes not permitted by access policies on the SDN switches can be redirected to a small set of high-interaction honeypots (interactive honeypots that mimics real devices/hosts on the production network) for further monitoring. The freedom of dynamically re-routing the network traffic is possible owing to the two-way IP address translation capability, eliminating the need to pre-plan and pre-deploy honeypots at fixed IP addresses, and misleads attackers (Chiang, Venkatesan, et al., 2018).

The two-way IP address translation technique is used to differentiate between legitimate and deceptive traffic. The SDN controller defines rules that determine whether network traffic is legitimate or malicious. Legitimate traffic is allowed to pass through without any alteration to its destination IP address, while traffic deemed as malicious by the SDN controller is redirected to a honeynet (a decoy network consisting of several honeypots) for further inspection. To create the illusion of successful compromise, the honeynet can generate fabricated responses to the attacker's requests which will be forwarded back to the attacker by the SDN controllers, which is known as "response-driven deception". This helps to deceive attackers into believing that they have successfully breached the actual production systems and may cause them to waste valuable time and resources attempting to exploit the fake environment (Chiang, Venkatesan, et al., 2018).

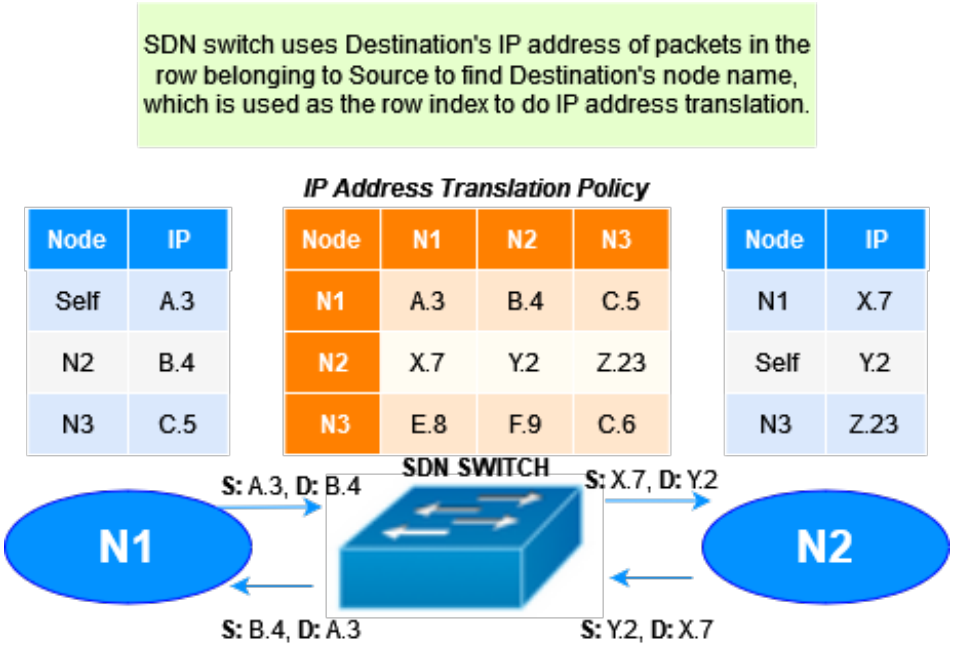

Figure 2.6: Example of SDN IP address translation adapted from Chiang, Venkatesan, et al. (2018)

If a legitimate host in the network is compromised, the SDN approach may not be effective in preventing the adversary from probing the network. This is because the adversary is using a legitimate host to carry out their activities, and the SDN controller cannot differentiate between legitimate and malicious activities coming from the same host. However, the SDN controller can still detect and respond to malicious activities that are identified as such based on the predefined rules in the SDN controller made by the defender, even if they originate from a legitimate host. The predefined rules are various characteristics of the traffic, such as the source and destination IP addresses, the type of protocol being used, and the content of the packets. Therefore, while the SDN approach may not prevent all attacks, it can still provide an additional layer of defense against some types of attacks (Chiang, Venkatesan, et al., 2018).

Shimanaka et al. (2019) proposes a deception scheme that also leverages SDN technology, specifically OpenFlow-enabled switches and controllers, to facilitate deception. This approach enables packet information to be rewritten when a compromise is detected on the production network, resulting in the redirection of each flow into the deception network. The deception network is an exact replica of the production network, utilizing the same IP addresses for devices in the production network as those in the deception network. The only distinguishable difference between the two is the use of different MAC addresses (Shimanaka et al., 2019).

In their paper, Islam and Al-Shaer (2020) present the Active Deception Framework (ADF), which provides cyber defenders with a powerful tool for the development and implementation of adaptive cyber deception techniques. This framework offers a development environment that allows the creation and customization of deception scenarios, including decoy systems, counterfeit documents, and other deceptive tactics that can mislead attackers and detect their actions. The architecture of the ADF is designed to be flexible and extensible, utilizing a modular framework that is built on top of a Java Virtual Machine (JVM). The ADF is composed of several distinct components, including a scenario editor, a deception engine, and a set of agents that can be distributed across networked systems. The scenario editor provides

a drag-and-drop interface that enables the creation and customization of deception scenarios in a user-friendly manner. The deception engine is responsible for managing the deployment of decoys and other deceptive techniques in response to attacks. The agents serve as the intermediary between the deception engine and the networked systems, communicating with the deception engine and reporting on the behavior of attackers (Islam and Al-Shaer, 2020).

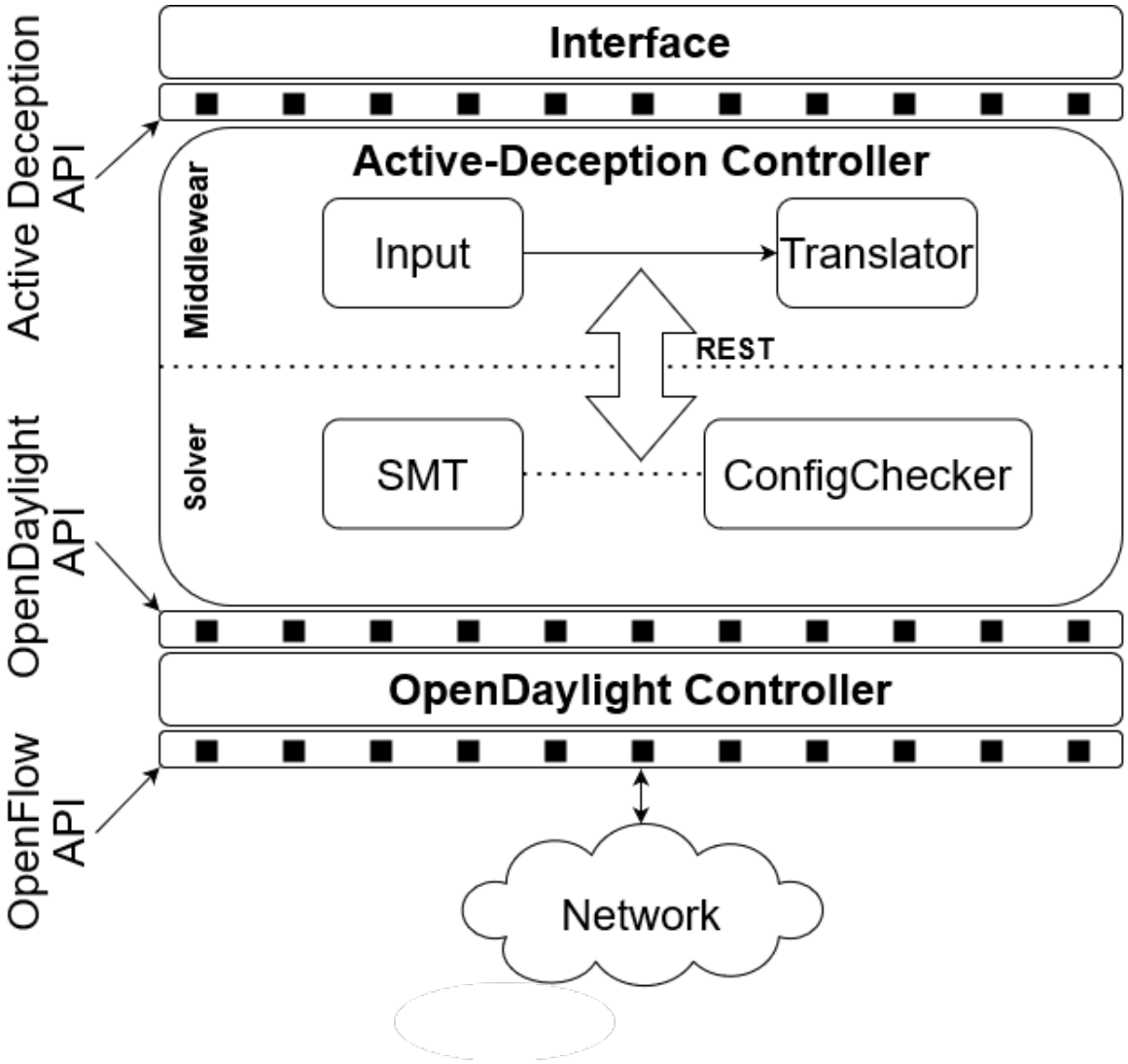

Figure 2.7: Active Defense Framework (ADF) adapted from Islam and Al-Shaer (2020)

ADF has a lot of sensors that observe adversary actions in order to analyze their attack behavior, capabilities, and predict its intention. The sensors collect these observations from resources such as hosts, IP addresses, operative systems (OS), services, switches, links, and much more. The sensor uses all this collected data to build a report, and by using this report the decision-making process deduces the ideal deception goals from deflection, depletion, distortion, or discovery. Furthermore, in the planning process, an optimal set of defensive actions has been chosen to be deployed by the deception engine. This paper will not give an extensive explanation of the ADF framework illustrated in Figure 2.7, but if there is a personal interest, the reader can visit Islam and Al-Shaer (2020) paper and go to Section III for further details. Essentially, the interface provides an easy way to play with the deception API to build complex deception planning, the Active Deception Controller (ADC) is the central orchestrator that handles the end-to-end processing of the cyber deception from initiation by the interface to the safe deployment in the network, and lastly the OpenDaylight Controller is a software-defined networking controller that implements the deception into the network, which is handled by the ADC (Islam and Al-Shaer, 2020).

Malware Deception

If an organization is subjected to a ransomware attack, it can have a devastating impact as we have seen by the Hydro case in Norway (Briggs, 2019). In this section we will present research findings on how cyber deception may strengthen an organizations resilience against malware attacks, such as ransomware. The article by Sajid et al. (2020) highlights the limitations of traditional static analysis methods in effectively detecting modern malware within networks. To address this issue, the authors propose a more dynamic approach to detecting and deceiving malware already in production networks. Specifically, the authors describe the development of a prototype system called DodgeTron, designed to detect and deceive attackers proactively, rather than solely reacting to attacks that have already taken place (Sajid et al., 2020).

DodgeTron is divided into four agents (detection agent, analysis agent, planning agent, and actuating agent) based on their activities and purposes. These four agents operate in two phases: (1) Malware Deception Playbook Construction (MDPC) phase, and (2) Dynamic of Deception Scheme (DoDS) phase (Sajid et al., 2020).

The MDPC phase, also referred to as the offline phase, is concerned with devising a comprehensive strategy to counter malware attacks through the use of deceptive techniques. This phase typically involves the identification of potential attack scenarios and the development of a detailed playbook that outlines specific tactics for detecting and misleading attackers. In this phase, defenders may conduct extensive research to uncover the specific characteristics of malware that may be utilized in attacks, such as the type of malware, target systems and networks, and potential methods of infiltration. This information can then be leveraged to devise tailored deception techniques that enable defenders to identify and isolate malicious software (Sajid et al., 2020).

Sajid et al. (2020) describe the Dynamic of Deception Scheme (DoDS) as the online phase of the Malware Deception Playbook Construction (MDPC) process. The DoDS involves the deployment and execution of the deception tactics outlined in the playbook during a live malware attack. During this phase, defenders monitor the behavior of the attacker and adjust their deception techniques in real-time to mislead and delay the attacker's progress. The DoDS requires defenders to maintain situational awareness and adapt their deception tactics to the evolving threat landscape, while also minimizing the risk of detection by the attacker. This phase is critical for the successful detection and mitigation of malware attacks using deception techniques (Sajid et al., 2020).

Islam, Dutta, et al. (2021) present CHIMERA as a novel approach to enhance cyber security using autonomous planning and orchestration techniques for malware deception. The CHIMERA system is an innovative approach designed to enhance computer system security by identifying and deceiving Advanced Persistent Threats (APTs) in real time. The system utilizes a variety of input sources, including APT techniques derived from the MITRE ATT&CK framework (ATT&CK, 2023), threat reports, and malware API traces from various analyzing tools. The API call traces are mapped to ATT&CK techniques, which are then employed to construct a deception graph. The deception graph is customized using a deception action state space, which is specifically tailored to counter targeted attack actions. The deception graph is subsequently used to generate optimal deception action planning, where the policy definition is given as input, such as APT type (Information Stealer or Ransomware) (Islam, Dutta, et al., 2021).

The CHIMERA system consists of a deception agent, which is installed on the production machine and is responsible for monitoring APT actor activity via IDS/API monitoring. The

agent selects the most appropriate deception action to deceive the attacker's next action when sensor alerts are triggered. In CHIMERA, the deception actions are implemented in the form of system-level API hooking, which retrieves honey resources from a Honey Factory to deceive the attacker (Islam, Dutta, et al., 2021).

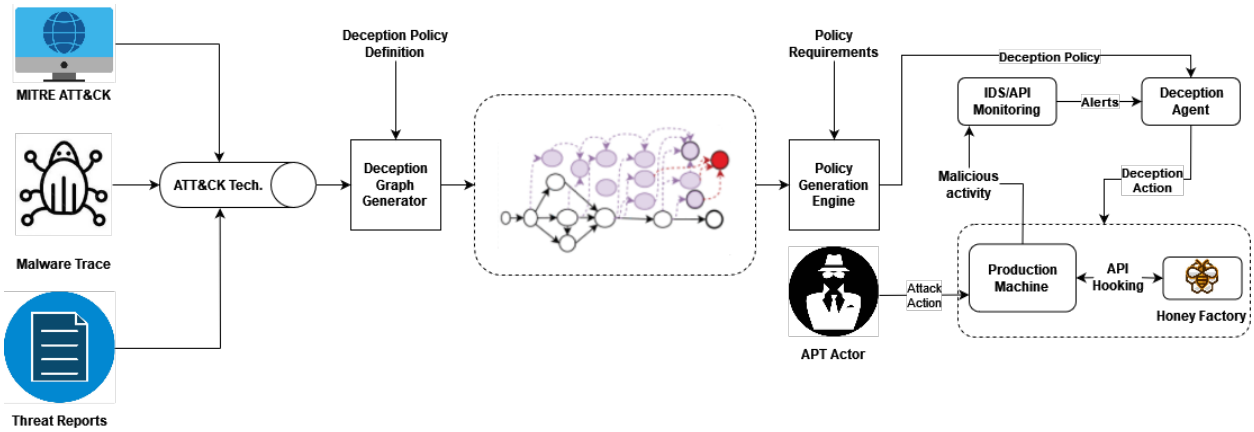

Figure 2.8: CHIMERA Architecture adapted from Islam, Dutta, et al. (2021)

Benefits

Since we now have an understanding of the fundamentals of deception in cyber security, and how cyber deception can be applied as a defensive tool, we will now present the benefits of utilizing defensive cyber deception. The benefits that we have identified from the literature can be broken down into 7 types of benefits, which will be explained throughout this section.

According to the Ponemon Institute's Cost of a Data Breach report for 2022, the average time taken to identify a breach from 2016 to 2022 was 203 days (Ponemon-Institute, 2022). This prolonged duration indicates that attackers can remain undetected within a network for an unacceptably long period. However, defensive cyber deception offers a compelling advantage in the form of **early detection**. Adding defensive cyber deception provides early detection of in-network threats that have successfully bypassed perimeter and antivirus defenses. By deploying defensive cyber deception measures, organizations can intercept and disrupt attackers in the reconnaissance phase of their attack, potentially neutralizing or minimizing the impact of cyber threats (Johansson and Falkman, 2009). Implementing defensive cyber deception enables organizations to identify and respond to breaches before any harm occurs, safeguarding their systems and data.

Defensive cyber deception employs various tactics, such as network decoys and breadcrumbs, to **disrupt** attackers, as mentioned earlier (Steingartner et al., 2021). This strategy introduces uncertainty and distorts the attackers' perception of the network topology (Sun et al., 2020). As a result, attackers are forced to validate information and question their discovery scans to identify genuine targets, effectively slowing down their malicious activities (Steingartner et al., 2021). By implementing defensive cyber deception, organizations can disrupt attackers' progress, impede their movements, and buy valuable time to detect and respond to potential threats.

Depletion is also a benefit from utilizing defensive cyber deception that buys valuable time for defenders to detect and respond to potential threats, which increases attacker resources expenditures while reducing those of the defender (Steingartner et al., 2021). Attackers who attempt to interact with deceptive elements while executing a cyber attack will waste pre-

cious time and resources with an asset that has no corporate production value and does not advance their attack (Steingartner et al., 2021).

Misinformation is an essential benefit from defensive cyber deception, where misleading information is being fed to an attacker which generates a mistaken certainty in the target's mind about what is and what is not real, making the target confident, certain and ready to act - but wrong (Heckman et al., 2015). Defenders use endpoints to deflect port and service scans to decoys for engagement, making it appear to attackers that they are interacting with a production system instead of a decoy (Heckman et al., 2015). This misinformation alters the attacker's understanding of the network, slows them down, and causes them to make mistakes (Steingartner et al., 2021).

The ultimate goal of defensive cyber deception is to lure and **deflect** attackers away from the production system and into an environment that appears to be the real system, but is actually a virtualized and controlled environment, where the attacker's behavior can be monitored and analyzed, thus providing an opportunity to learn the tactics and techniques of the attacker (Islam, Dutta, et al., 2021). This is done by adding decoys as additional components to your systems, and these decoys deflect an attacker away from the real system (Acosta et al., 2020). By placing multiple decoys or traps throughout a protected network, one can divert intruders away from genuine assets (Sun et al., 2020).

Further exploration of the aforementioned attacker tactics and techniques, significant valuable information can be **discovered** by observing attackers in action by utilizing defensive cyber deception. These observations provide significant insight and intelligence into the attacker's TTPs (Liebowitz et al., 2021; Shimanaka et al., 2019), which contributes to defeating the attackers as well as additional opportunities for capability enhancements in the short term (Steingartner et al., 2021). Deception can engage with the adversaries to scrutinize their hidden tactics and techniques, which could lead to the attackers leaking a zero-day attack on the deceptive environment (Islam and Al-Shaer, 2020).

In the field of cyber security, the use of deception as a defensive technique can be an effective way to **deter** against attacks (Steingartner et al., 2021). The deployment of defensive cyber deception creates additional layers of complexity in the attack process of an intruder, increasing the likelihood that the attacker will need to repeat their attacks, thereby reducing the economics of the attack. In particular, as attack processes become more complex, the likelihood of attackers being deterred by the use of deception increases, as they seek to find easier targets that do not employ such defensive measures. Thus, the use of defensive cyber deception can serve as a strong deterrent against attackers, making it a valuable tool in the arsenal (Steingartner et al., 2021).

Chapter 3

Theoretical Lens

The theoretical lens concept is a relatively new concept within research, with the first articles mentioning it between 1990 - 2000, and its use skyrocketing between 2000-2020 (Niederman and March, 2019). The concept describes a way to look at something through a certain point of view, for example, the way a bird looks and perceives the earth versus how a human would. This is a bit of an extreme example, but the point is that we can look at a certain problem or topic from many different perspectives in order to get different conclusions. As we are researching the adoption of defensive cyber deception, there are several frameworks to consider, two of them being: The Technology Acceptance model (TAM) originally proposed by Davis (1989) and the Technology, Organization, and Environment framework proposed by Tornatzky et al. (1990). These two frameworks are the ones we identified as most likely to be used within our area of research, the adoption of technological innovation.

3.1 Related theory and models

A theory that is relevant to mention while on the topic of TAM and TOE is The Diffusion of Innovation Theory (DOI) developed by Rogers (2010). DOI was originally proposed in 1962, but has seen several iterations over the years. The Theory establishes five levels of adopters: The Innovators, Early Adopters, Early Majority, Late Majority and Laggards. This theory is consistent with the TOE framework, as both consider the factors of relative advantage, compatibility and complexity. The theory has been used in various fields of research, such as: Organic agriculture (Simin and Janković, 2014) and health care (Lien and Jiang, 2017). Although its use in the organizational context has been critiqued (Lundblad, 2003) due to there being a gap in research and the use of diffusion of innovation in organizations. Therefore, we will need to explore alternative theoretical frameworks to be a suitable lens for our research.

The Technology Acceptance Model proposed by Venkatesh and Davis (1996) is based on two main variables: Perceived Usefulness (PU) and Perceived Ease of Use (PEOU). These variables are used to measure a person's or individual's acceptance of an information system (Lee et al., 2003). The model has been validated and changed a few times and in 1996, Venkatesh and Davis (1996) proposed the final TAM model. The model has five dimensions: The external variables, perceived usefulness, perceived ease of use, behavioral intention and usage behavior. In a study done by Lee et al. (2003), they identified four categories of information systems that TAM has been used on: Communication systems, general-purpose systems, office systems and specialized business systems. As we discovered that the TAM is primarily used to measure individual's perception of usefulness and ease of use, we will not be using the TAM for our research. We have decided to delve deeper into the TOE model and utilize it as our theoretical lens.

During our research on the applications of the TOE model in the field of IT, we came across several research articles that combine TOE and TAM in order to guide their research on adoption (Chatterjee et al., 2021; Dash and Anusandhan, 2018; Gangwar et al., 2015). The reason for this combination of acceptance/adoption models is discussed in a review by Bryan and Zuva (2021). The authors propose a combination of TAM and TOE to handle the limitation they identified in the TAM model. One of the limitations mentioned was that the TAM model focuses on future behavior and not current behavior.

3.2 TOE Model

We will be using the Technology, Organization, and Environment (TOE) framework proposed by Tornatzky et al. (1990) in their book as our theoretical lens. The TOE framework is a framework that examines the technological, organizational, and environmental contexts that either realizes or discards innovation.

Figure 3.1 is an adaptation of the original TOE model proposed in the framework from 1990. The model focuses on three key aspects, technology, organization and external task environment. External task environment will be referred to as environment in our thesis. The original TOE model primarily focuses on the factors encompassed within the three main aspects when examining an organization's approach to technological innovation decision making, for example government regulation in the environment, availability of the technology and size of the organization. These variables are not set in stone as we have seen several different variables in various papers using TOE.

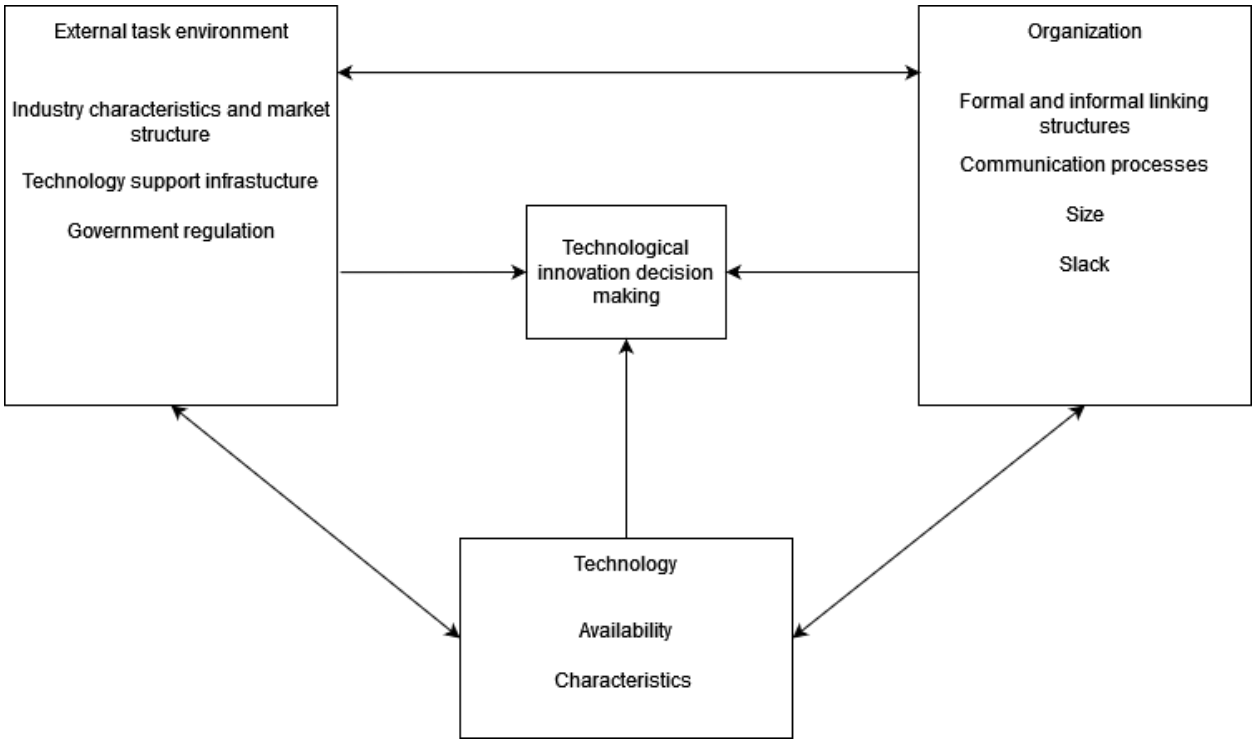

Figure 3.1: Original TOE model adopted from Tornatzky et al. (1990)

The literature has extensively utilized the TOE framework to examine the adoption of IT technologies, with a recent emphasis on cloud computing adoption (Kandil et al., 2018; Tashkandi and Al-Jabri, 2015), block chain adoption (Hanna et al., 2020), and social me-

dia adoption in Small or Medium Enterprises (SOMEs) (Effendi et al., 2020) to name a few. The TOE factors mentioned in these papers vary, three of the four mention relative advantage, which is a part of the technology aspect of TOE. The relative advantage is when one assumes that the product of innovation would be better than continuing using current technology within the organization.

We also discovered a TOE framework modeled specifically for cyber security adoption decisions proposed by Wallace et al. (2021). In their paper, the authors wanted to answer three main questions: What are the concerns of the IT leaders, What factors influence IT leaders' cyber security adoption decisions and What factors are considered post cyber security adoption (Wallace et al., 2021). The second and third question is most relevant to us, as they look at the adoption of technology. They researched this adoption by using the TOE framework and created their own which can be seen in figure 4.2.

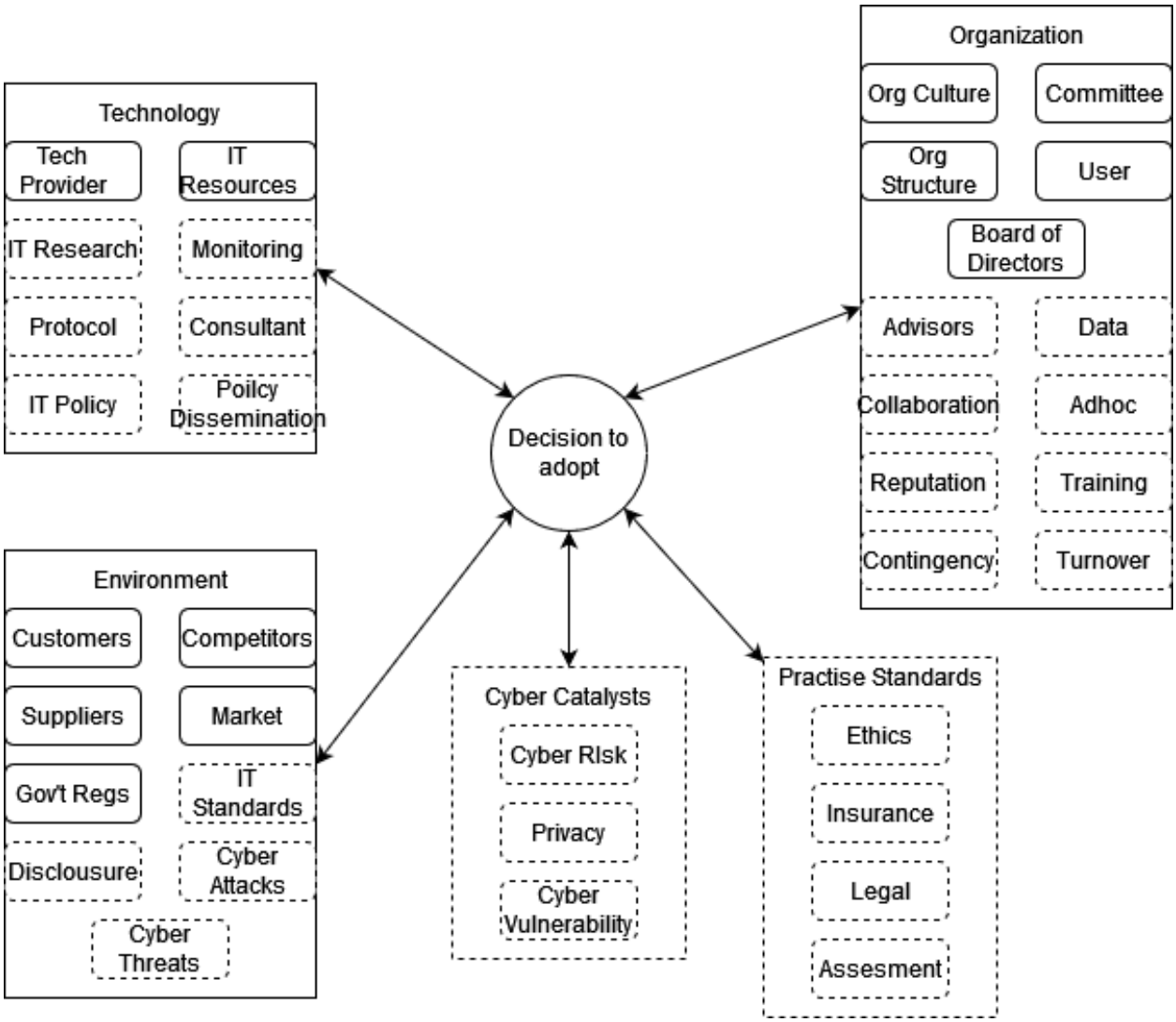

Figure 3.2: Extended TOE model for cyber security adopted from Wallace et al. (2021)

They propose two new dimensions that are not present in the traditional TOE model: Cyber Catalysts and Practise Standards. These dimensions were found through interviews that the authors had with several different high-standing IT leaders, such as CISOs and CIOs. The Cyber Catalysts are defined as "Cybersecurity specific factors that initiate adoption decisions that are beyond the traditional TOE framework". The catalysts presented by Wallace et al. (2021) include: Cyber vulnerability, privacy and cyber risk. The Practise Standards

which are referred to in the second dimension is "the underlying general best practices that influence cyber security decision-making". This framework will be beneficial as we develop our theoretical lens and our own framework for researching the adoption of defensive cyber deception. The framework includes a lot of independent variables which are not present in traditional TOE, which hopefully align with the empirical data we will be presenting later on in this thesis.

Drawing from the TOE aspects identified in the literature regarding defensive cyber deception and the practices of the researches before us, we hope to make a theoretical lens that could be useful for our research.

Chapter 4

Research Approach

The purpose of this thesis is to understand and document the factors that influence the adoption of defensive cyber deception in Norwegian organizations, seen through the eyes of the researches and interviewees. To accomplish this purpose, we have formulated these research questions:

- RQ1: What affects the adoption of defensive cyber deception in organizations in Norway?
- RQ2: What are the technological, organizational and environmental factors that affects adoption?

Our main research question is as stated above: "What affects the adoption of defensive cyber deception in organizations in Norway?" The reason for us specifying "in Norway" is merely for convenience sake, in order to make our research a bit more specific. If we were just researching the adoption in general, it would still only be for Norway, as all our interview subjects work in Norway, either within Norwegian organizations or Norwegian branches of international organizations. While doing some preliminary searches regarding defensive cyber deception in Norway, we found very little information regarding it, so this also made us interested in looking into the adoption in Norway in particular.

This chapter arguments for our choice of research approach, from our research design, the unit of analysis and subject selection, data collection, data collection and ethical considerations.

4.1 Qualitative approach

According to the definition of Hennink et al. (2020), qualitative research is in broad terms: " ...an approach that allows you to examine people's experiences in detail by using a specific set of research methods such as in-depth-interviews ..." The main reason for why we have chosen to have a qualitative approach, rather than an quantitative approach, is mainly because of the data we will be gathering. By using interviews as our data collection tool, we can gather much more in-depth responses about people's experiences, knowledge and opinions (Patton, 2014) rather than having a yes/no or 1-5 point based survey. As compared to a quantitative approach, a qualitative approach focuses on the how and why things occur. Qualitative approach mainly focuses on this things "within a context", leading the sample size of data to be smaller than what an quantitative sample would be (Recker, 2021)

While choosing our research methodology, there were several aspects of our research we had to consider:

- *Data*: What type of data is required to answer our research questions, is this type of data available, where can we gather this data and what will we do with the gathered data?

- *Risks*: What can go wrong while executing the research design, what strategies can be used to minimize the potential risks?
- *Theory*: How much literature on the research topic is available, what are the gaps in the literature, what findings in the literature might affect our work and choice of research design?
- *Feasibility*: Is the research design feasible as a Master study with regards to factors such as time limitations, resource limitations and experience?

(Recker, 2021)

Our main research question is "What affects the adoption of defensive cyber deception in organizations in Norway", so what kind of *Data* would be required to answer this question? The data we will be gathering will be discussed in greater detail in the data collection part of the chapter, but we will be collecting cyber security experts' thoughts and opinions regarding the adoption of defensive cyber deception within their respective organizations. This data is available, as we have identified experts who has experience in defensive cyber deception and/or the adoption of new cyber security technologies within organizations. This data is gathered through interviews with employees from different organizations in Norway and the gathered data will be analyzed and presented in a written form and as a model.

There are potential *Risks* associated with our research methodology, as various challenges can arise during the research process. If our interviewee participants does not want to share their knowledge or they have to cancel our data collection with them, this could very well be the downfall of our research and thesis. We mentioned that the data we needed for our research was present, but this does not refer to the literature, as there has been no studies on the adoption of defensive cyber deception in Norway, at least that to our knowledge. So our primary data source with regards to the adoption is the experts that work in the organizations. This is a potential risk which can be minimized by trying to have the data collection as early as possible during the thesis period, giving us time to get more interview participants if the original participants become unavailable.

The *Theory* of our precise research question is non-existing. However, we have identified a lot of theory regarding deception, defensive cyber deception and models and frameworks that focuses on the adoption of new technology within organizations. The findings in the literature might change our research question during the thesis period.

Our research design is *Feasible*. There are risks and various challenges that can arise, but with the scope we have set with the research questions and the gathered theory, it should be possible to finish the thesis during its designated period of Spring 2023. One problem could be experience, as neither of us two researchers have any prior experience with a thesis of this size, but everyone has to start somewhere.

After going through the four points mentioned above, it became clear that our research question and research is going in the qualitative direction and thus we should pursue a qualitative approach in our thesis.

4.2 Research design

A research design is a plan of action that comes after the formulation of the research question. It is a blueprint for the collection, measurement and analysis of the data that will help answer our research question (Recker, 2021). Recker (2021) propose intellectual reasoning

as the basis of all research design, with the three forms of intellectual reasoning being: *induction*, *deduction* and *abduction*.

In order to decide upon our research design, there are several factors that should be considered:

Spectrum	One end of continuum		Other end of continuum
Aim	Exploratory	vs.	Explanatory
Method	Qualitative	vs.	Quantitative
Boundary	Case	vs.	Statistical
Setting	Field	vs.	Laboratory
Timing	Cross-sectional	vs.	Longitudinal
Outcome	Descriptive	vs.	Casual
Ambition	Analysing	vs.	Designing

(Recker, 2021)

The table above contains factors that are important to consider when defining our research design.

Aim refers to exploration and explanation, do we wish to explore something new or explain something that is already present in literature and real life? As our research is looking at the adoption of a specific cyber security technology, we have not found research that specifically looks at the adoption of defensive cyber deception, we can consider our research design as exploratory. However, as our research is looking at adoption in an organizational setting, aiding organizations to determine the factors that influence the adoption of the technology, the research can also be explanatory. Therefore, we think that our research lands in the middle of the spectrum with regards to the aim factor.

Method refers to either a qualitative or quantitative approach. As for our method, as mentioned earlier in the chapter, we will be going for a qualitative methodology in our research.

Boundary refers to what kind of study it is, if it is based on a case study or statistical data. Our boundary will be several "case" studies, as we are gathering data from several organizations.

Setting refers to the location of our research. The two polar opposites are field and laboratory. We can argue for our research being closer to field, as we will be gathering data from professionals from their respective organizations, making it a more real world setting compared to a laboratory setting.

Timing refers to the time span of the research, longitudinal is one case over a long period of time and cross-sectional is several cases at one point in time. We land on the cross-sectional timing.

Outcomes refers to descriptive or casual, it can focus on a descriptive study of a previously unknown phenomenon or the discovery of some casual mechanisms that can explain why a certain phenomenon occurs. We are more on the casual side, as we focus on the factors or mechanisms of adoption in organizations.

Ambition refers to the goal of our research, is it to understand something or design something? Our approach is to understand something, we want to understand a phenomenon through our theoretical lens of choice, which focuses on adoption in organizations.

By looking at our answers above, it is hard to put our thesis in a "box" with regards to research design. That is why we chose not to have a specific research design and rather follow the different factors we have identified above in this section.

4.3 The unit of analysis and subject selection

Qualitative research uses purposive sampling as opposed to the probability sampling used in quantitative research (Hennink et al., 2020). This means that instead of selecting a certain demographic as one would in quantitative, we only select certain individuals that have knowledge and experience in our field of research. The logic and power behind purposeful sampling lies in the ability to choose information-rich cases to study (Patton, 2002).

At the start of our thesis, we wanted to gather data from cyber security professionals who had experience with defensive cyber deception, using it, implementing it and maintaining it. We held onto this thought for at least the first month, if not the two first month of our thesis. However, we realized that with our connections in the industry, it would be extremely difficult to know if an organization was using the techniques, let alone getting multiple interview candidates from several different organizations. Thus we decided on trying to find professionals that have either used or heard about defensive cyber deception.

These were gathered through contacting some organizations we identified through previous encounters in the industry and using our connections from previous jobs and acquaintances. We sent them a mail with the consent form which can be found in Appendix A.

The unit of analysis in our thesis is cyber security experts within organizations in Norway that has experience or knowledge with regards to defensive cyber deception. As our units of analysis are not tied to a specific type of organization, it helps mitigate the risk previously mentioned regarding the lack of cyber security experts with experience or knowledge in our subject. Originally, we wanted to focus the study on the experts with experience in maintaining, implementing and creating defensive deceptive solutions and tools, but we decided to also gather data from experts who had heard of it and did not necessarily have any technical experience. This was due to the high possibility of them having some interesting thoughts and opinions regarding the factors that promote or hinder the adoption of the technology.

As a result of this, we have gathered interview candidates from six different organizations and there are eight different interview participants in total. Some of the candidates are cyber security architects or engineers, while others have more "C-level" positions such as CISO or COO. We opted for a broader spectrum with regards to interview candidates in order to eliminate elite bias from our empirical findings as this could be a limitation to the data collected (Myers and Newman, 2007).

Pseudonym	Type	Nationality
Org1	Energy	Norway
Org2	Cyber security	Norway
Org3	Cyber security	Norway
Org4	Consultant	International
Org5	Consultant	International
Org6	Investment etc	Norway

Table 4.1: Organizations

We have conducted interviews with members of the Norwegian branches of the two international organizations mentioned in Table 4.1 .

Our recruitment strategy was done through informal networks and snowballing (Hennink et al., 2020). We used the "social media" Linkedin to identify interview candidates and sent emails to the candidates. Some were found through informal networks that the researchers had developed through internships and other events with organizations. Through these informal networks we could snowball to other people by asking our connections if they knew about someone with knowledge regarding our research topic. The different interviewees can be seen in table 4.2.

Pseudonym	Role	Years in Industry	Years in Role
CISO-A	Chief Information Security Officer	8 years	2 years
CISO-B	Chief Information Security Officer	22 years	5 years
CISO-C	Chief Information Security Officer	10 years	8 months
COO	Chief Operations Officer	10+ years	3 years
CyberSecDir	Cyber Security Director	15 years	2 years
CyberSecConsult	Cyber Security Consultant	7 months	7 months
CloudSecArchitect	Cloud and Cyber Security Architect	8 years	1.5 years
OT-Engineer	Operational Technology Engineer	15 years	10.5 years

Table 4.2: Interview Participants

4.4 Data collection

Data collection is a vital part of a qualitative research. As previously mentioned, the main reason for choosing qualitative over quantitative was the fact that we could have interviews. The data we are going to collect would not be suited for a quantitative data collection, as we are aiming to understand the nuances of the topic and that would be difficult to achieve through quantitative data collection techniques. Another reason is the amount of data there is to collect, defensive cyber deception seems to not be widely used in Norway, so there is a lack of data sets for research on this topic.

4.4.1 Interviews

Methodology

Qualitative interviews are one of the most common and important data gathering methods in qualitative research, and is commonly used in information systems research (Myers and Newman, 2007). The three forms for qualitative interviews stated by Myers and Newman (2007) are the following:

- Structured interview
- Unstructured or semi-structured interview
- Group interview

As our qualitative data collection approach, we will be using semi-structured interviews. Semi-structured interviews are different from the other two, as there is a need for improvisation during the interview. This can lead to more in-depth discussion between the interviewer and interviewee, which could lead to an enrichment of the empirical data.

For evaluating the quality of our interview questions, we examine our questions to see if they are interpretive, appropriate, coherent, valid, transparent, reflexive, cultural, saturated, new and ethical. It is important that the questions are formulated in a qualitative way, asking questions that cannot be answered through qualitative research, such as "How many false alarms does your organization receive on average in a week?" and rather ask "What is the reason for your false alarms and how can you prevent it (Hennink et al., 2020)?

Limitations

There are quite a few pitfalls and problems that can occur while doing qualitative interviews. Here are some points that we discovered through two sources:

Problem	*Description*
Artificiality	A qualitative interview is not natural, it is an interrogation of a stranger which in turn has to give opinions on a topic under time pressure.
Lack of trust	As mentioned earlier, the interviewee is a stranger, making it less likely that they will trust the interviewer with information the interviewee deems sensitive.
Lack of time	The lack of time during an interview may affect the quality of the data that is being gathered. It can be that the interview is too short time wise, creating gaps in the data that has been gathered. It can also cause interviewees to create opinions under pressure, making the data less reliable.
Level of entry	The level refers to the level of employee in their respective organization(s), if the interviewer's level of entry is too low, it might be hard to gain interviews with more high-standing employee's such as the C-Level executives for example.
Elite bias	If an interviewer only goes after the C-level executives in an organization, they will fail represent the broadness of knowledge that can be present in an organization. It obviously depends on the research topics, but most topics should benefit from interviewee diversity.
Hawthorne effects	The Hawthorne effect refers to a modification in behavior when a subject knows they are being observed. A person might act differently or say different things while being observed and interviewed than what they would do when left alone.
Constructing knowledge	Interviewers are not only soaking up existing knowledge, they are also constructing knowledge based on the interviewee's stories and their own existing knowledge.

Continued on next page

Table 4.2: (Continued)

Ambiguity of language	The meaning of certain words, whether they are written or spoken, can sometimes be up for debate, so one should not take for granted that interview questions will be fully understood by the interviewee.
Skills	It is important that the interviewer has the skills to establish rapport, listen, motivate and react to what is being said during the interview.
Flexibility	Needed to change topic order in interview guide to follow interviewee's story
Transcription	The actual transcriptions of the interviews are time consuming compared to a data set for example, however, easier to work with one could argue.
Interviews can go wrong	This point refers all the other points above, one can plan all they want, but there are several pitfalls and problems with qualitative interviews.

(Hennink et al., 2020; Myers and Newman, 2007)

All the previously points are things that are important to have in mind while preparing for and executing interviews. When a interview is done, it is done, you cannot "fix" the data you have gathered without going through the whole cycle again. The interview guide used for this thesis can be found in Appendix A.

4.5 Data analysis

Data analysis in qualitative research is crucial for a paper's or thesis' success. It helps the authors reduce and present text that makes sense to themselves and to the readers, rather than present large quantities of unprocessed text such as documents or interview transcripts. Not only does it make the data easier to read and understand for the readers, but also the authors working with the data (Miles and Huberman, 1994).

For the data analysis for our empirical data, we have used one of the most common set of techniques in qualitative research: coding (Recker, 2021). Coding of transcripts are done by categorizing different types of raw data, giving the data a "home". By doing this, it makes it a lot easier when for example writing about the results of the study as you know what your data contains. As our collected data consists of transcripts from interviews, coding the data makes the most sense analysis wise. Other methods that have been used previously for data analysis are: Memoing, critical incident analysis. content and relational analysis and discourse analysis (Recker, 2021).

Hennink et al. (2020) proposes the analytic cycle in their paper, the cycle contains: *Develop Codes*, *Develop Codes Describe and Compare*, *Categorize and Conceptualize* and *Develop Theory* (Hennink et al., 2020). Both our sources mentions codes as a vital part of the qualitative data analysis and is the only method mentioned by Hennink et al. (2020) in their analytic cycle below.

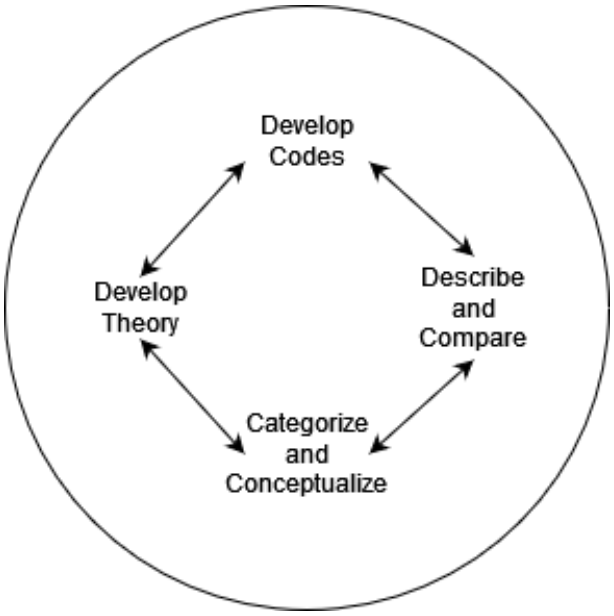

Figure 4.1: Analytic cycle for qualitative research adopted from Hennink et al. (2020)

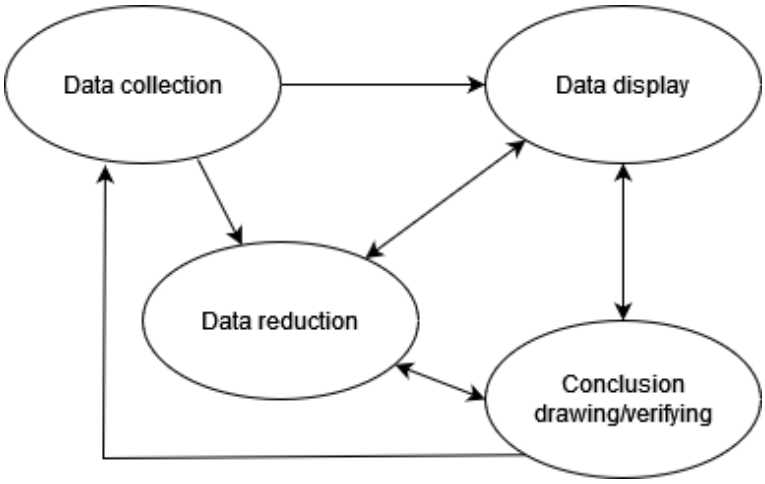

Figure 4.2: Qualitative data analysis model adopted from Miles and Huberman (1994)

We decided to structure our codes based on the TOE framework hierarchy, as this would make the data easier to work with when we write our result and discussion sections. We drew inspiration from both the models of Hennink et al. (2020) and Miles and Huberman (1994) for qualitative data analysis, with the data collection coming first, then developing codes, categorizing based on the developed codes and drawing conclusions for our findings from the coded data.

4.6 Ethical considerations

Here are is a list by Resnik (2016) of 6 ethical principles for scientific research:

- Scientific honesty
- Carefulness
- Intellectual freedom
- Openness

- Attribution of credit
- Public responsibility

All these points are important ethical considerations to take into account while doing research. As this is a master's thesis within cyber security, not all of these are as relevant for us. Public responsibility which refers to reporting to media if the research has an impact on human happiness will unlikely affect this thesis.

Scientific honesty: It is important in any research or academia, we would argue that honesty in itself is important in all facets of life. There should be no destruction, fabrication or misrepresentation of the data gathered in our thesis. This would directly affect not only our own reputation and ethics, but could also hurt our advisor and university. It could also have a negative affect on our interviewees.

Carefulness: Researches should be careful in all the aspects of the research, making sure to not make sloppy mistakes or errors out of carelessness.

Intellectual freedom: Researches has to be able to openly critique old ideas and pursue new ideas.

Openness: Sharing your techniques, results, data, methods, etc. This allows others like ourselves to learn and hopefully give a helping hand to new researches or master students. This makes it possible for others to use their intellectual freedom to critique your work and give you points to improve on.

Attribution of credit: While doing any type of research or thesis, we often get a helping hand, be it our families, supervisor or even interviewees. These people should be given credit where credit is due.

Although this is a master thesis, we think that the mentioned points are important in any facets of research, so we decided to mention these here.

4.7 Our maturity estimate model

While constructing our interview guide, a small part of the interview was to ask yes or no questions concerning cyber deception techniques found in the literature in order to set an estimated maturity level. These cyber deception techniques identified in the literature were broken down into 5 questions, which asked the interviewee if they had heard of or used: canary tokens, low-interaction honeypots, high-interaction honeypots, high-interaction honeynet with SDN, and lastly deceptive network or environment using AI. The interviewees were asked in that specific order, and was assigned an estimated maturity level from one to five accordingly. What we gather from the yes or no answers regarding different defensive cyber deception techniques is the level of their prior knowledge regarding the techniques. If the participants only has knowledge regarding the "low" maturity techniques such as canary tokens and low-interaction honeypots, would their views on the factors that adopt defensive cyber deception differ from the participants who has knowledge about the "high" maturity techniques such as high-interaction honeypots or honeypots used together with SDN? This is the basis for our maturity estimate model.

A maturity models describes and determines the state of perfection or completeness of certain capabilities of an entity, and the entities in our context are the interview candidates (Wendler, 2012). At the beginning, the maturity estimates of the interviewee candidates

were supposed to be for our eyes only, but later discovered that it could be used in our thesis to discern if the interviewees' view of cyber deception differentiate from each other or not. The maturity estimate model will be used together with the TOE framework, in order to enrich the framework with showing what factors originated from which maturity levels.

4.8 Our TOE Framework

For our TOE framework, we will be using the analyzed version of the empirical data we collected through our semi-structured interviews. The different answers from our interview participants will affect the factors that will shape our TOE model. We will also be using our maturity estimate model, which will be presented in the results chapter of our thesis, being colour coded in order to differentiate between the different levels. The colour schemes are used to label the factors we discovered through our analysis.

Chapter 5

Results

This chapter of our thesis will show the results from our data analysis of the empirical data we gathered through our semi-structured interviews. The chapter contains a section on our literature-based TOE Model, which was created before we even began analyzing the empirical data, a section on our maturity estimates and what role it will have for our thesis, and a section where we explore the data we analyzed through coding by using our theoretical lens.

The findings in the empirical data will not be discussed in this chapter, but it will be presented in a way that corresponds with our theoretical lens and the main contribution of our thesis.

5.1 Literature-based TOE Model

The model presented in this subchapter is the TOE model we modelled before going through the empirical data from our interviews. The model is visualised in Figure 5.1. This model is based on the findings in the literature regarding defensive cyber deception, the traditional TOE model presented in Figure 3.1 and the aspects taken from Figure 4.2 in the Theoretical Lens chapter. The factors taken from the existing cyber security TOE model are illustrated by a dotted line, so the following: Tech Provider, Cyber attacks and the whole cyber catalysts section. Availability was taken from the traditional TOE and the rest of the factors were based on findings in the literature.

5.2 Maturity Estimates

In the following section, we will be using the term maturity about the TOE models created from the empirically gathered data. At the start of our thesis work, when we were developing our interview questions and interview guide, we found it intriguing to assign a maturity level to each interviewee based on their knowledge and practical experiences with defensive cyber deception. This was done by simply asking the interviewees if they had experience with or knowledge to existing defensive cyber deception techniques/mechanisms such as: Canary token(s) (Maturity level 1), Low-interaction honeypot(s) (Maturity Level 2), High-interaction honeypot(s) (Maturity Level 3), High-interactive honeynet(s) with SDN (Maturity Level 4) and Deceptive network or environment utilizing AI (Maturity Level 5). The mentioned mechanisms were identified by us during the literature review for our Thesis.

Factor	Description
Technology	
Compatibility	Defensive cyber deception's compatibility with existing traditional cyber security mechanisms, such as firewalls, anti-virus and IDS etc
Relative Advantage	The advantages defensive cyber deception brings to organizations cyber security abilities.
Complexity	The complexity of correctly implementing and managing, and maintaining the techniques and mechanisms.
Open Source	The availability of open source projects that could act as an inspiration to an organization's implementation.
Opportunity	The opportunity for future improvements in defensive cyber deception techniques and implementations in Norway.
Organization	
Readiness	The preparedness or readiness of the organization, if they have a sufficient infrastructure in place.
Risk	Risk estimates that are done within the organization in order to identify the need for new cyber security measures.
Size	Size of the IT/Cybersec unit in the organization.
Cost	The cost of implementing, maintaining or purchasing the service/technology.
C-Level Support	Support from top-management with regards to cyber security investments/improvements
Environment	
Service Providers	The available cyber security service providers within Norway and what they provide.
Standards	IT/OT-standards that guides organizations cyber security decisions.
Cyber Threats	The threat landscape that the organization resides in, in our case: specific sectors in Norway.
Available Expertise	The available expertise of defensive cyber deception in Norway.
Other Organizations	Learnings and influences an organization may get from other organization's cyber security practices
Rules & Regulations	Rules & regulations that affect the organization directly or their sector/domain.
Education	The education available for cyber security professionals, enthusiasts or students regarding defensive cyber deception.
Graduates	New generational employees/graduates that bring fresh ideas and a new pair of eyes with regards to cyber security practices and techniques.

Table 5.1: Glossary of TOE Factors

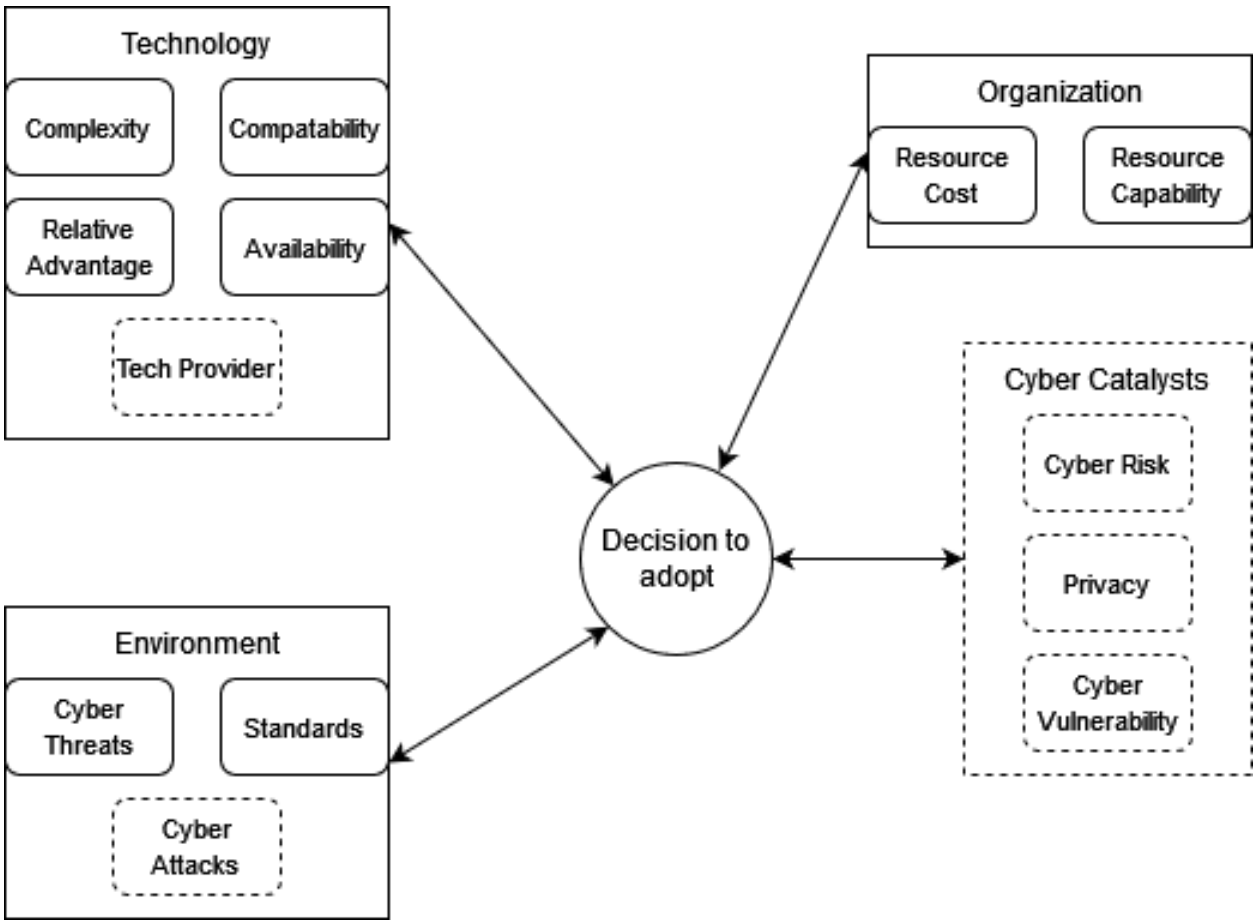

Figure 5.1: TOE model based on our literature review and existing TOE models

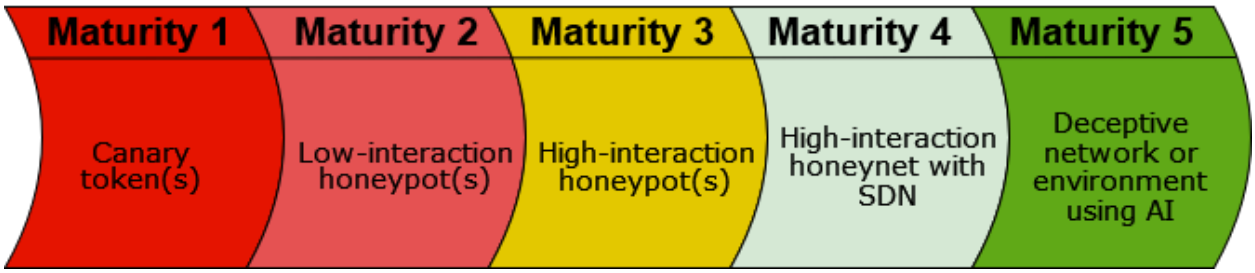

Figure 5.2: Maturity Estimate Model

5.3 Empirical Data TOE Model

Our TOE model for defensive cyber deception has the three aspects that correspond to traditional TOE: Technology, Organization and Environment. Within these aspects are the factors, which are placed according to their importance within their respective aspect, from left to right, top-down. Our empirical data was coded based on the maturity estimation we mentioned previously in the thesis. This chapter will have have a single model, containing the factors from each estimated maturity level. The factors that were mentioned will be colour coded with regards to Figure 5.2. We will be going through the various factors we discovered that affect organization's adoption of defensive cyber deception. The factor's descriptions can be found in Table 5.1. Our TOE model for the adoption of defensive cyber deception can be found in Figure 5.3.

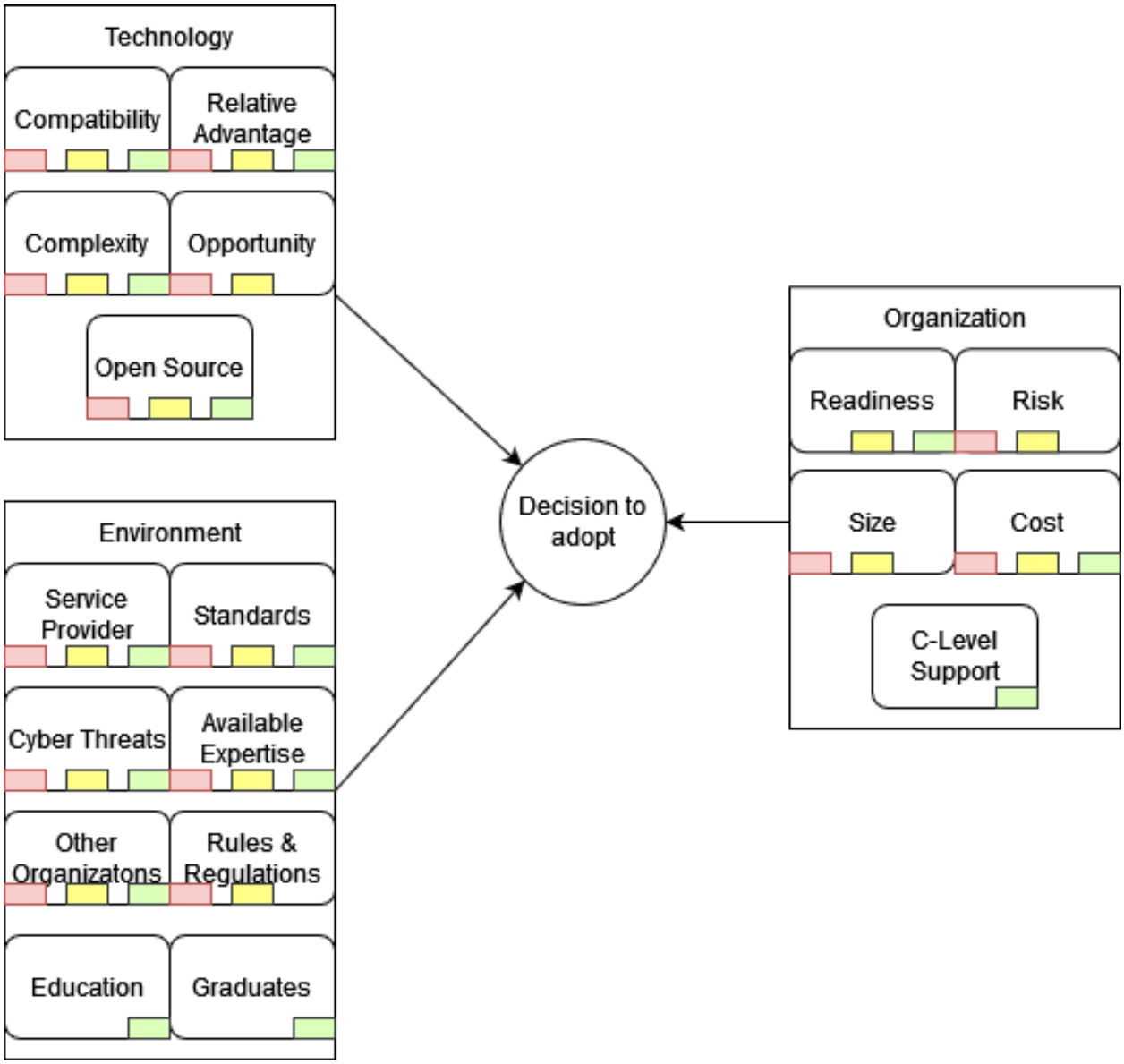

Figure 5.3: TOE Model for Defensive Cyber Deception

We will be going through each of the main three aspects, technology, organization and environment and the factors within them. The data will be quotes taken from our interviews with the six different organizations and eight different interview participants. We analyzed the empirical data in a way that correspond with our theoretical lens, taking the factors identified through coding and showing the data that support its addition in our TOE framework for defensive cyber deception

5.3.1 Technology

The technology aspect of TOE focuses on the technological factors that could affect adoption. For example, the compatibility of the technology an organization wants to adopt with their existing infrastructure/technology. The identified technological factors are: Compatibility, Relative Advantage, Complexity, Open Source, and Opportunity.

Compatibility

Compatibility reflects defensive cyber deception's compatibility with existing traditional cyber security mechanisms, such as firewalls, anti-virus, and IDS, among others. This factor was mentioned in all our three maturity levels. The compatibility of defensive cyber deception with other cyber security products or services in an organization's cyber security infrastructure is crucial in the organization's adoption, as no technique or product is sufficient on its own. We argue that this is one of the most pivotal factor for adoption, as many or all organizations who would adopt defensive cyber deception would do this into an existing cyber security environment.

Most of the interview participants had something to say regarding defensive cyber deception's compatibility with existing cyber security mechanisms. While talking about defensive cyber deception's compatibility in general, CyberSecConsult argues that it has to be compatible with existing technologies. You should not have to rearrange your network or environment to adopt a new product or service, it should be able to work nicely with existing technologies. They also mention that defensive cyber deception sounds like something that could logically fit into an organization's network, if the deception product was delivered from someone like Microsoft or Amazon:

> *Of course it has to be compatible. You can't get a nice product thrown in your face and get told that you should change everything in your existing systems to accommodate it. (...) It sounds like something that can logically fit into the network (...) if it is something from Microsoft or Amazon.*

CISO-A aligns/agrees with CyberSecConsultant's perspective that the lack of compatibility between a product or software can impede an organization's adoption of such solutions.:

> *(...) It is what hinders an organization's adoption of new software, that it may not be integrated into what you already have.*

There is also an additional cost or expense that an organization has to pay if a product is not compatible with the cyber security solutions they already possess, making the probability of adoption lower if compatibility is a problem. CISO-A argues that integrating something into a network or infrastructure is expensive. Cost is also a factor in the organizational aspect, which will be discussed further in its respected section.

For CISO-B, CyberSecDir, OT-Engineer and CISO-C the consensus was that defensive cyber deception is compatible with existing cyber security measures, CISO-B mentions that they see no problem having it run parallel with their existing measures within the organization:

> *I think it can be very compatible. (...) I see no problem with having it run parallel with existing cyber security measures.*

OT-Engineer argues that it has to be integrated into the "larger cyber security system" so that the cyber security administrators gain a more whole view of what is going on in the system and its components:

> *(...) it has to be integrated in a larger "cyber security system" so that the user can have a more whole view of what is actually going on (...)*

We have spoken a lot about defensive cyber deception's compatibility and that it is compatible and should be compatible, but is it possible to base your cyber security solely on deceptive techniques? CyberSecDir has a kind of different view on the compatibility, stating that existing cyber security measures have to be in place before you can implement cyber deception and that cyber deception would not have a value if you do not have a existing secure perimeter in your organization:

> *You have to have the two things [IDS & Firewall] you mentioned before you can have cyber deception. The thing about cyber deception is that it helps existing technology. So if you do not have a secure perimeter and so on, then I do not think cyber deception will have value.*

It is important to note that defensive cyber deception is an umbrella term which contains different techniques that can be compatible with different measures. CISO-C mentions honey users, which are essentially just fake accounts that are not associated with real people. CISO-C talks about the honey user's compatibility with Security Information and Event Management (SIEM) technologies and rules in log analysis, because this can use existing technologies to "mark" the honey users such that existing systems can be used to monitor them:

> *(...) if we take honey users for example, then Security Information and Event Management (SIEM) technologies and rules in log analysis will fit very nicely, because then you could mark the user as a honey user. (...) I think it could easily be integrated into existing cyber security architectures.*

CloudSecArchitect has used and implemented defensive cyber deception within their existing cyber security infrastructure, and explains that it is already compatible and relatively easy to implement with existing IDS/IPS functionality. They emphasize that personally they had no complications when integrating defensive cyber deception with IDS/IPS:

> *(...) I believe that to put in place integrations between honeypots and canary tokens with existing IDS/IPS functionality is relatively. (...) but I have at least not had any challenges so far when making integrations across the solutions implemented in the last two years.*

COO also has hands-on-experience and agrees with CloudSecArchitect. They also mention that defensive cyber deception is compatible with existing technologies as deceptive elements are already integrated with the existing logging and will not require extra components because it will use the existing components already invested in your network:

> *I believe that it is very compatible (...). (...) honeytokens, fake users, fake documents, fake network traffic, and such, the deceptive elements will already be integrated with the logging you already have today. It will be picked up by the log-forwarding on your hosts, networking logs etc. It will not require extra components, it uses the components already invested in your network.*

Through the empirical data we have gathered about defensive cyber deception's compatibility with existing cyber security mechanisms, we have gathered that it is crucial for most organizations that it is compatible with what you already have in your cyber security environment. For the most advanced or ready/prepared organizations, the compatibility might not affect it as much, as they are able to make it fit into their system with the competence they have in that regard. As stated earlier in the section, we think that this is a factor that is important primarily due to importance many of our interview participants placed on compatibility.

Relative Advantage

Relative Advantage reflects the advantages defensive cyber deception brings to organizations cyber security abilities. The factor was mentioned by all of our identified maturity levels in the interviews. The advantages or benefits that defensive cyber deception provides to an organization is a very important factor we have discovered through our empirical data analysis. If deception does not provide any advantage or benefits over what the organization already possesses or what is already available to them through service providers, why bother even considering the adoption of deceptive techniques?

One of the advantages/benefits of defensive cyber deception that was mentioned quite frequently during our interviews was early detection. When we mention early detection, we mean early on in an attacker's attack tree. A cyber attack can often be represented as a tree often used in algorithms, with reconnaissance and traversing within the network/system being close to the top or parent node of the tree. This is where you want to detect an attacker as early as possible, in order to make sure they can not get any lower in their attack phases.

CISO-C thinks that defensive cyber deception is a useful technique because the user gets both early detection and relatively high amount of alerts if the defender uses honeypots:

> *In my opinion, it is a very useful technique, you get both early detection and with the honeypots you will get relatively high amount of alerts. (...)*

The high amount of alerts CISO-C refers to is that you can get a lot of alert data from the use of a honeypot.

CISO-A refers to a tripwire honeypot account, which is basically just a honey token mentioned in our background chapter, saying that it is best designed for static environments because of the high-fidelity that would be created, referring to it as an early warning system which correlates great to our view on deception's use in early detection:

> *The advantages with a tripwire honeypot account is that you can have high fidelity right away. (...) it becomes an early warning system that is best designed for static environments.*

CISO-B mentions earlier detection, not early in time, but earlier in the attack phase or tree that was mentioned earlier in this section. They state that when the alarm goes of at a higher point in an event tree, it reduces the defender's vulnerability as the attackers has not gotten too far in their attack phases:

> *I think they [people who adopt defensive cyber deception] can get the opportunity to discover something [cyber attack] a little faster, not necessarily faster in time, but earlier in the attack phase, (...) the alarm goes off at a higher point in your event tree thus reducing your vulnerability.*

CloudSecArchitect proposes an interesting way of using canary tokens (honey tokens), using them as a way for early detection in a ransomware attack scenario. They state that one can make the tokens imitate sensitive files and monitor them. This way, the defender can know if there has been an attacker on the inside their infrastructure who has tried to extract or interact with the fake files:

> *(...) and it is a very good indication of or give us an insight if there is anyone who has managed to extract data from the infrastructure. (...) we have canary tokens that sit on the inside and then imitate legitimate files which are then used to imitate sensitive files. And with canary tokens it is much easier to see if an attacker has been inside and tried to extract sensitive files in that connection [ransomware].*

CloudSecArchitect thinks that solutions such as canary tokens can provide a very large advantage by making it possible to discover if there has been abuse or extraction of data:

> *(...) canary token solutions will actually provide a very large advantage to be able to discover whether there has been abuse or extraction of data (...)*

CISO-A proposes an interesting use-case for cyber deception's early detection capabilities, where they refer to the LastByte hack, where a compromised legitimate user was used to perform the hack. CISO-A claims that techniques such as honeypots provide some value against compromised legitimate users, because the real legitimate user would never go into the honeypot:

> *(...) so there honeypots provide some value. If you can then implement something that the regular employees would not have gone into (...) it is against that threat then, compromised legitimate accounts.*

One of the other advantages/benefits one can gain from adopting defensive cyber deception is TTPs or tactics, techniques and procedures of attackers. If an organization uses for example a honeypot or a deceptive environment, they can monitor it and learn what type of attacks the attackers perform against their deceptive elements in order to secure the real systems or environments against it.

While talking about what direct value an organization could get from the adoption of defensive cyber deception, CISO-C mentions that one could acquire better forensics basis, a forensics foundation one could say. It could help organizations get closer to identifying a bit more about the TTPs of the attackers, making it so that you could increase your basis for defense as well:

> *I think the direct value would be that you can acquire better forensics basis. You can get closer to identify the TTPs of the attackers, you would have a better basis for defence if you know these (...).*

CyberSecDir shares the same perspective as the researchers and CISO-C regarding the advantages a defender can get from gathering an attacker's TTPs. Additionally, they describe a scenario where the attackers are allowed to enter a deceptive environment referred to as a "room". They also mention that you can waste the attackers time, which is an additional benefit of learning their TTPs. The attackers are not utilizing their techniques on your actual network or environment:

> *(...) You can get a very good gain by letting the attackers enter the "room" and observe what they are up to. Then they waste their time as well as you gain a lot of information regarding TTPs and their behavior.*

COO and CISO-B agrees that deception can give useful information about the attackers, with CISO-B saying that one can look at the patterns of the attacks in order to find out if it is an actual person behind the attack or if it is automated, thus gaining a better understating of the attack type:

> *(...) Are there known patterns, is it automated, or is it a person, so you will get a distinct understanding of what the attack type is.*

COO mentions his interest in the domain (defensive cyber deception) and states that it can give the defenders very useful information:

> *(...) but a domain which can give us very useful information.*

CyberSecDir mentions three benefits they expect from defensive cyber deception: the time aspect, referring to both early detection and the time waste of attackers, the telemetry one can gather from attackers, and their behavior information:

(...) So I think the time aspect is important and the telemetry and behavior information. You get a lot of information about the attacker in the environment, in the deceptive environment.

There are other benefits than just learning the attacker's TTPs and the early detection that defensive cyber deception provides. In our background chapter, we discussed malware deception, where a defender can deceive malware into giving information about itself and its techniques/exploits. CISO-A mentions that their organization utilizes something they refer to as a sinkhole honeypot. This honeypot tries to communicate with malware in order to make it leak information about itself:

(...) And our sinkhole is a honeypot in the sense that it is trying to communicate with the malware and make the malware leak a lot of information about itself.

CyberSecDir mentions that they think that defensive cyber deception would be more applicable towards advanced threats, in other words, it is a good solution for advanced defenders who defend against threat actors that use several years on their software and attacks:

(...) I consider it [cyber deception] more applicable towards advanced threats, so PST, NSM, E-tjenesten, they [the organizations] work with these kinds of threats that use several years on their software and attacks.

While talking about the potential advantages/benefits one can get from implementing defensive deception, there is also the mental "warfare" aspect of it. COO mentions that while defending against attackers, the defenders should use the opportunity to deceive the attackers and play with the attackers head. They argue this is crucial if defenders wants to respond to attacks in real time:

(...) while on defense we should use the opportunity to deceive the attacker (...) So that you [redacted] with the attacker's head. It is absolutely crucial if we want to be able to respond in real time.

They also argue that the goal of cyber deception is to ensure more intelligence in their alarms, increasing the high-fidelity of alarms, so in an event where an alarm is triggered, the defenders can be certain that there must be something suspicious or concerning occurring in their network:

The goal of cyber deception is to ensure that we get even more intelligence in our alarms and make it so that we can say "Damn, this must be some shit, this is almost guaranteed to be some shit" because (...) someone does something that they absolutely should not do.

Another benefit an organization can get from adopting deception in their cyber security environment is the knowledge of what or who is targeting their organization. This can be done by deploying an exposed honeypot that is open towards the Internet, which could lead to a massive amount of "random" or automated attacks targeting the honeypot. But CloudSecArchitect argues that this could provide a pointer for an organization to see what attackers are actually trying to do against their infrastructure:

(...) I tend to recommend clients to have honeypots or the like that are available externally. Because it will also provide a type of pointer to see what the attacker is actually trying to do a bit more offensively (...)

Through this section, we have discussed the advantages/benefits an organization could get from adopting defensive cyber deception, including early detection, learning attacker's TTPs, mapping attackers that target the organization and more. As stated earlier in the section, we think that this is a crucial part of the adoption because in order to adopt any cyber security technique, it should be beneficial or advantageous for an organization to adopt.

Complexity

Complexity refers to the complexity of correctly implementing, managing, and maintaining the defensive cyber deception techniques and mechanisms. This factor was mentioned by all of maturity levels in the interviews. When an organization is considering adopting a new product, the complexity of the new product may make the adopters think twice before determining a decision. If a new product proves to be complex and challenging to implement, maintain and manage, the cost induced may be higher than the cost removed by the product, which may do more harm than good.

CISO-C touches upon the complexity of defensive cyber deception solutions such as dynamic and flexible networks using SDN. They worry that if it is not implemented correctly, it could cause more harm than good. In the case of using SDN as a solution, CISO-C argues that insufficient segmentation and zoning may cause problems as well:

> *...let's say you are working on a flexible network where you use SDN and you are moving around your environment. Suddenly, your segmentation and zoning between the networks are not sufficient. This might provoke an attack for real, if your segmentation and zoning is not sufficient. ...*

OT-Engineer has first-hand experience regarding the complexity of defensive cyber deception in an OT setting, and provides some insight on the complexity of falsifying actual systems such as PLCs:

> *We did an attempt on cyber deception once before in collaboration with [Redacted] where we made a layer between OT and IT, and this layer was a replica of a control system with virtual PLCs, or rather a process station in this case, with several virtual machines, servers and so on. These virtual components communicated with their corresponding protocols. The attempt was successful, we managed to to set up a system that functioned, but the inconvenience was the maintenance afterwards. It was not a "place-then-go" and then come back half a year later to do some tweaks.*

The challenge of falsifying actual systems is that there is a lot of data that consistently needs to be updated and falsified due to their dynamic nature, which requires a lot of effort. OT-Engineer states that a fake control system with no frequent changes to its logic will seem too static, and an attacker may pick up on the fact that it is all fake:

> *It got too complex that a 20%-25% position was necessary just to take care of the system day to day due to the frequent change in the logic of the control systems. (...) a fake control system with no frequent change to its logic will seem too static, and an attacker can realize that it is fake.*

CISO-B, CyberSecDir, and COO talks about different degrees of complexity within defensive cyber deception. CISO-B says that it is fairly easy to set up dummy accounts that act as a honeypot, but at the same time, CISO-B is aware that an advanced attacker requires an advanced solution. Furthermore, CyberSecDir argues that in order to gain anything from deceptive elements, you need high-interactive elements because an APT can quickly identify and expose low-interaction elements as fake:

> *I think you should have a more, what is it called, high-interactive environment in order to gain anything, because after all, it is of greatest value when it is the APTs that come and are tricked into communicating with a low-interaction honeypot and they reveal a low-interaction honeypot, perhaps in a flash, that it is only fake, so it must be high-interaction environments and it must give intelligent answers, preferably a little fussy so that the attacker has to spend more time analyzing and is unable to fully comprehend what are lateral and vertical movements.*

COO argues that it is challenging for an attacker to resist temptations that is right in front of them, which means that they do not necessarily completely agree that high-interaction environments are needed to gain any value. Reason being that if an attacker, advanced or not, communicates with any simple deceptive element, you will know immediately that an attacker is inside your network, which is a win in itself. On the other hand, COO agrees with CyberSecDir that if you attempt to make a very sophisticated solution such as a honeynet, consisting of a lot of high-interactive honeypots, the complexity gets rather high:

> *It is very hard to say no to gold when you're an attacker. And we can understand attackers today, and that's why the complexity is very low. But if you're going to try and build a honeynet with a lot of high-interactive honeypots and you will instrument complete monitoring of this without being detected that you in fact monitor it. That is [redacted] complex. (...) It is very hard to make it perfect.*

Defensive cyber deception can be something complex, or it can be something very easy to implement, maintain, and manage. It all depends on what you choose to use. Deceptive elements such as canary tokens and low-interaction honeypots are very easy to implement, maintain, and manage and can be effective as tripwires. These tripwires can be easily dodged by a more careful and advanced attacker, but a more reckless and less advanced attacker can quickly fall for the traps. When the complexity of defensive cyber deception gets higher and it gets harder to implement, maintain, and manage if an organization chooses to implement dynamic and flexible networking using SDN or implementing a honeynet consisting of several high-interactive honeypots. If not properly implemented, these sophisticated systems can cause more harm than good, but as stated previously, a more advanced attacker requires a more advanced solution. In order to actually gain more insight of the TTPs of an attacker, high-interactive elements needs to implemented in order to prevent an attacker from unmasking the deceptive nature of the deceptive elements.

Open Source

Open Source refers to the availability of open source projects that could guide an organization's implementation or give them inspiration. This factor was mentioned in all our three maturity levels. Open source leans more towards the inspiration, as some open source projects regarding defensive cyber deception can spark an interest on what and how defensive cyber deception can be used, which can then lead to testing, experimenting, and evaluating various solutions to determine which solution suits the adopter best.

CISO-C, CyberSecConsultat and OT-Engineer agrees that the availability of open sources would not affect the choice of adoption as much. OT-Engineer argues that open source solutions are often heavy to implement than other solutions:

> *Open source solutions are often more heavy to implement than other solutions.*

CISO-B mentions that open source solutions could be a great way to get inspiration, which then can be discussed with their service provider and then ask them for a solution based on a interesting open source solution:

> *It is more that we let us get inspired, and then go to our partners and have a discussion on a service- or partner meeting, and then say that we thought that this seems exciting, e.g., honeypots. We would like this kind of open source honeypot solution, and then we ask if they would be able to make a service out of it.*

OT-Engineer touches on the same logic, that by being able to test, play, and lab with an open source solution, it would make it easier to transition to a full-scale solution by a service provider. CISO-A, CISO-B, and CyberSecDir agrees that open source solutions would generally just be used as inspiration. COO emphasizes that they are a big fan of the

phrase *seeing is believing*, and argues that people should test and lab open source solutions with real data:

> *I'm not much a fan of vendors. (...) I'm a much bigger fan of "seeing is believing". Lab it, test it, try it a little bit in production, God forbid you take anything down, but hello, you have to be able to test it with real data to see which capacity you gain from the open source environment.*

With that said, COO argues that the open source environment of defensive cyber deception has had its golden days, but has decline and is unfortunately not good enough for their uses.

Open source solutions can be a great way to bring ideas and inspiration, but does not necessarily affect the choice of adoption. In-house defensive cyber deception solutions are fairly rare in Norway, and the use of service providers for such solutions would be more popular. Organizations may use the inspiration of open source solutions to bring ideas to a service provider and then ask for a tailored deception solution.

Opportunity

When we say opportunity, we refer to defensive cyber deception's opportunity of growth or improvement into the future. The factor was mentioned by all our identified maturity levels. The opportunity for improvement or growth in a solution is crucial in an organization's adoption of a solution, as no one wants to have a service or product that does not get updates or improvements, making the techniques possibly obsolete a few years after implementation.

With the recently flourishing market for AI, with ChatGPT taking over headlines in news outlets, CyberSecDir mentions that they have seen an example of ChatGPT acting like a PLC and giving fake information that was believable:

> *(...) because I think the way ChatGPT can pretend to be a PLC is very exciting. And no matter which way you ask him [ChatGPT], he answers quite intelligently.*

CyberSecDir also mentions that they think that these kinds of products/tools, such as AI, can make it a lot easier to implement really intelligent deceptive environments:

> *(...) so I think tool development ala AI can make it much easier to implement proper intelligent deception environments.*

What CyberSecDir said above supports our thoughts regarding AI and opportunity. It is obvious for us that the emulation of entire environments and APIs are very difficult to perfect. In order to effectively deceive attackers, the fake systems they communicate with must be indistinguishable from the real thing. With language models and AIs such as ChatGPT in the picture, it is possible to emulate these complex systems and environments. As CloudSecArchitect stresses that it is currently hard and requires a lot of effort to emulate different APIs in order to emulate a cloud environment, but with the introduction to new GPT models and language models, it may be a lot easier to imitate or emulate a platform or interface:

> *It is currently a little complex and requires a lot of effort to emulate different APIs in order to imitate a type of cloud environment. I assume now with the introduction of new GPT models, language models, it is perhaps easier to create engines that can imitate or emulate a platform or an interface.*

OT-Engineer did not mention AI in their interview, however they have a concern, which AI could solve if defensive cyber deception can use AI to grow and improve like CyberSecDir and CloudSecArchitect envisions. OT-Engineer thinks that defensive cyber deception has to become a lot more advanced and specialized towards certain systems:

(...) I think that it [defensive cyber deception] has to become a lot more advanced and a lot more specialized towards certain systems than what we can see today.

They also mention that in order to trick an advanced attacker, you have to fake a real control system, which there is an opportunity for in ChatGPT and other more advanced AI that will be developed in the future:

(...) an advanced attacker will quickly be able to look at the systems, what they contain, what messages are being received. (...) So you have to fake a real control-system in a way.

The opportunities mentioned in the empirical data are strictly referring to AI and ChatGPT, that does not mean there are no other opportunities for its growth. The ability of the language models will only increase overtime, making deceptive environments more realistic and easier for service providers to develop products or users to implement it. We think that defensive cyber deception's ability or opportunity to get better and better could affect an organization's adoption, making it a factor in our TOE model.

5.3.2 Organization

The organization aspect of our TOE contains factors that has something to do with the organizational side of the adoption of a new technology. In our case, the factors are: Readiness, Risk, Size, Cost and C-Level Support.

Readiness

Readiness reflects the preparedness or readiness of the organization, if they have sufficient infrastructure in place. An organization could be more likely to adopt defensive cyber deception if their preparedness or readiness is high, it is crucial for an organization to have basic cyber security measures in place before they start thinking about adopting something new. This factor was mentioned by maturity level 3 and 4 during our interviews. This could also tie together with our compatibility factor, if there is nothing to be compatible to, most implementations of defensive cyber deception would not increase cyber security, thus showing the importance of a cyber security foundation and readiness in an organization.

The readiness of Norwegian organization's cyber security practices and infrastructures is not something we have studied, so we can not say for certain if organizations are ready to adopt defensive cyber deception or not. However, COO mentions in their interview that they think that our "industry" is not receptive to defensive cyber deception, that the timing is not right. They argue that we (organizations in Norway) are not ready enough yet and are still focusing on how to make better use of SOCs:

(...) but our industry is in a way not receptive yet, just as if the timing is not right. We are not mature yet. We are still figuring out how to get less false positives on the SOC. And how do we could make the SOC even better right? (...)

But why does COO think that organizations are not ready to adopt defensive cyber deception? Could it be as they state, that organizations simply are not ready yet? CyberSecDir continues with this view, saying that they have seen a lot of organizations whom has a "fairly" low level of readiness with regards to cyber security. They claim that this is due to a lack of hygiene measures and hardening and thinks that this should be in place before organizations should even consider adopting defensive cyber deception:

(...) I see a lot of organizations that are fairly low on the maturity level regarding cyber security, (...) they need to introduce hygiene measures and hardening of their cyber security before they can even consider going in the direction of cyber deception.

One of the questions we asked our interview participants was: "What do you think affects the adoption of technology at a organizational level?". The responses we received varied, and one of them, shared by the COO, mentioned "the expected degree of maturity" or "the path of maturity". This refers to what we have mentioned previously, readiness within cyber security in an organization:

> *I think it is the expected degree of maturity or the path of maturity or whatever we should call it. In other words, when organizations are trying to mature within information security, they often start with prevention, firewalls, endpoint detection response, such as antivirus, (...) then they set their sights on a SOC. (...)*

Could the fact that if an organization has only reached endpoint detection response and still has a "low" level of readiness in cyber security affect their decision to adopt defensive cyber deception? CyberSecDir states that defensive cyber deception is a very good mechanism for organizations with a sophisticated cyber security level, the existing cyber security readiness makes deception more applicable in the infrastructure:

> *I think it [defensive cyber deception] is very good as mechanism for organizations with a mature cyber security level (...) And then deception becomes more applicable.*

To summarize, readiness could be a factor that affects the adoption of defensive cyber deception. The interview participants who spoke on the subject were quite adamant that a certain level of readiness is needed, however, the exact level was not specified. An organization should at least have done basic hygiene tasks like inventory, hardening of their systems and so on.

Risk

Risk refers to the risk estimates, which are produced by the risk level towards the organization, that are done within the organization in order to identify the need for new cyber security measures. This factor was mentioned by maturity level 2 and 3 in the interviews. An example could be that an organization assess the risk they have in their infrastructure or systems, then measure what solution to implement in order to lower the risk, and in our case the solution would be defensive cyber deception.

Risk management and risk assessment is an important factor for every organization, and is crucial for identifying, controlling or reducing potential risks. While conducting the interviews, the interview participants were asked if standards, regulations, and requirements dictate what new technologies, or products their organization adopt - risk came up during the conversations frequently. Risk is an important input factor that affects their choice of cyber security controls, and is weighted more than regulatory requirements, as CISO-C argues:

> *If I speak for myself as CISO, I choose technology based on risk, not based on regulatory requirements.*

Risks are usually labeled and priorities are assigned to them. CISO-C elaborates that the risks with a high priority would be the input factor that would instigate change the most:

> *Then we will typically look at the risk that is the highest and see what technologies or organizational or administrative changes we can make to renew the risk.*

CISO-B explains that risk can also be viewed as the gap between a desired situation and an actual situation, and that this kind of assessment affects the adoption. The situations that CISO-B mentions can be anything from high priority risks to organizational goals brought forward by stakeholders. Risks varies from organization to organization:

> *How risky is it that we have a gap between the desired situation and the actual situation. It is that type of assessment that affects the adoption.*

When an organization plans on adopting a new product, CloudSecArchitect explains that requirements within an organization needs to be met in order to implement it. CloudSecArchitect mentions an example of a requirement can be the lowering of a risk, which seems to be universal for all the interview subjects that talked about risk as an input factor for the decision to adopt a new product:

> *(...) it is very often that implementation of any product is about the fact that there must be some requirement in place that is the basis for us to implement something to reduce the risk or put in place a measure.*

Risk is an important factor in regards to an organization choosing a new technology to adopt. Performing a risk assessment and then determining solutions accordingly seems like an action that most of the interviewees agree on. If the organization assesses a risk that defensive cyber deception can effectively solve or reduce, it could greatly affect their decision to adopt.

Size

Size is refers to the size of the IT/Cybersec unit in the organization. This factor was mentioned at maturity level 2 and 3. Thus, we assume that the size of an organization's IT/Cybersec unit could affect the adoption of defensive cyber deception, as if there is a lot of people in the team, there will be more hands on deck to handle the implementation process and so on.

In a previous section of this chapter, we spoke about the readiness factor and its part in our TOE model, but what affects the readiness of an organization? Could the size or the number of people working actively with cyber security within an organization affect the readiness? CISO-C argues the readiness for defensive cyber deception is low and thinks the readiness is dependent on the size of the organization:

> *My impression is that there is a relatively low maturity on it [cyber deception] in Norway. (...) I think it depends on the size of the organization*

Another mentioning of size in the empirical data was when CISO-B was asked about what could affect an organization's adoption of defensive cyber deception. CISO-B said that if there was an upside and if they had the available resources to do it, they would consider it. However, they mentioned that they do not have unlimited people/resources in their organization and that most of them are busy 100% of the time:

> *I am so simple that if it gives an upside and we have the means to implement it, (...) then we prioritize resources on that. But we do not have an infinite number of people.*

So if CISO-B wants to adopt defensive cyber deception, it could be decided by the size of their cyber security team and the number of available resources within it.

If we take a look back at the advantages/benefits mentioned in the relative advantage section, one of the most mentioned benefits was TTPs. This is a lot of information that has to processed and looked at by someone in the organization's cyber security team. So what happens if the cyber security team is already very small and is struggling with their current tasks, would they bother adopting if they knew that their size could limit the benefits they would receive from defensive cyber deception? CloudSecArchitect raises awareness on this question, stating that there are many small IT organizations around in Norway that could

implement defensive cyber deception, but it is no use implementing it if they do not have the capacity to use and learn from for example the TTPs:

> *(...) because there are many small IT organizations around in Norway that can obviously implement such functionality. But they does not have the capacity to make sufficient use of the information they receive. (...)*

The size of an organization's cyber security team could very possibly affect their decision to adopt defensive cyber deception. We mentioned that the readiness of an organization could be directly affected by the size of their cyber security team and lack of resources if they considered adopting defensive cyber deception. Small organizations could implement defensive cyber deception, but would not have the capacity to handle all the data the deceptive elements would produce.

Cost

Cost refers to the cost of implementing, maintaining or purchasing services or technology. This factor was mentioned by all of our identified maturity levels. Everything has a price, and this factor look at the cost that comes with implementing defensive cyber deception, which can have a negative impact on the adoption if it is high, and vice versa if the cost is low.

CISO-C mentions a potential cost regarding logs when implementing defensive cyber deception such as honeypots, which could have a negative impact on the adoption:

> *When you set it [honeypot] on the Internet, how will you separate the good from the bad when there are so many logs. And yes, there comes the question about cost, right? Who is gonna analyze it? How long is it going to store and take care of the logs? Taking care of logs cost money. So that is a kind of an argument that I think, with regards to the future adoption, could be a minus.*

While discussing the costs of defensive cyber deception, CyberSecConsultant is more flexible regarding it, and talks about that the price of the product has to be equivalent to the value of what the product brings to the organization:

> *The price of it always depends on the value of it [product]. It is clear that if defensive cyber deception brings huge safety, that it makes the value of the service worth it, then we're in.*

When OT-Engineer was asked if the cost of a technology, such as defensive cyber deception, was a factor when considering adopting it, they answered that it would not necessarily be a factor:

> *Not necessarily, at least not in my industry [Energy production] if the price-range isn't exaggerated. Let's say you can get an approval for a product for, let's say 10 million [NOK] if it is insanely good, and it is something that we need.*

With that said, OT-Engineer argues that a solution such as defensive cyber deception would most definitively end up being outsourced by service providers, hence the cost of implementing cyber deception would depend on the price of it as a product. CloudSecArchitect argues that in most instances, more simple deceptive solutions, such as canary tokens, are relatively cheaper than other cyber security products, as well as the cost imposed to an organization:

> *In most instances those types of services [canary token, honeypots] have been relatively cheaper than other cyber security products. Plus, the implementation also isn't something that take up a lot of time. It also has a very low impact in regards to the total cost in an organization.*

CISO-A agrees on CloudSecArchitect's statement, but makes a comment that when you have an operated solution, for example a SOC, the alarms requires follow-ups:

> *The only thing is that you would need detection on the usage of admin accounts, so it goes from the very elementary that you can implement for free to more advanced where you have an operated solution, where there needs to be a follow-up on the alarms.*

The cost of implementing defensive cyber deception may impose, as well as remove costs. When it comes to cost imposed, it can be everything from follow-ups on the alarms to handling the logs from the deceptive elements an organization has chosen to implement. Some are more strict when it comes to the cost factor, and some are more flexible where they look at the value of what defensive cyber deception can provide to an organization. If the value is worth the cost, then some may chose to adopt the technology. Elementary deceptive elements, such as canary tokens and honeypots, are relatively easy and low cost to implement, but if you want to to implement follow-ups on the alarms, the cost may increase. Generally, deceptive elements that triggers alarms create high-fidelity alarms, or in other words, reliable alarms. The amount of false-positives are extremely low, reason being that these deceptive elements should not be interacted with by anyone, and if someone does, then most probably it is an intruder. False-positive alarms can be very exhaustive and ends up consuming a lot of resources and money, but the high-fidelity alarms provided by the deceptive elements removes the cost of excessive false-positives alarms.

C-Level Support

C-Level support or support from top management is when for example the IT department in an organization gets enough funding or support from top management in order to adopt new technologies like defensive cyber deception. This factor was mentioned by maturity level 4. We believe that this is obviously an important factor, they all are, but we are not sure about the C-Level's actual involvement while adopting defensive cyber deception.

It is important that a new cyber security implementation in the organization is seen as a good thing by the top management, something to be celebrated and not just another cost for the organization. CloudSecArchitect was the only interview participant who mentioned that it is important that IT and IT security is viewed as an important part of the organization rather than just an additional cost, in order to increase the likelihood to get funds to invest into new technologies like deception:

> *(...) also what visibility does IT and IT security have up to, call it, the highest levels or say levels in the organisation? Clearly if the IT department is seen as a type of cost center instead of an important part of the organisation, this will also mean that it will receive much less funds to invest in IT security solutions.*

It is obviously important that IT security is seen as something beneficial to the organization and not just a cost, but we are not sure if the C-Level is active in the process of adopting for example defensive cyber deception, they might just allocate a yearly budget to IT and IT Security and what the department does with the money is up to them. Regardless, it is an factor that is good to consider when considering adopting defensive cyber deception.

5.3.3 Environment

This aspect concerns the environment the organization resides in. As we are focusing on the adoption of defensive cyber deception in Norway, the environmental factors like Available Expertise, Cyber Threats, Other Organizations, Rules & Regulations, Service Provider,

Standards, Education, and Graduates are seen through a Norwegian "lens". The environment is also sector based, meaning that the Cyber Threats or Rules & Regulations factors might differ between organizations

Service Provider

Service Provider reflects the available cyber security service providers within Norway and what they provide. This is a factor that was mentioned at all of our maturity levels. How does most organizations today get their cyber security technology or software, do they develop it themselves? If you develop something yourself, you have to implement it, maintain it and so on. So most organizations today purchase cyber security services from service providers. So if there is a lack of defensive cyber deception services on the market in Norway, how could this affect the adoption?

There seems to be a consensus between most of our interview participants that it is hard to find defensive cyber deception as a service in Norway today. There are also those who think this could have a negative impact on the adoption. While discussing defensive cyber deception with CyberSecConsult, they state that it is a really interesting area and they wish it was more established, but they do not think it has reached the point of being a service yet:

> *It seems like a really interesting area and I wish it was more established, but it has not reached the point of it being a service yet.(...)*

When asked about the future of defensive cyber deception in Norway, CyberSecConsult had this to say:

> *I can see it happening, I really hope it happens. But I cant imagine that without it being released as a complete service from a service provider. (...)*

Another interviewee who mentions the lack of deceptive products in the market is CyberSecDir. CyberSecDir mentions that, in the recent years, they have not heard of any deceptive products at all:

> *And in recent years I have not heard of cyber deception products at all.*

CyberSecDir also mentions that the use of more sophisticated high-interaction honeypots is service provider controlled due to the difficulty of implementing them and maintaining them and that it is not easy to just buy it as a service as the market is currently:

> *(...) And then it will be somewhat supplier controlled and now as of today, it is not easy to just go out and buy it as one, either as a product or as a service.*

When we asked CloudSecArchitect if they knew of any service providers who supplies deceptive technologies in Norway, they answered not to their knowledge. It seems like there is a severe lack of defensive cyber deception products being provided by service providers in Norway. Is there a way to change this, or is the technology just not attractive enough for providers and customers alike? CloudSecArchitect proposes a solution to this question, where deceptive techniques should be delivered as a part of the service provider's total "package", the package where all the cyber security monitoring is included:

> *I think as part of any provider that provides cyber security monitoring should take responsibility for all cyber security monitoring on your infrastructure. (...) but there are very few of the suppliers who implement honeypots as part of the total package they deliver.*

After the previous statements from the interviewees, one could get the impression that there exists zero deception products on the market today, but this is not the case according to COO and CISO-B. COO says that there exists solutions out there in the market, but they argue that they are often "over the top", which can make them unaffordable for organizations and calls it an "all or nothing approach":

> *(...) cyber deception solutions are often like that, the solutions that one can purchase out there [service providers], they are often a bit over the top. It is unaffordable for companies, it is like an all or nothing approach.*

CISO-B mentions that they know of others who sells it as a service and believes it will become more common:

> *I know of others who sell it as a service, so I think it will be more and more common. (...) I also think that there will be a service that is delivered as part of the opportunity or a part of the services that you can buy from typically MSS companies. (...)*

CloudSecArchitect shares CISO-B's opinion that deception services can become more common, due to them adopting an "assume breach" mentality, giving honeypots and canary tokens a place in their service "bundle":

> *(...) but then we are now seeing a bit of a shift. You have several suppliers who think like assume breach, and then of course the services like honeypots and canary tokens are slightly more important tools to have in their portfolio. (...)*

Most organizations nowadays do not have their own development team, thus having to rely on service providers for their software or technology. And if these providers do not offer defensive cyber deception as a part of their service, most organizations, except a few, will most likely not adopt it. Most of our interviewees had no knowledge of any existing deception services being sold in Norway and one of them who knew thought that the services were often "over the top" and unaffordable to organizations. We think that service providers can very likely affect the adoption of defensive cyber deception in Norway, because if the product is not delivered as a service, we doubt most organizations will bother to adopt it.

Standards

Standards reflect the IT/OT-standards that guides organizations cyber security decisions. This is a factor that was mentioned at all of our maturity levels. Standards are for some a guiding hand into what technologies or what best practices to follow when adopting, implementing and maintaining cyber security in their organization. For others it is what cyber security is, for example if someone is ISO-certified, they have to follow the standard and everything the standard says. Because of how many organizations use standards to guide their cyber security adoption, we think that it is an important factor for when organizations consider adopting defensive cyber deception.

As mentioned above, standards can act as a guiding hand for organizations who wants to adopt new cyber security technologies. But how much does it really affect them? CISO-B mentions that when they look for new technologies or solutions, it being mentioned in a standard helps them push the adoption further:

> *(...) it is what makes us go out and look for new technology and new solutions. It is when something is mentioned (...), or in a typical standard, such as IEC 62443, it is what helps push us further.*

CyberSecDir shares the same thought as CISO-B regarding adoption of cyber security measures within their organization, they often base it on best practices, standards or legislation:

So that when you go back and introduce your own cyber security mechanisms (...). It is often rather based on best practices or standards or legislation.

COO explains that when they are adopting new technologies, they are affected by standards such as ISO 27001 and ISO 27002 which contains guidelines and different controls one can implement into their organization. COO thinks that if defensive cyber deception was briefly mentioned in one of the standards, it could make a big difference for the adoption:

(...) you have some frameworks, safety management system it is called, for example ISO 27001 which has a kind of guideline. And then you have the 27002 which has many of the controls that you can choose to implement. Just imagine if cyber deception was a tiny bit of it. It could make a crazy big difference.

As mentioned above, IT and OT standards effect on organization's adoption decisions seem to be substantial. During our interviews, many of our interview participants commented on deception's lack of mentions in standards, such as ISO 27001 and IEC 62443. CISO-A mentions a lot of things they have read in different standards, such as vulnerability scanning, malware detection and so on, but they have yet to see a mention about defensive cyber deception:

(...) there are requirements for, among other things, vulnerability scanning and malware detection, lots of things like that I have included in the standard, but I have not yet seen anything on deceptive cyber technologies (...)

CISO-B agrees with CISO-A, saying that they have seen very little about deception in standards and that there is very little in international standards as well, stating that the reason could be that the area is under-focused or has not been given its proper place in the standards:

There is very little about deception in the standards, (...) it is possible that it is under-focused or has not been given its proper place, but I dare say that it is, there is very little in international standards (...) regarding this.

CyberSecDir continues the consensus, stating that in ISO 27001, IEC62443 and NIST2, they have seen no mentions of cyber deception at all:

(...) we typically use ISO 27001. (...) There is probably nothing that mentions anything in the direction of cyber deception there. Within the industry, one has IEC62443 (...) NIST 2 is coming and in these standards and frameworks there is also nothing about cyber deception. (...)

CloudSecArchitect mentions that many organizations within Norway are governed by "NSM's grunnprinsipper" and that these focus on securing an organization's perimeter and does not mention deceptive solutions at all:

Many are governed by, call it, NSM's basic principles, and mentions of those [deception] services are not defined at all, because there is a lot of focus on the securing of perimeter and protect the things around it. (...)

It is slightly concerning that the organizations adoption of new technologies is often based on standards and best practices, but none of our interviewees has read anything about defensive cyber deception in these standards or best practices. Why is there no mention in these standards? CyberSecDir proposes a reason for why, they think that it is the result of a lack of focus on it, that other technologies and methods get the limelight before deception:

(...) because the other things come first, i.e. out in the environment that our organization and other organizations are in, there are many other things that come into play within cyber security, and then the lack of cyber deception [in standards] is something that means that there will be a lack of focus on it.

So what could the benefits to the adoption of having defensive cyber deception mentioned in the standards be? CISO-B argues that the mentions of deceptive topic in cyber security standards or requirements could make it more attractive for service providers to sell it as a service as well as something for organizations to look for in the market:

> *(...) but I believe that if such a deceptive topic had been in the NIST standard or the ISO standard, or in the power industry's requirements, then it would clearly have become more attractive to sell as a service from the commercial actors and much more attractive from us who buy services to look for.*

They also argue that deceptive solutions could become more accessible if standards described them more often:

> *(...) techniques had been more described in the standard, then I think it [deceptive techniques] would have been more easily accessible.*

While talking about how organizations can increase their knowledge about defensive cyber deception, COO mentions that standards should mention it, have a checkbox where it is "do you have cyber deception" with a yes or no answer. They think that this could get organizations to start educate themselves on the technology:

> *Maybe industry standards should take it [defensive cyber deception] in a bit and sort of start flagging it out. Have a "do you have cyber deception", yes or no, as if there is some kind of checkpoint that you should ask yourself so that you start educating yourself.*

There seems to be a severe lack of mentions regarding defensive cyber deception in industry standards such as ISO, IEC, and NIST. This is concerning for the future adoption of defensive cyber deception in Norway because several of our interview participants mentioned how important standards and best practices were to their organization's adoption process. If deceptive techniques and technologies were included in the standards, this could lead to making defensive cyber deception more attractive to those who provide the services and those who buy them. We think that the factor Standards is a crucial component to the adoption of defensive cyber deception and that it will need a lot more mentions in standards if deceptive technologies is to become more accessible to normal organizations.

Cyber Threats

Cyber Threats reflects the threat landscape that the organization resides in, in our case: specific sectors in Norway. The factor was mentioned by all three levels of maturity in our interviews. So different organizations within different sectors would be operating within different threat landscapes. If we take for example a local groceries store, do you think they have a different threat landscape than, say a power line organization or an energy production organization, where both are defined as critical infrastructure within Norway? The reason why we have a risk factor in organization that talks about cyber risk and this one in environment that talks about cyber threats, is that everyone has a certain degree of cyber risk, but it is ultimately the environment and the cyber threats that are present in said environment that control the cyber risk towards an organization. Cyber threats towards an organization directly affect their decision to adopt defensive cyber deception, but how does it affect it?

One of the ways cyber threats can affect an organization's adoption is through funding and greater investment in cyber security within the organization. OT-Engineer raises this point in their interview, where they talk about the last year and how much has changed. They refer to the international threat level, which is the current (as of spring 2023) Ukraine conflict:

(...) If you just take a look at the last year, we have gone from crawling to being able to walk within that world [cyber security]. Accordingly, the international threat level is affecting the focus [on cyber security] and (...) how much time we use on the implementation of new systems compared to maintaining our old ones.

But could getting hacked by a cyber threat or the acknowledgement of a cyber threat in the organization's environment lead to considering adoption? COO thinks that getting hacked or understanding the threat that one can get hacked can kick off or foster innovation, leading organizations to "open their wallets" and start investing:

(...) there is one thing that kicks off or fosters innovation, and that's when you've already been hacked. When you see that your defenses have been crushed, it is like, damn it, now we have to open the wallet here. (...) there is the threat and the understanding that this can happen.

While being asked about what they think affects the adoption of defensive cyber deception, CyberSecDir mentions that they believe the threat landscape and media headlines affect it a lot. The threat example mentioned by CyberSecDir was ransomware and that many organizations chose to deal with this threat with for example insurance against it:

Threat landscape and media headlines affects it a lot. Most people now talk to insurance companies about the cost to insure against ransomware, that is because in the last few years the headlines have been influenced by ransomware. (...) So media and what the media focuses on, and what there is a lot of, namely ransomware, phishing and fraud, it affects the decisions a lot.

CISO-B also agrees that the threat landscape/cyber threats affect the adoption of deceptive technologies as well how they manage existing cyber security measures within their organization. Being in the energy business, with the current world climate, it is important that the organization is safe against potential cyber threats that could halt their operations:

(...) It is clear that the threat landscape generally absolutely influences the way we manage both traditional defense mechanisms and deceptive defense mechanisms. It is obvious that the threat landscape operates a lot of the work today. (...) especially because we are a major producer of [redacted], (...) So it [threat landscape] affects a lot.

COO thinks that many of today's threat actors against organizations in Norway are looking for information to sell or different ways they can make profit of the organizations they compromise:

Many threat actors are looking for information or looking to make money of you and often money can be made from the information they steal from you.

These kinds of attacks are often done through ransomware. But is defensive cyber deception an effective tool as a defense mechanism against the different cyber threats found in the Norwegian threat landscape today? There has been some mentioning of deception's impact against ransomware attacks in the relative advantage factor and COO thinks that it could be an effective tool against ransomware threats:

(...) For example, we can attract ransomware attackers with deception that causes them to encrypt the wrong files or they delete the wrong backup. (...)

The cyber threats or the threat landscape that sectors in Norway find themselves in today varies, some are affected by the Ukraine conflict and some are still affected by ransomware groups and groups that just want to make quick money of them. Defensive cyber deception can be useful against the later mentioned threats as stated by COO and others in the relative advantage factor. So could cyber threats affect the adoption decision in organizations? We think so, because more cyber threats could lead to more money or investment into cyber security which in turn could lead to the adoption of defensive cyber deception.

Available Expertise

Available Expertise refers to the available expertise of defensive cyber deception in Norway. This factor was mentioned by all the maturity levels. In other words, it is a factor that looks at the availability of cyber security professionals in Norway that have experience with defensive cyber deception. If the available expertise is low in Norway, it could explain the low popularity of defensive cyber deception in Norway, and vice versa.

CyberSecConsultant believes that the market for defensive cyber deception is very small and the available expertise of it is not so widespread, even though it sounds like something organizations could benefit from:

> *(...) I think with cyber deception in Norway, the market for it is very small, it is incredibly niche. (...) it sounds like it is something we can benefit from, but the available expertise is not so widespread.*

OT-Engineer has the same thoughts about the available expertise as CyberSecConsultant, arguing that the available expertise of defensive cyber deception in Norway is depressingly low. OT-Engineer also mentions some vendors they have been in touch with that provide deceptive solutions, but their solutions was not good enough for them on the OT side. They are currently in the process of changing service providers within their organization:

> *There are extremely few, and just as an example, we are currently changing service provider, it is a different organization, you will probably find out about it on the Internet. They will deliver some services to OT, and what we've seen for now is relatively depressing, and this is an international, or at least a European organization. We've been on the market to search for people, and yeah, it is depressing.*

CISO-A and CISO-B agrees that the available expertise for defensive cyber deception in Norway is quite lackluster. CISO-B explains that defensive cyber deception is an area that is a little unripe for them, and they are not aware of what kind of expertise exists in the area of defensive cyber deception:

> *(...) As for defensive cyber deception, I do not actually know what kind of expertise exists in that area. (...) it is still an area that is a little immature for me. (...)*

CloudSecArchitect briefly mentions that most of the traditional cyber security experts in Norway focus mainly on SOC and monitoring, but nothing on defensive cyber deception, which might be the reason for the absence of available expertise within Norway. COO has the same view on the available expertise of cyber deception as CloudSecArchitect. COO explains that, from personal experience, the available expertise of defensive cyber deception is limited in Norway, and that people have the wrong perception of cyber deception:

> *I feel like the knowledge of cyber deception is very, very low, and I think this has something to do with people learned about cyber deception a long time ago, because those who have been in the industry for a long time, they learned that cyber deception is honeypots that you place somewhere on the Internet. This is not true. It is far more than that. A honeypot is a tool that you can choose to use in a larger cyber deception strategy and implementation. So I think subjectively, from my experience, the available expertise is very low when it comes to cyber deception.*

CyberSecDir talks about the absence of cyber security expertise in general, as everything is getting more and more digitalized, but there is inadequate capacity and expertise to guide this digitalization:

> *In general, in terms of cyber security, it is completely lights out. There is not enough capacity and expertise in relation to what is needed. It is a bit of a perfect storm that I talk about a lot, that we throw more and more of our values in society into a digital world or ruled by a digital world. (...)*

CISO-C had a different approach on the matter. They mention that some networking environments, such as Telenor and ISPs, have high readiness on defensive cyber deception due to their networking competence and high degree of exposure:

> *I believe that in some networking environments that works heavily towards Internet, let's say Telenor and ISPs, are relatively mature on the subject, because there exists a project within telecommunication called ADLOG or something like that. It is a type of token ring of honeypots which is used as a collaboration. They exchange information about how these honeypots are being used or misused, so I believe within ISP business the maturity is relatively high, and that is because the networking competence and the degree of exposure is high.*

With that said, CISO-C argues that outside of the network environments as mentioned above, the available expertise of defensive cyber deception is fairly low.

It is very obvious from the answers by the interview participants that the available expertise of defensive cyber deception in Norway is very low. They all agree that the available expertise of it in Norway is quite lackluster. The reason for the absence of available expertise is closely linked to what CyberSecDir mentioned regarding the overall shortage of cyber security expertise within Norway. Organizations may prioritize refining their existing technologies rather than actively seeking new and effective solutions.

Other Organizations

Other Organizations reflects the learnings and influences an organization may get from other organizations' cyber security practices. This factor was mentioned in all three of our present maturity levels. We think that the methods or techniques or practices used by other organizations could affect an organization's adoption decision. Personally, while buying a product or service, it would help immensely if a friend or colleague had good things to say about the product and it would also affect us negatively if the friend had negative things to say, making us steer away from the product or service. We believe this could translate over to cyber security professionals, hearing about other professionals experiences with defensive cyber deception could affect their own decision to adopt.

In today's cyber security or IT industry, conferences are very common. Conferences are used for selling products, networking with fellow cyber security peers and sharing experiences and expertise, among other things. Quite a few of our interview participants mentions conferences as a great place to learn from other organizations regarding what to do and what not to do. CISO-C mentions that in their experience, when people are attending conferences or network meetings, they are most interested in hearing about how certain technologies has worked for other organizations and notes that this is a crucial component for adoption:

> *People are most interested in, during conferences or network meetings (...) people are very interested to hear about what has worked for other organizations. And that is an crucial component for the adoption of something, if other people or organizations has had an good experience with it.*

When asked about how other organizations affect their adoption of technologies like defensive cyber deception, OT-Engineer shares CISO-C's view that conferences and forums is a great way to see what others have done and show what they have done as well:

> *Yes, I would say a lot, to a large extent. After all, we are around at type of large and small conferences and type of forums (...) look at what others have done and others look at what we have done to get inspiration and possibly move on in relation to technology choice then.*

CyberSecDir shares OT-Engineer and CISO-C's consensus of conferences and other gatherings being useful in order to learn what other organizations are doing. But they are a bit sceptic towards the lack of information about the organization's actual experience with the technology, they often do not show if the technology works as they advertise it:

> *It is very useful to go to conferences, courses and seminars, and to hear about cyber security programs and projects that various organizations are doing. But then, there is a little limited information about what experiences they have had, (...) we do not know if it works.*

While trying to learn from other organizations, should one have an elite-bias or not? Should you only look to large organizations that have a high level of readiness due to their size and investments? CISO-B does not look at size while looking at other organizations, they state that as long as an organization has a clever idea, they are willing to learn and get inspired by them:

> *We get inspired by anyone who is clever, whether they are small or large organizations, as long as they have hatched a concept that works and we see that it will give us added value (...). There are a lot of clever people, so we can just sit and absorb.*

CISO-A is a special case among the interview participants, as they are a CISO in an organization that specialized within cyber security, the organization travels abroad on conferences to look at what other people are doing and does not focus too much on what other organizations are doing in Norway:

> *(...) But it also means that we go out of the country a bit for conferences and a bit of other things and see what's there and then. Yes, I am. I follow what others are doing, but no, I really listen more to what happens internally.*

CISO-C raises the point that today, there are so many service providers and sales representatives that wants to sell you a product, that it makes it impossible to know which product is good and which is bad. They note that if a colleague or an other organization has had an positive experience with a product, it makes the sale towards their organization a lot easier:

> *(...) There are so many service providers and sales representatives out there that (...) makes it impossible to know which product is good and which is bad. But if a colleague, fellow CISO or a cyber security organization has deployed something and has had an positive experience with it, it makes the sale towards my organization or the organization in general a lot easier. (...)*

It is nice to see that many of our interview participants are learning from other organizations and well as giving back and teaching themselves. It seems like most of the interviewees are positive that other organizations can affect the adoption of defensive cyber deception and that it can help organizations chose between good and bad products from their cyber security measures. There was also the concern that the actual experience from a product or service is not discussed enough but hopefully this is not the norm in information sharing between organizations.

Rules & Regulations

Rules & Regulations reflects the rules and regulations that affect the organization directly in their sector/domain, and is the most dynamic of the environment factors. This factor was mentioned by maturity level 2 and 3 during our interviews. Some organizations may operate within healthcare, energy, etc. This affects what rules and regulations they have to follow as an organization in general as well as the rules and regulations that affect their cyber security practices. If there were some small mentions of defensive cyber deception in the rules and regulations an organization follows, it could affect the decision to adopt, and vice versa.

CISO-C mentions that there are not much rules and regulations that dictate what their organization should adopt or not, but rather their cyber risk and value assessment that could regulate or affect the activity level on capital business:

> *Right now in my organization, we aren't regulated by something in particular (...). It is the cyber risk, value assessment and pen-testing that regulates or affects the activity level on investor business, on capital business.*

CISO-A agrees with CISO-C that there is an input factor from risk that affects what their organizations chooses to adopt, rather than laws and regulations. They also argue that a government fails if they start requiring specific technologies:

> *The government fails if they start requiring specific technologies (...). In a way, it is the input factor from a risk, a total risk assessment rather than laws and regulations.*

CISO-B talks more about the lack of deception in the standards, rules and regulations, that there is nothing about deception in them. CyberSecDir shares CISO-B's opinion that there is a lack of mentions of defensive cyber deception in rules and regulations, and argues that other things comes before deception:

> *Yes because the other things comes before it [cyber deception], so out there in the environment that our business and other businesses stand in there are many other things that comes on the field within cyber security, and then the lack of cyber deception makes it something which is not being focused on.*

The adoption of certain technologies or practices by organizations within various sectors may not be directly influenced by applicable rules and regulations. This could be attributed to the absence of specific regulations that are designed to govern or address those particular technologies or practices. Risk is a more important factor for them, when it comes to adopting new solutions or technologies. As CISO-A commented, a government can not just start demanding or requiring specific technologies, which is also why defensive cyber deception can not just be thrown into rules and regulations and be required to be implemented. This means that defensive cyber deception needs to be objectively acknowledged and proven in order to contribute as a value for a risk. If this ends up being true, then slight mentions of it in rules and regulations could definitely have an influence on an organization's decision to adopt defensive cyber deception.

Education

Education refers to the the education available for cyber security professionals, enthusiasts, or students regarding defensive cyber deception. This factor was only mentioned by maturity level 4. More specifically, the factor describes the availability of lectures, conferences, tech news outlets that has defensive cyber deception in their agenda. If cyber security professionals had the opportunity to attend lectures and stay updated through news outlets on defensive cyber deception, and students could enroll in cyber security degrees that include

defensive cyber deception as part of their coursework, the increased awareness of its benefits could potentially influence the decision to adopt.

There were not many mentions of education while conducting the interviews, but COO had some comments regarding it. COO mentioned that education will be a big part on the future adoption of defensive cyber deception:

> *Yes, when we are able to educate, when we are able to explain and create frameworks and implementation guides for how to raise the bar just a little bit.*

When asked about how organization's should increase their readiness within defensive cyber deception, COO mentioned education again:

> *It is about education, really, reading and learning and maybe something like [Norwegian tech/it news outlets], maybe they'll start writing a little more about that topic.*

Even though the education factor was only briefly discussed with COO, they made a good point regarding educating people would raise the bar just a little bit. This small raise of awareness of defensive cyber deception is a great first move into making people understand how organizations can benefit from it. If professionals or enthusiasts, or even academic students are educated regarding defensive cyber deception, more people would start vouching for it, and it could affect the decision to adopt it in the future.

Graduates

Graduates reflects the new generation of employees/graduates that bring fresh ideas and a new pair of eyes with regards to cyber security practices and techniques. This factor was only mentioned by maturity level 4. This means that when newly graduated employees start a new position within an organization that works with cyber security, their mindset may differ from the ones that have been in the industry for decades. The change in mindset could instigate a change within the organization, making it more open for new promising ideas, which can affect the decision to adopt defensive cyber deception.

COO was the only interview participant that mentioned anything about graduates, which they referred to as "fresh blood". Their point was that the old generation will be replaced by the wave of new generations wants to take cyber security seriously and that they understand the consequences if the defenses fail, and wants to see it blossom:

> *The expertise has begun to grow and blossom very well within cyber defense. (...) the old cyber security chiefs and so on, are on their way out, and there is room for new blood, fresh blood that wants to see things that work. They actually want to take things seriously, and they understand the consequences that follows if they do not take it seriously.*

The graduates factor only came up once during the interviews, but COO made a valid point when they say that the old generation will be replaced by a new one that are not afraid to make changes if it is for the greater good. Experienced cyber professionals who have been in the industry for several decades may have a tendency to be conservative and prefer to rely on what they are already familiar with rather than embracing new technologies or approaches. The wave of a new generation will be more open to new ideas, and as COO mentioned, they want to see things that work. If defensive cyber deception is perceived as a valuable solution that offers benefits to the adopter, the new generation of employees are likely to be more open to the idea of adopting it.

Chapter 6

Discussion

In this chapter of our thesis, we will be looking at the theoretical and practical implications of our research, as well as the thesis' limitations and its directions for future research.

6.1 Theoretical Implications

In this section of our thesis, we will be looking at the theoretical implications of our research and thesis. We have identified three main theoretical implications, those being: A brand new TOE framework for defensive cyber deception, the awareness versus the adoption of defensive cyber deception among our interview participants, and a prototype of a maturity model for defensive cyber deception.

6.1.1 New TOE framework for Defensive Cyber Deception

Our TOE model is shown in Figure 5.3. It has the three main aspects and 18 factors spread across the aspects. The TOE model contains the three original TOE aspects: Technology, Organization, and Environment, as we did not see a need to add additional aspects from the extended TOE Framework for cyber security proposed by Wallace et al. (2021). In their framework, they present two additional aspects, the Cyber Catalysts and Practise Standards, which did not fit with the answers we got from interview participants. The one thing that was mentioned a lot in the interviews that coincide with one of the cyber catalyst factors was cyber risk. However, we decided to place cyber risk under organizational risk, because everything within organizations is getting digitalized, the cyber risk towards an organization translates to a risk of the organization's functions and well being.

We have chosen to present the top factor of each of our three aspects, Readiness, Compatibility and Service Provider, we will be discussing why we deem these factors more important than others:

Readiness is deemed as a more significant factor than others, reason being that an organization needs to be on a higher maturity level in order to be able to implement defensive cyber deception as a solution. From the empirical findings, it seems that Norwegian organizations are not mature enough yet, and are either focusing on perfecting what they already have, or they focus their resources on perfecting the use of SOCs. When we say that they are perfecting what they already have, we refer to the organizations performing "hygiene measures" on their cyber infrastructure. "Hygiene measures" is a term used by one of our interviewees which describes introducing good architecture, good hygiene regarding patching and maintenance, and general detection capacity (IDS/IPS). We find it strange that neither the readiness nor the maturity of the existing cyber security environment in an organization

was mentioned in TOE framework presented by Wallace et al. (2021). All the aforementioned measures are necessary for an organization to reach a certain degree of high maturity in order to be ready to consider adopting more advanced defensive cyber deception. Some mentions in the empirical data is that the maturity of the cyber security in a lot of Norwegian organizations is fairly low, the idea that the timing of defensive cyber deception is not ideal. The timing is not ideal due to the earlier mentions of the lack of hygiene measures and readiness in general in Norwegian organizations. They are not receptive to defensive cyber deception. As the level of maturity in organizations' cyber security increases, the conditions for the adoption of defensive cyber deception become more favorable, and organizations become more open to the concept. The readiness of an organization plays a crucial role in the decision-making process of the adoption. If an organization is not adequately prepared to adopt defensive cyber deception, it can greatly influence their choice to refrain from implementing it. Therefore, readiness stands out as a vital factor that holds greater significance compared to others.

The integration of defensive cyber deception with existing cyber security products or services within an organization's cyber security infrastructure is of utmost importance for its adoption, as it is recognized that no single technique or product is sufficient on its own. Wallace et al. (2021) mentioned in their paper that technology integration did not surface as a adoption factor in their cyber security TOE model. We find this strange, as our empirical data emphasises the importance of the compatibility or integration of the new technology that is being adopted into their existing infrastructure. When our interview participants seek to adopt new products, it is crucial for them that the product is compatible with their existing infrastructure. This is because organizations are reluctant to undergo significant rearrangements and restructuring of their cyber security architecture solely to accommodate a single product. The interview participants who have practical experience with defensive cyber deception assert that it is already seamlessly compatible and integrated with various existing perimeter functionalities, including IDS/IPS, logging, SIEM, firewalls, and others. Our literature findings also state that defensive cyber deception can be integrated with existing functionalities with minimal effort (Steingartner et al., 2021). An example of the compatibility of defensive cyber deception, as reveled in our empirical data, is the integration of honey users with existing SIEM technologies that use log analysis, which could help keep track of the honey users and mark them as such in the cyber security environment. Our empirical data emphasize that compatibility is regarded as a crucial factor on the decision to adopt defensive cyber deception, which is why it is considered more important compared to others. Fortunately, the empirical data confirms that defensive cyber deception is already compatible with existing cyber security technologies, further facilitating the decision to adopt it as a strategic cyber security solution.

There was a debate regarding if service providers or standards was the more important factor, but it was decided that service providers played a more significant role in the decision-making process of adopting defensive cyber deception, particularly for Norwegian organizations that prefer outsourcing their cyber security monitoring instead of developing in-house monitoring capabilities. This allows organizations to allocate resources efficiently and rely on service providers to implement and maintain cyber security solutions on their behalf. In the extended cyber security TOE by Wallace et al. (2021), they propose the factor "Tech Provider" rather than Service Provider. This factor is under the technology aspect. We argue that the Service Provider factor is valid in our case of the adoption of defensive cyber deception, as organizations would purchase both the technology and the service of implementation, maintenance and support, rather than just purchasing the technology as in the extended cyber security TOE. However, our empirical data indicate a consensus regarding the lack of defensive cyber deception products by the available service providers. While some acknowledged the existence of some service providers offering defensive cyber deception, their quality was deemed

inadequate. Furthermore, it was highlighted that the few available defensive cyber deception products are often financially inaccessible. The availability of service providers offering affordable and effective defensive cyber deception solutions would significantly impact the adoption rate, which is why the service provider factor is considered as more crucial than others.

We discussed the top factor from each of the TOE aspects, and we will proceed to discuss two of the factors that are distinctive to our TOE model, compared to the existing TOE for Cyber Security (Wallace et al., 2021): Graduates and Opportunity:

The graduates factor, which is located in the environment aspect, examines the new generation of employees within an organization. The emerging generation of employees within an organization, whether they are recent graduates or self-taught individuals, are expected to bring a fresh perspective and novel ideas regarding existing cyber security technologies and techniques. The empirical data argues that the graduates want to do things seriously, and that they are aware of the consequences that could follow if cyber security is not taken seriously. Aligned with this perspective, as prospective graduates within an organization, we anticipate leveraging our insights and fresh perspective to critically evaluate cyber security measures and potentially enhance them based on the knowledge and expertise we have gained during our studies. The graduates factor was not present in the extended TOE framework (Wallace et al., 2021).

The opportunity factor which is located in the technology aspect refers to defensive cyber deception's opportunity of growth or improvements in the future. There were numerous mentions regarding ChatGPT in the empirical data, regarding how ChatGPT can pretend to be a PLC and that its answers are quite intelligent. The empirical data also mentions that these kind of AI tool developments could make it easier to implement proper intelligent deception environments. We agree that one of the challenges associated with these sophisticated deception environments lies in the creation process. How can an organization develop an environment that can deceive even the most advanced attacker? This opportunity could entice organizations which have previously been sceptical towards advanced defensive cyber deception techniques, due to its complexity and cost. This was mentioned in the empirical data, indicating that for organizations to adopt defensive cyber deception, it would require sophistication and specialization tailored to specific systems within their environments. A part of our literature findings' research is on the usage of machine-learning and AI for scalable and automated generation of realistic deceptions (Liebowitz et al., 2021), which illustrates that defensive cyber deception with AI and/or machine-learning is attainable and an opportunity for the future.

6.1.2 Understanding participants' awareness vs. Adoption of defensive cyber deception

After conducting our interviews, it seems like the majority of the interview participants are aware of defensive cyber deception and know of its existence, but still some of the interview participants have not adopted it. Why is it that they have heard of it, but not adopted it? The empirical data stated that many of the interview participants rely on service providers, and emphasize that if they ever consider adopting defensive cyber deception, it would be as a product from a service provider. A question that emerges then is, are there any deceptive products from the service providers, or are they even good? From the empirical findings, there are not any providers who supply deceptive technologies in Norway. Conversely, some interview participants says that there exists solutions on the market, but that they are expensive and are often unaffordable. In addition to the prohibitive prices of the deceptive technology products offered by service providers, the empirical findings ex-

plain that the service providers they have been in touch with are European organization, which offer solutions that are poor. The lackluster of deceptive products provided by service providers is not limited to Norway, it seems like it could be an issue across Europe in general.

Our empirical findings explains the reason why some would prefer outsourcing defensive cyber deception, rather than building it in-house. The preference of outsourcing is tied with if one seeks a more intricate defensive cyber deception solution in order to combat more sophisticated attackers, it would increase the complexity significantly. Our literature findings state a similar thought, that deploying and managing cyber deception in real-life operational networks is extremely complex (Islam and Al-Shaer, 2020; Liebowitz et al., 2021; Sajid et al., 2020), time consuming (Islam and Al-Shaer, 2020), and costly (Islam, Dutta, et al., 2021). Contrarily, a small part of our literature findings and empirical data state that complexity is not generally the case with defensive cyber deception, reason being that deception integrate with existing systems in a way that requires minimal effort to deploy, operate, and manage (Steingartner et al., 2021). This contradiction may hold true for less sophisticated deceptive elements, in contrast to the more advanced solutions discussed in the literature, which involve machine-learning or autonomous technologies like DodgeTron (Sajid et al., 2020). The perceived complexity of these solutions is subjective and contingent upon an individual's knowledge and expertise in the field of defensive cyber deception. For someone with a lower maturity level, a honeynet integrated with SDN might appear complex and unattainable, whereas those with a higher level of maturity may consider it relatively straightforward. In essence, the notion of complexity is relative.

The absence of available products from service providers may be tied with the lack of available expertise regarding defensive cyber deception in Norway, and Europe in general, and mentions in standards. The empirical data state that there are only a handful of service providers that sell defensive cyber deception as a product, and these products are either poor or unafforable, the maturity of the available defensive cyber deception products are fairly low. Contradictory, our literature findings state that there are several mature and sophisticated defensive deception solutions by providers such as: Attivo, Countercraft, Thinkst, TrapX, among others (Liebowitz et al., 2021). These mentioned companies that offer defensive cyber deception as a product are originally based outside of Europe, so we are not certain about their involvement as service providers in the market environment of the organizations we have gathered data from. In regards to the service providers within the market environment, it makes sense why they do not put in too much effort into selling a viable defensive cyber deception solution, because as our empirical data state, most organizations are focusing on perfecting what they have, which is firewalls, anti-virus, endpoint-detection, and SOC, among others. The demand for the aforementioned mechanisms are significantly higher than the demand for defensive cyber deception, prompting service providers to prioritize the refinement of their solutions to cater to market needs. If the conventional approach of relying on perimeter cyber security and fortifying existing defenses remains the preferred choice, service providers will keep adapting their solutions to cater specifically to that market segment.

Traditional cyber security features that the organizations are focusing on perfecting can successfully prevent many cyber attacks (Cifranic et al., 2020), but the sole reliance on perimeter cyber security will pose as a problem that will never guarantee any security (Acosta et al., 2020) against sophisticated attacker, as most of the traditional cyber security features are reactive (Liebowitz et al., 2021). Our literature findings cite to Symantec (2018), which state that well-resourced attackers are able to evade current perimeter cyber security systems and gain stealthy access to the target system and its assets. A few other of our literature findings comment on exactly this, that reactive cyber security mechanisms did not prove to be effective against stealthy attacks (Ajmal et al., 2021). Our literature findings also cite to Duan

et al. (2018) where it is explained that skilled attackers can easily avoid static signature-based detection through exhaustive reconnaissance, fingerprinting, and social engineering in order to remain stealthy. The literature findings refer to defensive cyber deception as a promising defense that will break the defender's asymmetry (Islam and Al-Shaer, 2020; Islam, Dutta, et al., 2021; Sun et al., 2020). As our empirical data explains, organizations and service providers persist in relying on traditional reactive measures rather than adopting more proactive approaches, the asymmetry will not change and the attackers will always have the upper-hand by only needing to be right once (Cifranic et al., 2020).

The absence of references to defensive cyber deception in standards was briefly mentioned. We want to delve into the potential reasons behind individuals being aware of defensive cyber deception but opting not to implement it. As described in our Standards section in Results, standards serve as a guiding hand for organizations' cyber security decisions. They provide a framework for selecting technologies and best practices in cyber security. Some view standards as the definitive reference for security, such as ISO certification requirements that mandate strict compliance to the standard's guidelines. The emphasis on ISO certification in an organization may lead to a reduced likelihood of considering the adoption of defensive cyber deception techniques. Similarly, organizations not bound by any specific standard face a comparable situation, as the absence of references to defensive cyber deception in other applicable standards further reinforces the limited awareness and consideration of such techniques among Norwegian organizations. A part of our empirical data highlighted precisely this point, emphasizing that the absence of defenive cyber deception in standards leads to a lack of focus on its implementation and consideration. According to the empirical data, even a small inclusion of defensive cyber deception references in standards like ISO 27001/ISO 27002 or "NSM's grunnprinsipper", could have a significant impact into the consideration and adoption of it. Our literature findings does not mention anything regards to the mentioning of defensive cyber deception in standards.

6.1.3 Maturity estimate model

We have also created a maturity estimate model. You could also call it a prototype of maturity model for defensive cyber deception. It is a one-dimensional model and it operates around the subject's prior knowledge about defensive cyber deception techniques such as honeypots, canary tokens and SDN. If the subject only has knowledge about canary tokens, they will be put into level 1 and so on. We acknowledge that the maturity model we developed is limited because of its one-dimensionality. Nonetheless, we find that its capacity to categorize the studied organizations based on their maturity at different levels adds depth to our analysis. The improvements and further development of this maturity estimate model is something that we wish to happen, as we have not identified a maturity model specifically created for defensive cyber deception.

6.2 Practical Implications

In this section of the chapter, we will be discussing the practical implications to the industry that our research presents. We have identified three main practical implications: Spreading the awareness of the benefits of defensive cyber deception, spreading the awareness of defensive cyber deception in Norwegian research, and how our thesis and framework can aid organizations who are considering the adoption of defensive cyber deception.

6.2.1 Awareness of the benefits of defensive cyber deception

In the relative advantage factor of our findings chapter, we presented the different benefits/advantages an organization can expect from implementing defensive cyber deception into

their cyber security systems. We hope that our findings from the empirical data and our literature review can spread the awareness of why an organization should adopt defensive cyber deception and what benefits they can get from doing it. The benefits which were identified in our literature findings are the following: Detection, Disruption, Depletion, Misinformation, Deflection, Discovery, and Deterrence. The relative advantages or benefits we identified in our data analysis were focused on early detection and disruption, with there being several mentions of it throughout our empirical data. There was also a large focus on the Discovery benefits in the empirical data, learning from the attacker's TTPs, learning about their tactics, techniques and procedures through honeypots, deceptive environments and canary tokens in order to understand the attacker. We hope that these mentioned benefits can help encourage and spread awareness of the usefulness of defensive cyber deception for organizations in the practical sense in their day-to-day cyber security operations.

6.2.2 Awareness of defensive cyber deception in Norwegian research

When our thesis is released, it will be the only TOE framework for defensive cyber deception that we have knowledge of. We have not discovered other TOE frameworks for specifically deception, we have discovered one for cyber security which was mentioned in our Theoretical Lens chapter (Wallace et al., 2021), but not specifically for defensive cyber deception. As the interview participants were from Norway, we have set the scope of our model to Norway, which makes this research on Norwegian organization's adoption of defensive cyber deception. We hope that our thesis will inspire researches and make them more interested in researching defensive cyber deception, the research does not have to be about adoption, it could be a case study of an organization that is actually using defensive cyber deception.

6.2.3 Aiding the adoption of defensive cyber deception in Norway

With the new presence of a TOE framework specifically made for defensive cyber deception, we hope that our framework can aid organizations who are considering adopting defensive cyber deception. The organizations can take a look at the different factors we have identified and see if they meet the "requirements" or if they are missing something that should be in place before they consider adoption. The existence of our TOE framework could also serve as encouragement to organizations which has been considering the adoption, but were not sure where to start or what they should have present in their infrastructure before they start their adoption.

6.3 Limitations & Directions for future research

Although the thesis is done and delivered, there are still some limitations we have identified throughout this period which we would like to address. These limitations are not detrimental to our thesis, but they would be nice to consider for someone who is thinking of doing the same type of research as us: Lack of validation of our TOE model, too broad selection of organizations, maturity estimate model, lack of practical empirical data regarding defensive cyber deception, and the size and expertise of our interview participant pool.

Using the limitations we have discovered, we will be presenting possibilities for future research that could help combat the previously mentioned limitations:

One direction for the future research of our TOE framework is the validation of it. Our framework for defensive cyber deception is the first of its kind and we hope that others will continue improving the factors and aspects we have identified through our research. This could be done through interviews with people who has experience in the adoption of defensive cyber deception, so the future researchers would have to do something we would not do,

gather eight to ten interview participants with hands-on experience with the adoption of the techniques and technology.

While making our framework, we thought that factors that are present in the environment aspect could change greatly based upon in which sector the organizations are located. In our current framework, most of the organizations are from different sectors, making the framework quite broad. We think it could be interesting to focus on either a specific type of organization, for example hospitals, or a specific type of sector within Norway, for example healthcare. If the framework is tailored towards a specific type of organization or sector, maybe the organizations within this sector or organization types will have a higher probability of adopting defensive cyber deception.

In our thesis, we have presented a maturity estimate model for defensive cyber deception. However, as it currently is a one-dimensional model, we see a opportunity for researchers to create a more sophisticated maturity model for defensive cyber deception. The model could be useful in the future if the level of adoption of defensive cyber deception in Norway rises. One could measure organization's level of maturity more efficiently and perhaps do some research based on this.

Our research and analysis has not provided any practical evidence that directly demonstrates the effectiveness of defensive cyber deception. However, conducting a comprehensive case study would likely have a significant impact on the adoption rate of defensive cyber deception in Norway. Through a case study, one could provide a practical example of how defensive cyber deception works and its actual effectiveness. Additionally, the study could offer insights on implementation strategies and recommendations based on our own implementation experience. Despite our efforts, we were unable to find an organization in Norway willing to participate in the case study. For researchers interested in conducting similar studies, incorporating a case study would greatly enhance the research process and outcomes.

As stated in our research approach chapter, we had eight different interview participants from six different organizations within Norway. We had to settle on our number of interview participants due to both a lack of time towards the end of data collection and the lack of connections at the start of data collection. Ideally, we would have liked to have a larger number of both interview participants and different organizations. We think that a larger participation in interviews would have an enriching effect on the empirical data and could lead to the discovery of new factors or make the argument for the existing factors even stronger.

When we first started our research on defensive cyber deception in Norway, we wanted to interview people within organizations that had experience with the implementation and maintenance of defensive cyber deception technologies. However, as we continued trying to get interview participants with hands-on experience, we noticed how challenging it was and that we would have an insufficient amount of data to work with. It would be interesting to see what a participation pool made up by professionals who all have hands-on experience with the implementation and maintenance of defensive cyber deception thinks affects the adoption of it within organizations.

Chapter 7

Conclusion

Defensive cyber deception is an approach on cyber security that can provide defenders with many benefits to their cyber security infrastructure, such as detection, disruption, misinformation, among others. Despite its stated benefits in the literature, it has not been extensively adopted like the more traditional cyber security measures such as IDS or IPS. We started our thesis with a question: "What affects the adoption of defensive cyber deception in organizations in Norway?". Through our work with both the literature review and the analysis of our empirical data, our findings suggest that there are eighteen different factors within the three different aspects of our TOE model that affect the adoption. Our key findings from our research is the top factors from the three different aspects within our TOE model, being Readiness, Compatibility and Service Providers. Readiness refers to the existing level of cyber security and practices an organization has, so if an organization wants to adopt defensive cyber deception, they should have the basics down first, like patching etc. Compatibility refers to defensive cyber deception's integration possibilities with what the organizations already have in their cyber security infrastructure, and Service Providers refers to the existence of suppliers/providers of defensive cyber deception in the organization's environment, in our case, Norway. We have discovered that these factors are crucial to an organization's adoption of defensive cyber deception. We also discovered seven different cyber security benefits an organization can expect if they implement and use defensive cyber deception in the intended manner, which include early detection, disruption, depletion, misinformation, deflection, discovery, and deterrence. We hope that our model will be of use, in both the theoretical and practical sense, and that other researchers or fellow master students can continue the research of defensive cyber deception in Norway using our TOE model as their base or inspiration.

Bibliography

Acosta, J. C., Basak, A., Kiekintveld, C., Leslie, N., & Kamhoua, C. (2020). Cybersecurity deception experimentation system. *2020 IEEE Secure Development (SecDev)*, 34–40.

Ajmal, A. B., Alam, M., Khaliq, A. A., Khan, S., Qadir, Z., & Mahmud, M. P. (2021). Last line of defense: Reliability through inducing cyber threat hunting with deception in scada networks. *IEEE Access*, *9*, 126789–126800.

Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060.

ATT&CK. (2023). *Mitre att&ck* [Accessed: 2023-04-17]. https://attack.mitre.org/

Bennett, M., & Waltz, E. (2007). *Counterdeception principles and applications for national security*. Artech House.

Briggs, B. (2019). Hackers hit norsk hydro with ransomware. the company responded with transparency. https://news.microsoft.com/source/features/digital-transformation/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

Bryan, J. D., & Zuva, T. (2021). A review on tam and toe framework progression and how these models integrate. *Advances in Science, Technology and Engineering Systems Journal*, *6*(3), 137–145.

Buller, D. B., & Burgoon, J. K. (1996). Interpersonal deception theory. *Communication theory*, *6*(3), 203–242.

Butavicius, M., Taib, R., & Han, S. J. (2022). Why people keep falling for phishing scams: The effects of time pressure and deception cues on the detection of phishing emails. *Computers & Security*, *123*, 102937.

Chatterjee, S., Rana, N. P., Dwivedi, Y. K., & Baabdullah, A. M. (2021). Understanding ai adoption in manufacturing and production firms using an integrated tam-toe model. *Technological Forecasting and Social Change*, *170*, 120880.

Chiang, C.-Y. J., Gottlieb, Y. M., Sugrim, S. J., Chadha, R., Serban, C., Poylisher, A., Marvel, L. M., & Santos, J. (2016). Acyds: An adaptive cyber deception system. *MILCOM 2016-2016 IEEE Military Communications Conference*, 800–805.

Chiang, C.-Y. J., Venkatesan, S., Sugrim, S., Youzwak, J. A., Chadha, R., Colbert, E. I., Cam, H., & Albanese, M. (2018). On defensive cyber deception: A case study using sdn. *MILCOM 2018-2018 IEEE Military Communications Conference (MILCOM)*, 110–115.

Cifranic, N., Hallman, R. A., Romero-Mariona, J., Souza, B., Calton, T., & Coca, G. (2020). Deceptiscada: A cyber deception framework for active defense of networked critical infrastructures. *Internet of Things*, *12*, 100320.

Cranford, E. A., Gonzalez, C., Aggarwal, P., Tambe, M., Cooney, S., & Lebiere, C. (2021). Towards a cognitive theory of cyber deception. *Cognitive Science*, *45*(7), e13013.

Dash, M., & Anusandhan, S. O. (2018). Exploring cloud computing adoption in private hospitals in india: An investigation of doi and toe model. *Journal of Advanced Research in Dynamical and Control Systems*, *15*(1), 10–17.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319–340.

Duan, Q., Al-Shaer, E., Islam, M., & Jafarian, H. (2018). Conceal: A strategy composition for resilient cyber deception-framework, metrics and deployment. *2018 IEEE Conference on Communications and Network Security (CNS)*, 1–9.

Effendi, M. I., Sugandini, D., & Istanto, Y. (2020). Social media adoption in smes impacted by covid-19: The toe model. *The Journal of Asian Finance, Economics and Business*, *7*(11), 915–925.

Ferguson-Walter, K., Shade, T., Rogers, A., Trumbo, M. C. S., Nauer, K. S., Divis, K. M., Jones, A., Combs, A., & Abbott, R. G. (2018). *The tularosa study: An experimental design and implementation to quantify the effectiveness of cyber deception.* (tech. rep.). Sandia National Lab.(SNL-NM), Albuquerque, NM (United States).

Ferguson-Walter, K. J., Major, M. M., Johnson, C. K., Johnson, C. J., Scott, D. D., Gutzwiller, R. S., & Shade, T. (2023). Cyber expert feedback: Experiences, expectations, and opinions about cyber deception. *Computers & Security*, 103268.

Gangwar, H., Date, H., & Ramaswamy, R. (2015). Understanding determinants of cloud computing adoption using an integrated tam-toe model. *Journal of enterprise information management*.

Hanna, H., Haroun, M. H., & Gohar, N. (2020). Developing a framework for block chain adoption using toe model. *Journal of Business and Retail Management Research*, *15*(1).

Heckman, K. E., Stech, F. J., Thomas, R. K., Schmoker, B., & Tsow, A. W. (2015). Cyber denial, deception and counter deception. *Advances in Information Security*, *64*.

Hennink, M., Hutter, I., & Bailey, A. (2020). *Qualitative research methods*. Sage.

Huang, Y., Huang, L., & Zhu, Q. (2022). Reinforcement learning for feedback-enabled cyber resilience. *Annual Reviews in Control*.

IBM. (2023). *Ibm x-force threat intelligence index 2023* (tech. rep.). IBM Security. https://www.ibm.com/downloads/cas/DB4GL8YM

Islam, M. M., & Al-Shaer, E. (2020). Active deception framework: An extensible development environment for adaptive cyber deception. *2020 IEEE Secure Development (SecDev)*, 41–48.

Islam, M. M., Dutta, A., Sajid, M. S. I., Al-Shaer, E., Wei, J., & Farhang, S. (2021). Chimera: Autonomous planning and orchestration for malware deception. *2021 IEEE Conference on Communications and Network Security (CNS)*, 173–181.

Johansson, F., & Falkman, G. (2009). A testbed based on survivability for comparing threat evaluation algorithms. *Intelligent Sensing, Situation Management, Impact Assessment, and Cyber-Sensing*, *7352*, 119–129.

Kandil, A. M. N. A., Ragheb, M. A., Ragab, A. A., & Farouk, M. (2018). Examining the effect of toe model on cloud computing adoption in egypt. *The Business & Management Review*, *9*(4), 113–123.

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, *33*(2004), 1–26.

Lee, Y., Kozar, K. A., & Larsen, K. R. (2003). The technology acceptance model: Past, present, and future. *Communications of the Association for information systems*, *12*(1), 50.

Li, H., Guo, Y., Huo, S., & Ding, Y. (2021). Edge: An enticing deceptive-content generator as defensive deception. *KSII Transactions on Internet and Information Systems (TIIS)*, *15*(5), 1891–1908.

Liebowitz, D., Nepal, S., Moore, K., Christopher, C. J., Kanhere, S. S., Nguyen, D., Timmer, R. C., Longland, M., & Rathakumar, K. (2021). Deception for cyber defence: Challenges and opportunities. *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 173–182.

Lien, A. S.-Y., & Jiang, Y.-D. (2017). Integration of diffusion of innovation theory into diabetes care. *Journal of diabetes investigation*, *8*(3), 259.

Lundblad, J. P. (2003). A review and critique of rogers' diffusion of innovation theory as it applies to organizations. *Organization Development Journal*, *21*(4), 50.

Mashima, D. (2022). Mitre att&ck based evaluation on in-network deception technology for modernized electrical substation systems. *Sustainability*, *14*(3), 1256.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook*. sage.

Mohan, P. V., Dixit, S., Gyaneshwar, A., Chadha, U., Srinivasan, K., & Seo, J. T. (2022). Leveraging computational intelligence techniques for defensive deception: A review, recent advances, open problems and future directions. *Sensors*, *22*(6), 2194.

Myers, M. D., & Newman, M. (2007). The qualitative interview in is research: Examining the craft. *Information and organization*, *17*(1), 2–26.

Niederman, F., & March, S. (2019). The "theoretical lens" concept: We all know what it means, but do we all know the same thing? *Communications of the Association for Information Systems*, *44*(1), 1.

NSM. (2023). *Risiko 2023* (tech. rep.).

Patton, M. Q. (2014). *Qualitative research & evaluation methods: Integrating theory and practice*. Sage publications.

Patton, M. Q. (2002). Two decades of developments in qualitative inquiry: A personal, experiential perspective. *Qualitative social work*, *1*(3), 261–283.

Ponemon-Institute. (2022). *2022 cost of data breach study* (tech. rep.).

Recker, J. (2021). *Scientific research in information systems: A beginner's guide second edition*. Springer.

Resnik, D. B. (2016). Ethics in Science. In *The Oxford Handbook of Philosophy of Science*. Oxford University Press.

Rogers, E. M. (2010). *Diffusion of innovations*. Simon; Schuster.

Rowe, N. C. (2007). Deception in defense of computer systems from cyber attack. In *Cyber warfare and cyber terrorism* (pp. 97–104). IGI global.

Rowe, N. C., & Rrushi, J. (2016). *Introduction to cyberdeception*. Springer.

Rue, L. D., et al. (1994). *By the grace of guile: The role of deception in natural history and human affairs*. Oxford University Press on Demand.

Sajid, M. S. I., Wei, J., Alam, M. R., Aghaei, E., & Al-Shaer, E. (2020). Dodgetron: Towards autonomous cyber deception using dynamic hybrid analysis of malware. *2020 IEEE Conference on Communications and Network Security (CNS)*, 1–9.

Searcy, W. A., & Nowicki, S. (2010). The evolution of animal communication. In *The evolution of animal communication*. Princeton University Press.

Shimanaka, T., Masuoka, R., & Hay, B. (2019). Cyber deception architecture: Covert attack reconnaissance using a safe sdn approach. *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Simin, M. T., & Janković, D. (2014). Applicability of diffusion of innovation theory in organic agriculture. *Economics of Agriculture*, *61*(2), 517–529.

Skarda, B., Mills, R. F., McDonald, T., & Strouble, D. (2008). *Operationalizing social engineering for offensive cyber operations* (tech. rep.). AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH.

Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. *Symmetry*, *13*(4), 597.

Sun, J., Sun, K., & Li, Q. (2020). Towards a believable decoy system: Replaying network activities from real system. *2020 IEEE Conference on Communications and Network Security (CNS)*, 1–9.

Symantec. (2018). *2018 internet security report* (tech. rep.).

Tan, H. C., Cheh, C., Chen, B., & Mashima, D. (2019). Tabulating cybersecurity solutions for substations: Towards pragmatic design and planning. *2019 IEEE Innovative Smart Grid Technologies-Asia (ISGT Asia)*, 1018–1023.

Tashkandi, A., & Al-Jabri, I. (2015). Cloud computing adoption by higher education institutions in saudi arabia: Analysis based on toe. *2015 International Conference on Cloud Computing (ICCC)*, 1–8.

Tornatzky, L. G., Fleischer, M., & Chakrabarti, A. K. (1990). *Processes of technological innovation*. Lexington books.

Venkatesh, V., & Davis, F. D. (1996). A model of the antecedents of perceived ease of use: Development and test. *Decision sciences*, *27*(3), 451–481.

Wallace, S., Green, K., Johnson, C., Cooper, J., & Gilstrap, C. (2021). An extended toe framework for cybersecurity adoption decisions. *Communications of the Association for Information Systems*, *47*(2020), 51.

Wendler, R. (2012). The maturity of maturity model research: A systematic mapping study. *Information and software technology*, *54*(12), 1317–1339.

Xiao, Y., & Watson, M. (2019). Guidance on conducting a systematic literature review. *Journal of planning education and research*, *39*(1), 93–112.

Yang, D., Mashima, D., Lin, W., & Zhou, J. (2020). Decied: Scalable k-anonymous deception for iec61850-compliant smart grid systems. *Proceedings of the 6th ACM on Cyber-Physical System Security Workshop*, 54–65.

Zahavi, A. [Amotz], & Zahavi, A. [Avishag]. (1999). *The handicap principle: A missing piece of darwin's puzzle*. Oxford University Press.

Appendix A

Interview Guide

The questions you see under are not set in stone, as we are conducting a semi-structured interview. These questions are meant to help guide us, the interviewers, during the interview, in order to achieve a red "line" through the process. This is due to the data collection methodology we have chosen to use for this thesis.

Generally about you and the organization

1. What is your role in your organization?
2. How many years of experience do you have within cyber security?
   (a) How many years within your role?
3. What are your work tasks?

Defensive Cyber Deception

1. What are your opinions on cyber deception as a defensive mechanism?
   (a) What made you interested in defensive cyber deception?
2. Have you heard of or used any of the mentioned defensive deception techniques?
   (a) Canary Tokens (Maturity Lvl 1)
   (b) Low-interaction/static honeypot(s) (Maturity Lvl 2)
   (c) High-interaction honeypot(s) (Maturity Lvl 3)
   (d) High-interaction honeynet(s) with SDN (Maturity Lvl 4)
   (e) Deceptive network/system environment utilizing AI (Maturity Lvl 5)
3. In a cyber security incident, what utility do you think the use of defensive cyber deception has?
4. Can you see defensive cyber deception being adopted more frequently in the future?
   (a) Why?
   (b) Why not?

Now we will move on to the TOE part of the interview. TOE is a framework from 1990 that stands for technological, organizational and environmental. These aspects should help the user of the framework to understand the adoption of a new technology in an organization, so we will see what influences the adoption of defensive cyber deception using the 3 different points. The different aspects can either be positive or negative, i.e. something that will provide an incentive for the adoption and something that will work against the adoption.

TOE Questions

1. What is your view on the available expertise in cyber security and or cyber deception in Norway?
2. Hoes does government regulations/IT standards impact the way you approach cyber security?
3. How does other organization's cyber security techniques affect the way you implement/think about different security mechanisms?
4. How would the existence of frameworks/open source solutions affect your adoption of defensive cyber deception?
5. How does the threat level towards your organization/sector affect the adoption of new defensive cyber security technologies/mechanisms?
6. What affects the decision of adopting a new cyber security technology/mechanism on an organizational level?
7. What are your opinions on defensive cyber deception's effect on organizational resource cost, such as high-fidelity alarms (i.e., removing false-positives), and fast detection that prevents successful cyber attacks already in your network?
8. How compatible do you think cyber deception is with already existing security measures such as firewalls, antivirus, IDS etc (perimeter defense mechanisms)?
9. What advantages can organizations get if they adopt defensive cyber deception?
10. What are your thoughts on the complexity of defensive cyber deception?
    (a) What is required to correctly implement defensive cyber deception?

Appendix B

Consent Form

Informasjon om forskningsprosjektet

Adopsjonen av Defensiv Cyber Deception i Norge

I dette skrivet gir vi deg informasjon om målene for dette forskningsprosjektet og hva prosjektet innebærer for deg.

Formål
Dette er en masteroppgave (Studentoppgave/forskningsprosjekt) i faget IS-507 ved linjen Cybersikkerhet ved Universitetet i Agder. Vi forsker på adopsjonen av defensiv cyber deception i Norge. Dette skal vi gjøre gjennom intervjuer som er basert på en TOE (Technological, Organizational, Environmental) model. Det er viktig at vi har de rette intervjuobjektene når vi bruker denne forskningsmetoden, men det er ingen riktige eller feil svar i et slikt intervju, ettersom vi er ute etter intervjuobjektene sine meninger basert på sine erfaringer innen organisasjonen sin.

Dataen som blir hentet inn under intervjuet vil kun bli brukt til dette prosjektet.

Hvem er ansvarlig for forskningsprosjektet?
Det er to masterstudenter fra Universitetet i Agder (UiA) ved fakultet for samfunnsvitenskap og institutt for informasjonssystemer som er ansvarlige for dette prosjektet. Vi har ansvaret for prosjektet, designe intervjuet, samle inn data og prosessere den innsamlede dataen.

Hvorfor er du inkludert i studien?
Du blir spurt om å være med i undersøkelsen vår grunnet din kompetanse innen cybersikkerhet og at du har noe/mye kunnskap om bruken av defensiv cyber deception. Vi fant utvalget vårt gjennom linkedin og kontakter i diverse cybersikkerhetsmiljøer.

Hva innebærer prosjektet for deg?
- Vi vil hente inn informasjon gjennom intervjuer. Intervjuene vil bli gjort digitalt over Teams eller Zoom og vil bli tatt opp og lagret sikkert som et digital videoopptak. Videoopptaket vil senere bli transkribert. Vi vil lagre følgende informasjon om intervjuobjektet:
    - Navn
    - Arbeidsplass/Organisasjon
    - Stillingstittel
- Vi anslår at intervjuene vil ta cirka 50-60 minutter

Du kan protestere
Du kan når som helst protestere mot at du inkluderes i dette forskningsprosjektet, og du trenger ikke å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du velger å protestere.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger
Vi vil bare bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

- Bare behandlingsansvarlige Jarl Tengesdal Lygre og Dan Bojovic vil ha tilgang til dine opplysninger

- Bare behandlingsansvarlige Jarl Tengesdal Lygre og Dan Bojovic vil samle inn, bearbeide og lagre data
- Tiltak for at ingen uvedkommende får tilgang til personopplysningene dine:
    - Navn og annen identifiserende opplysninger vil bli kodet gjennom en liste med kodeord (feks CyberSecProff1,2,3) som blir lagret i et adskilt kryptert/låst dokument fra resten av dataen som blir hentet inn.
    - All materiale vil bli lagret og bearbeidet på UiA sin sikre OneDrive med to-faktor autentisering
    - Personopplysninger og annen sensitiv informasjon vil bli lagret i egen kryptert mappe på OneDrive, adskilt fra intervjudata.

Deltakerne vil ikke kunne bli identifisert gjennom publikasjonen. Ingen informasjon om deltakerne eller deres informasjon vil bli publisert uten at de har fått et kodeord feks: (Jarl: Ivrig Student 1, Dan: Ivrig Student 2) eller (UiA: Universitetet A, NTNU: Universitetet B).

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Alle opplysningene vi har lagret om deg vil bli slettet ved endt prosjekt.

Hva gir oss rett til å behandle personopplysninger om deg?
Vi behandler opplysninger om deg basert på ditt samtykke.

På oppdrag fra Jarl Tengesdal Lygre og Dan Bojovic har Sikt – Kunnskapssektorens tjenesteleverandørs personverntjenester vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:
- å protestere
- innsyn i hvilke personopplysninger som er registrert om deg
- å få rettet personopplysninger om deg,
- å få slettet personopplysninger om deg, og
- å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

Hvis du har spørsmål til studien, eller ønsker å vite mer eller å benytte deg av dine rettigheter, ta kontakt med:
- Institutt for informasjonssystemer, Jarl Tengesdal Lygre (Jarltl@uia.no) og Dan Bojovic (Danb@uia.no) og/eller veileder Wael Anwar Abdel Aziz Soliman (Wael.soliman@uia.no)
- Vårt personvernombud: Rådgiver/Personvernombud ved UiA: Trond Hauso (trond.hauso@uia.no) +4793601625

Hvis du har spørsmål knyttet til vurderingen av prosjektet som er gjort av Sikts personverntjenester, kan du ta kontakt med:
- Personverntjenester på epost (personverntjenester@sikt.no) eller på telefon: 73 98 40 40.

Med vennlig hilsen

Jarl Tengesdal Lygre *Dan Bojovic*

Samtykkeerklæring

Jeg har mottatt og forstått informasjonsskrivet om prosjektet "Adopsjonen av Defensiv Cyber Deception i Norge" og har fått muligheten til å stille spørsmål angående skrivet. Jeg samtykker til:

- ☐ Jeg vil delta i intervju
- ☐ Jarl Tengesdal Lygre og Dan Bojovic kan gi opplysninger om meg til prosjektet

---

(Signert av prosjektdeltaker, dato)

Appendix C

Identified Literature

Identified Literature		
Author(s)	**Title**	**Theme(s)**
Islam, Al-Shaer, 2020	Active Deception Framework: An Extensible Development Environment for Adaptive Cyber Deception	Active Defense Framework (ADF), Cyber Deception
Cifranic, et al., 2020	Decepti-SCADA: A Framework for Actively Defending Networked Critical Infrastructures	SCADA systems, Framework, Decepti-SCADA
Sajid, et al.., 2020	DodgeTron: Towards Autonomous Cyber Deception Using Dynamic Hybrid Analysis of Malware	Cyber Deception, Malware Analysis, Framework
Islam. et al., 2021	CHIMERA: Autonomous Planning and Orchestration for Malware Deception	Malware Deception, Deception Goals, Probability Theory
Steingartner, et al.., 2021	Threat Defense: Cyber Deception Approach and Education for Resilience in Hybrid Threats Model	Cyber Deception, Warfare, Hybrid Threat Modelling
Mashima, 2022	MITRE ATT&CK Based Evaluation on In-Network Deception Technology for Modernized Electrical Substation Systems	Cyber Deception, IEC, MITRE ATT&CK
Ajmal, et al.., 2021	Last Line of Defense: Reliability Through Inducing Cyber Threat Hunting With Deception in SCADA Networks	SCADA, Cyber Deception, Networking, Decoys
Shimanka, Masouka, Hay., 2019	Cyber Deception Architecture: Covert Attack Reconnaissance Using a Safe SDN Approach	Cyber Deception, Software Defined Networking, Deceptive Networking
Sun, Sun, Li., 2020	Towards a Believable Decoy System: Replaying Network Activities from Real System	Cyber Deception, Networking, Decoys
Acosta, et al.., 2020	Cybersecurity Deception Experimentation System	Cyber Deception, Technical Framework
Liebowitz, et al., 2021	Deception for Cyber Defence: Challenges and Opportunities	Cyber Deception, Simulation, Generative Modelling
Chiang, et al.., 2018	On Defensive Cyber Deception: A Case Study using SDN	Cyber Deception, Software Defined Networking
Heckman, et al., 2015	Cyber Denial, Deception, and Counter Deception	Active Cyber Defense, Deception & Denial

Table C.1: Identified Literature