UiA University of Agder

Master

Cyber Security in Procurement of Third-Party Suppliers: A Case Study of the Norwegian Power Sector

BRAGE FAGSTAD & KNUT ANDREAS AAS

SUPERVISORS

Marko Ilmari Niemimaa & Paolo Spagnoletti

University of Agder, 2022
Faculty of Social Science
Department of Information Systems

ACKNOWLEDGEMENTS

Firstly, we would like to thank Marko Ilmari Niemimaa & Paolo Spagnoletti for being our supervisors throughout the master thesis, for their support, feedback, and advice.

Thanks to Netsecurity AS for being our stakeholder throughout the master thesis. We really appreciate the time and resources all of you have provided to the project.

Lastly, thanks to all research subjects that have contributed to the study, providing their experiences and knowledge making it possible to conduct our research.

Kristiansand,
June 3rd, 2022

Brage Fagstad	Knut Andreas Aas
Brage Fagstad	Knut Andreas Aas

ABSTRACT

The Norwegian power sector is currently experiencing an increasingly complex supply chain, affected by digitalization. This case study examines how digitalization has changed the procurement of third-party suppliers of Information Technology (IT) and Operational Technology (OT), focusing on cyber security, in the Norwegian power sector. The thesis investigates why cyber security in current procurements of third-party suppliers is challenging, in addition to how it is possible to make better decisions with the procurement of third-party suppliers. Literature findings originating from our Systematic Literature Review (SLR) identifies the need for conducting an exploration of procurement challenges, related to cyber security, in the Norwegian power sector. Qualitative research by utilizing Semi-Structured Interviews (SSI) was applied to acquire an in-depth understanding of participants' experiences concerning procurement. Our study includes a total of ten interviewees which was divided into four segments of the Norwegian power sector: Production, Support System, Distribution System Operator (DSO) and Transmission System Operator (TSO). By analyzing of our empirical findings and literature findings we demonstrated that there is a variety of cyber security challenges in the procurement of third-party suppliers. Most centrally, a lack of cyber security competence and low capacity of in-house expertise within the Norwegian power sector. Additionally, there is a lack of standardized requirements regarding cyber security in procurements of third-party suppliers. Certain Norwegian power companies are too small to make demands towards larger third-party suppliers making it challenging to apply desired cyber security requirements. On this basis, it is recommended that the Norwegian power sector apply competence and capacity enhancing measures.

Keywords: Cyber security, Digitalization, Norwegian power sector, Procurement, Supply chain, Third-party suppliers

Table of contents

List of figures

List of tables

ABBREVIATIONS

CI	Critical Infrastructure
DSO	Distribution System Operator
ICT	Information and Communication Technologies
IT	Information Technology
NSD	Norsk Senter for Forskningsdata (Norwegian Center for Research Data)
NSF	National Science Foundation
NSM	Nasjonal Sikkerhetsmyndighet (Norwegian National Security Authority)
NVE	Norges Vassdrags- og Energidirektorat (The Norwegian Water Resources and Energy Directorate)
OT	Operational Technology
PST	Politiets Sikkerhetstjeneste (Police Security Service)
RQ	Research Question
SC	Supply Chain
SLR	Systematic Literature Review
SSI	Semi-Structured Interview
TSO	Transmission System Operator

1 INTRODUCTION

As the power industry has become more digital, cyber threats to Critical Infrastructures (CI) have been one of the most contested topics in the policy and scholarly domains over the last decade (Cassotta & Sidortsov, 2019, p.129). From 2009 to 2017, observations show that the power sector has become the second most targeted sector (Venkatachary, Prasad & Samikannu, 2017, p.259). This is one of the most significant and complicated environments on which different industries rely to provide essential services (Salvi, Spagnoletti & Noori, 2021, p.6). An audit conducted by Riksrevisjonen identifies that the Norwegian Power industry lacks Information and Communication Technologies (ICT) security expertise, which poses a considerable threat to cyber security (Riksrevisjonen, 2021, p.8). Successful cyber-attacks aimed at the power sector might cause cascading effects due to increased interconnectivity, resulting in failures and multi-sector collapses (Cassotta & Sidortsov, 2019, p.130). A consequence that arises from digitalization is the enlarged attack surface, increasing the opportunity for exploitation (Livingston, Sanborn, Slaughter & Zonneveld, 2018, p.2). Additionally, there is an increasing trend in the number of new third-party suppliers offering new digital and technological solutions (Haver, Valdal, Vernholt & Wiencke, 2021, p.10). Power companies are compelled to rely on third-party suppliers to a large extent, and only segments of the cyber security can be verified (Hagen, Houmb, Smevold, Kalstad & Nygård, 2020, p.6). The reliance on third-party suppliers has elevated the risk of cyber-attacks in many areas of the Supply Chain (SC) (Liang, Shetty, Tosh, Ji & Li, 2018, p.45). Due to the increasing reliance on complicated value chains and SC's, it is difficult to get a complete view of the entire vulnerability landscape (NSM, 2020, p.24).

The majority of actors in the power sector is highly reliant on openness and trust-based interactions with their SC (Ghadge, Weiß, Caldwell & Wilding, 2019, p.232). However, it is unclear what requirements are needed to properly select third-party suppliers and how is this followed up. This might complicate the process of identifying appropriate third-party suppliers of IT and OT services. The issue that will be examined is related to why cyber security in current procurements of third-party suppliers in the Norwegian power sector is challenging. Additionally, identifying how the Norwegian power sector can make better decisions with future procurements of third-party suppliers.

Qualitative research approach will be applied to collect data for our study, which intends to enrich our ability to explore the problem domain of choice, which is as follows: "How has digitalization changed the procurement of third-party suppliers of IT and OT technologies, focusing on cyber security, in the Norwegian power sector." This study includes ten interview subjects distributed between production, support system, TSO, and DSO.

1.1 Research Motivation

The number of incidents in the Norwegian power sector where full incident response was applied increased by 49% in 2019 (NSM, 2020, p.26). Safeguarding this sector from cyber-attacks and cyber threats is needed to reduce the likelihood of destroying IT systems, which can have fatal consequences (Azam, 2017, p.3). Multiple cyber-attacks have occurred on a large scale in Norway, caused by unauthorized personnel which acquired access to services through ineffective processes in the acquisition of IT and OT supplies (Kirkebø & Ljøsne, 2018, p.6). This sector is experiencing long supply chains with branches across national borders, which means that the values of Norwegian power companies are no longer only domestic but are integrated towards a more comprehensive and international picture (NSM, 2020, p.26).

> *A buyer is not stronger than the weakest link in its supply chain. If only one business does not fully meet your ambitions or guidelines for responsible purchasing and perform poorly, you will not live up to the standards you have set for yourself (Achilles, 2019).*

After meetings and discussions with our stakeholders, we concluded that an in-depth investigation of the SC in the Norwegian power sector is highly relevant. The majority of companies and inhabitants in Norway are largely dependent on electrical power, and electricity customers expect light in the light bulb 24/7 365 days a year. Consequences which may arise as a result of successful cyber-attack against the Norwegian power sector might cause extensive cascading effects, which affect other critical infrastructures in Norway such as healthcare and finance. As there is limited research on this topic, it is highly motivating to advance the research with a study that can potentially shed light on the importance of prioritizing cyber security in procurement of third-party suppliers.

1.2 Research Questions

To delimit our focus of the thesis, appliance of Research Questions (RQ) has been utilized. The purpose of the RQs is to shape and direct our case study in order to limit the chance of issues that could influence all later phases of our research

(Agee, 2009, p.431). The RQs explores challenges that exist in current procurement of third-party suppliers and how companies within the Norwegian power sector can make better decisions with the procurement of third-party suppliers. The defined RQs that will be addressed through our case study are:

RQ 1: Why is cyber security in current procurements of third-party suppliers in the Norwegian power sector challenging?

RQ 2: How can the management in the Norwegian power sector make better decisions in the procurement of third-party suppliers?

Qualitative research methods will be applied to acquire information related to our problem domain, which intends to develop deeper knowledge to answer our RQs.

1.3 Thesis Structure

The thesis structure initiates with chapter 1 which briefly explains our problem domain and provides a holistic view of the project. Further on, chapter 2 presents our background and related work. This chapter includes our literature findings originating from conducting a Systematic Literature Review (SLR). Chapter 3 then elaborates the methodologies applied in the process of conducting the literature review, research approach and research design. Additionally, explaining our data collection and analysis processes. Chapter 4 entails our empirical findings retrieved from our data analysis. Chapter 5 includes a discussion, where our literature findings provided in background and related work and the empirical findings are discussed. Furthermore, practical contributions are provided. The chapter then include suggested further research, in addition to project limitations. Chapter 6 includes a conclusion for the thesis. The figure below illustrates the thesis structure. The blue dotted arrow illustrates how the findings figure in chapter 2 Background and Related Work and chapter 4 Empirical Findings are linked together in the discussion chapter (see figure 1).

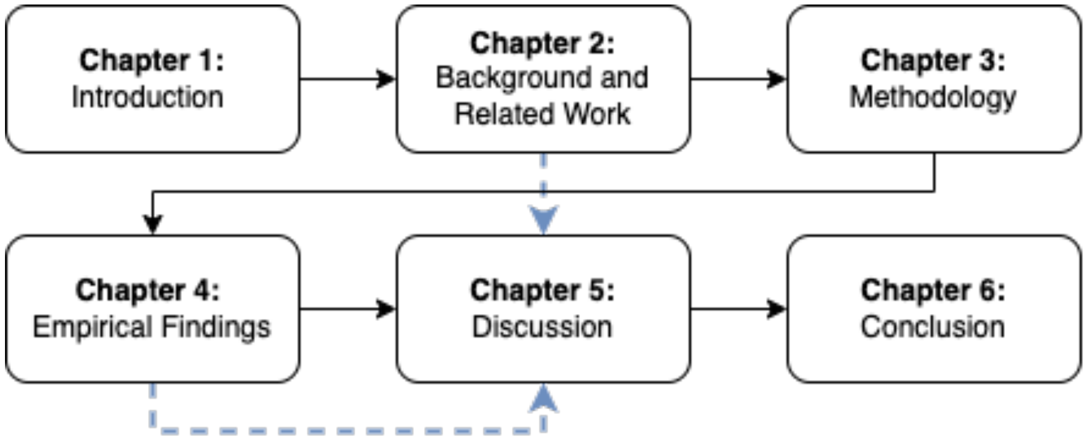


Figure 1 Thesis structure

2 BACKGROUND AND RELATED WORK

The following chapter includes the literature findings which presents our background and related work. The chapter is divided into subchapters beginning broad with threats to critical infrastructures, consequences of digitalization, dependency on the supply chain, and vulnerabilities and attacks against the supply chain. A literature discussion is then provided to narrow down our focus to the particular aspect to be empirically investigated, in order to explore the technical and managerial challenges regarding the procurement of third-party suppliers.

2.1 Threats to Critical Infrastructure

The power supply is a central part of the CI in Norway (Riksrevisjonen, 2021, p.4). This sector is arguably one of the most important, complex environments which multiple sectors depend on to deliver essential services (Salvi et al., 2021, p.6). Access to power is increasingly important to maintain normal activities in the community, secure critical societal functions in crisis situations and secure the country's defense capability during readiness and in war (Riksrevisjonen, 2021, p.4). A cyber-attack that causes a power outage can have major ramifications for all sectors of Norwegian society including the digital systems that society relies on (Riksrevisjonen, 2021, p.5). Large parts of society will come to a halt if the power source fails in Norway (NSM, 2020, p.8). Norwegian National Security Authority (NSM) and Police Security Service (PST) fear sabotage against the Norwegian power sector and other CI's (Azam, 2017, p.4). According to national threat assessments, power sector systems are important infrastructures that are especially sensitive to intelligence and advanced network operations (Riksrevisjonen, 2021, p.4).

Successful cyber-attacks against the power sector may cause a cascading effect which is a circumstance that causes CI to become more interdependent, potentially leading to cascading failures and multi-sector collapses. The chances of such events are low, but the consequences are severe (Cassotta & Sidortsov, 2019, p.130). Because of its importance and impact on everyday operations, cyber-attacks on CI are lucrative (Kumar, Prasad, & Samikannu, 2018 p.106). Countries throughout the world consider electrical infrastructure to be fundamental to a functional civilization. Power is one of the most essential infrastructure sectors identified by the US government, being so important that their incapacity or destruction would have a devastating effect on security, national economy, as well as national public health or safety (Livingston et al., 2018, p.2).

Cyber threats against CI have in the past decade become one of the most debated concerns in the energy policy and scholarly domains as the sector has become more digitized (Cassotta & Sidortsov, 2019, p.129). According to Venkatachary et al. observations indicate that the power sector has become the second most targeted sector from the time period 2009 to 2017 (Venkatachary et al., 2017, p.259). Furthermore, Kumar et al. confirms in the research article "Critical review of cyber security and cyber terrorism – threats to critical infrastructure in the energy sector" from 2018, that cyber-attacks has considerably increased compared to previous years. Where the power sector is still the most vulnerable sector in terms of cyber-attack, second only to financials (Kumar et al., 2018, p.111). Because of the broad attack surface of the intertwined systems of IT and OT networks, the power sector is an excellent target for state actors and criminal organizations (Vozikis, Darra, Kuusk, Kavallieros, Reintam & Bellekens, 2020, p.1). According to PST's 2017 threat assessment, the Norwegian CI is one of the main areas where intelligence activities may occur. Foreign countries can gain in-depth information about CI through network-based intelligence operations in peacetime. In times of crisis, this sort of information might be exploited for sabotage activities. Several governments are developing malware that can be used to disrupt or sabotage critical social operations (Azam, 2017, p.11).

Seasonal darkness and a severe climate which has become less predictable as a result of global climatic changes are the kinds of characteristics present in the Arctic European High North (Cassotta & Sidortsov, 2019, p.129). Experiencing consequences such as profound blackouts in an environment with less resilience is comparable to potential cyber-attacks in the power sector. The similarities between these are unpredictability, rapidity and vulnerability in the area affected by the consequences (Cassotta & Sidortsov, 2019, p.130). Multiple attacks have been recorded in the last decades (Kumar et al., 2018, p.109). An example of this is the blackout in 2003 which left the East Coast of the USA and parts of Canada without power for two days. This incident left approximately 50 million people without power in temperatures of over 32 degrees Celsius. Additionally, the blackout affected many CI's systems like transport and emergency services (Horne, 2019). The impact of disruptions of the CI in the power sector, regardless of time intervals, could potentially impact a large number of people, affecting operations and reputation of the affected organization (Salvi et al., p.1) which reflects the 2003 blackout. Other consequences which come as a result of cyber incidents today have the potential to disrupt energy services, damage highly specialized equipment and endanger human health and safety (Lamba, 2018, p.76865).

The current operating society necessitates a high level of electrical reliability (Lamba, 2018, p.76866). The impact and damage caused by cyber-attacks can be as lethal as any conventional warfare. As a result, it is critical to safeguard data and ensure the proper operation of CI in the power sector (Kumar et al., 2018, p.103). Over the period of time, the motivations of the threat actors have changed where it is driven by financial gain. It has now evolved into organized crime with well-established marketplaces trading in malware to attacks designed to cause havoc to the CI (Kumar et al., 2018, p.103). However, disconnecting critical IT systems within the power sector as an extreme measure is not possible, compared to other less critical IT systems. This would have resulted in major consequences in crucial processes that cannot operate without power (Salvi et al., 2021, p.7). Numerous breaches in recent years have indicated that even more work is required to safeguard CI in the power sector against more sophisticated and focused attacks (Lamba, 2018, p.76866).

2.2 Consequences of Digitalization

Digitalization is a process that has an impact on a variety of industries, including the power sector (NSM, 2020, p.8). New solutions, working techniques, and routines emerge as a result of digitalization (Azam, 2017, p.10). From large-scale industries to household consumption, digitalization has a significant influence on all aspects of society (Azam, 2017, p.3). One of the causes for the digitalization wave in the power sector is the usage of unregulated energy production and growing power consumption as a result of electrification (Hagen et al., 2020, p.6). The digital agenda is additionally being driven by several different aspects of IT such as cloud computing, machine learning and big data. These, as well as multiple other technologies, data, and intelligence, are central regarding digitalization (Azam, 2017, p.3).

There are a significant number of operational benefits which come as a result of digitalization in the power sector. The use of ICT creates opportunities for companies to streamline operations, reduce costs, create new jobs, stimulate economic growth, and protect the environment (Azam, 2017, p.3). According to the Norwegian Department, politicians encourage companies to apply digital solutions, with the intention to provide greater opportunities for efficiency, competitiveness, and the creation of new jobs (Departementene, 2019, p.3). The scientific journal "*Energy Research & Social Science*" by Cassotta & Sudirtsov confirms that the rapid increasing digitalization has contributed to economic and social development, in addition to increasing environmental protection (Cassotta & Sidortsov, 2019, p.129). Additionally, there are clear advantages in terms of performance within the power sector. The digitalization has provided more precision, faster responses in the main areas of power generation, transmission and management of the network opposed to systems that are entirely managed by humans (Salvi et al., 2021, p.7).

For regulating energy production and distribution, as well as transferring and monitoring demand data, digital technologies are becoming increasingly important in the energy infrastructure (Azam, 2017, p.3). Digital technologies are becoming a more significant aspect of running complex power supply and ensuring a high degree of security throughout the delivery of energy and district heating. The reliance of these digital systems increases overall vulnerability, necessitating a greater need for security (Hagen et al., 2020, p.3). The increasing interconnectivity between organizations and systems in addition to the widespread use of digital communication increases the risk of experiencing cyber-attacks (Vozikis et al., 2020, p.2). It is anticipated that in the future, there will be more interconnections directly to the control system, allowing IT and OT to integrate furthermore (Haver et al., 2021, p.15). Control systems that govern the processes have previously been physically separated. This is evolving as remote control of systems has provided more efficient operation and utilizes areas for data from the systems to open new services. As a result, control systems are more vulnerable to the same sorts of cyber-attacks that threaten traditional ICT systems (Azam, 2017, p.5). Both technical and organizational transformation has exposed energy critical cyber infrastructure to numerous new cyber threats (Salvi et al., 2021, p.7).

As a result of increased digitalization, all industries are becoming increasingly vulnerable to cyber risk (NSM, 2020, p.8). According to research published by Riksrevisjonen in 2021, the use of new technologies, cloud services, and foreign third-party suppliers, in addition to the integration of multiple internet-connected systems, increase the risk further (Riksrevisjonen, 2021, p.4). The power sector is more likely to experience cyber-attacks as a result of digitalization (Kirkebø & Ljøsne, 2018, p.12). The advent of digitalization provides solutions for smart, energy-efficient homes. However, as more components get digitized and connected to the internet, they become vulnerable to a variety of cyber-attacks and adverse events. Many of these incidents are not well known (Azam, 2017, p.2). Vozikis et al. identifies that the majority of cyber-attacks against the power sector are targeted at power generation and DSO`s (Vozikis et al., 2020, p.2).

The power sector is moving towards smart grid and distribution system operations which increase the risk of experiencing cyber-attacks, resulting from the enlarged attack surface (Vozikis et al., 2020, p.2). Additionally, control systems that are connected to other systems through less secure networks, further enhance the number of vulnerabilities resulting in exposure to cyber threats (Haver et al., 2021, p.15). Livingston et al. confirms that the global digitalization of the power grid increases the attack surface, which enlarges the exploitation opportunities. The grid has additionally become significantly “smarter” by utilizing ICT and devices embedded throughout, networks are being linked, the system is becoming more complex, and the amount of access points is increasing (Livingston et al., 2018, p.5). As more systems are integrated into the power grid, the tendency of cyber-attacks will become increasingly complex and widespread (Kumar et al., 2018, p.114). To illustrate the Norwegian power grid, which consists of a variety of segments, a figure from the Norwegian Water Resources and Energy Directorate (NVE), "Roadmap for NVE's follow-up of ICT security in the supply chain," has been included. The figure visualizes third-party suppliers that are connected to actors within the power sector which are critical to provide power distribution to the society (see figure 2) (Haver et al., 2021, p.7).

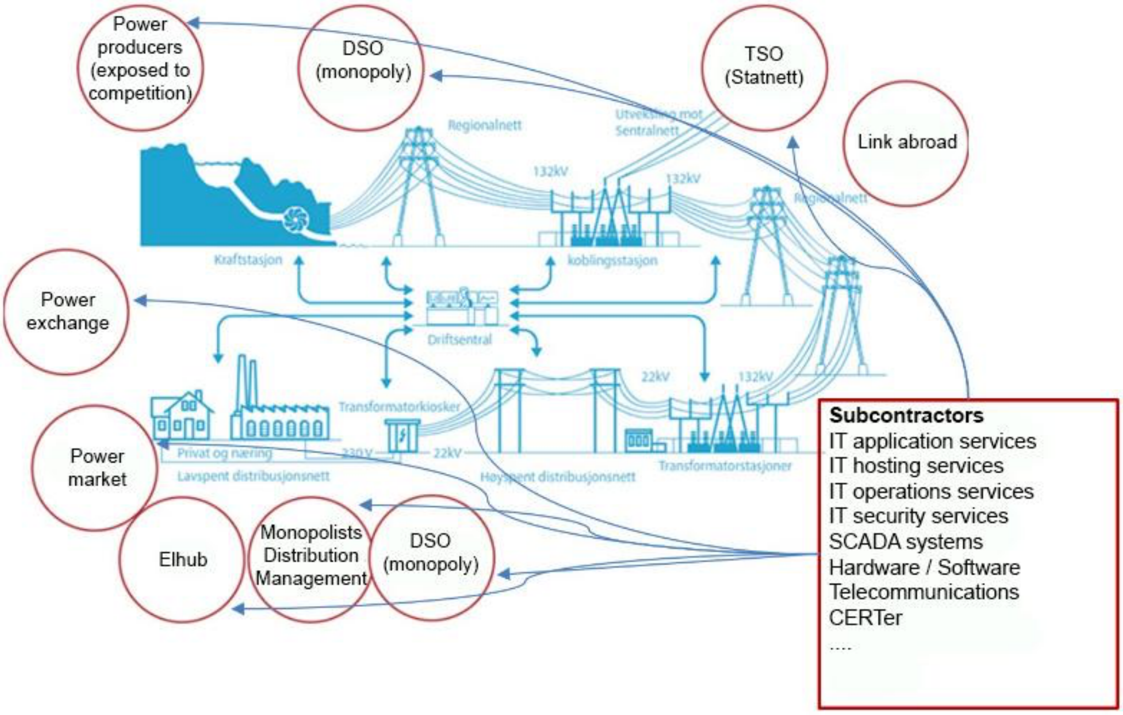


Figure 2 Norwegian power infrastructure (Haver et al., 2021, p.8)

Comprehensive security, covering all levels and going into depth on hardware, is required for successful digitalization. However, hardware security expertise is in limited supply in Norway. This is highlighted in an NVE report from 2018, which focuses on SC security (Hagen et al., 2020, p.4). The process of digitalization will always involve risks which affect the society, organizations, and individuals. An extensive approach to cyber security, as well as methods to mitigate threats and handle incidents as they arise, assist the digitalization process to become more secure (NSM, 2020, p.8). Successful digitalization requires that solutions fulfill standards for security and individual privacy in a satisfactory manner, and that we have faith in the digital solutions to perform as they should (Departementene, 2019, p.3).

2.3 Vulnerabilities, Threats, and Attacks

The rapid digitalization makes it demanding to predict which kind of threats that may affect the risk picture. Known threats such as ransomware, industrial espionage, sabotage, extortion, online violations, and identity theft, will continue to have an impact on the risk picture in the future. The consequences can be significant for those who are affected, which can be private individuals and companies (Departementene, 2019, p.6). Within the power sector, the landscape of cyber risks is changing and expanding. This expansion includes a higher frequency of cyber-attacks, numerous threat actors, significantly more sophisticated malware and tools which are more widely available and occasionally indis-criminately deployed (Livingston et al., 2018, p.12). Malware does not propagate on its own the way traditional computer viruses did in the past. Instead, they are distributed using a compromised software package, phishing emails or malicious URLs. As a result, threat actors frequently obtain an initial entrance in the target system with the assistance of an unaware employee (Vozikis et al., 2020, p.5). NVE states that there is a trend in cyber threats that includes international crime, espionage, extortion, and sabotage (Hagen et al., 2020, p.4). Cyber threats come in a variety of forms, and many people believe that technology is impervious to failure, accident, misjudgment, or sabotage. Cyber-attacks occur on a daily basis and have a variety of dimensions (Kumar et al., 2018, p.106). In the 2020 threat assessment, DNB highlights ransomware as an increasing trend, which has also been detected in the power sector. This is reflected in the Norwegian media and international reportage. NSM expects that ransomware attacks on the Norwegian power sector will continue to rise in the coming future (NSM, 2020, p.12).

Phishing, or cyberattacks conducted via email asking users to click on a link that subsequently injects malware into their computers, or by email asking for personal details to enable unauthorized personnel network access, is one of the most prevalent attack vectors in the power industry (Livingston et al., 2018, p.3). According to NSM, numerous threat actors have attempted online fraud attempts and digital operations aimed at vulnerabilities opened by COVID-19 topics (NSM, 2020, p.7). Additionally, Europol states in a report that cyber criminals are exploiting the pandemic and the resulting weakness in society to commit cybercrimes (Hagen et al., 2020, p.6). This has resulted in increased pressure on a variety of critical industries, including the power sector (Hagen et al., 2020, p.6). These sectors have vital operational competence and functioning which make them exposed to cyber-attacks. In addition, the increasing usage of home office solutions introduces weaknesses in remote access solutions, which necessitated enhanced ICT security vigilance and knowledge (NSM, 2020, p.7). Vozikis et al. have identified the most common cyber-attacks in the power sector which are included in table 1 (Vozikis et al., 2020, p.2).

Table 1 Cyber-attacks (Vozikis et al., 2020, p.2)

Cyber-attack(s)	Description
Malware	A software or file that is intended to cause harm. There are several different methods such as: Virus, Worm, Trojan horse, Ransomware, Spyware and Adware.
Denial of Service (DoS)	Sending more requests than the services can manage, to crash the program/service.
Social Engineering	Users might be tricked into giving private information in this type of attack. The majority of social engineering assaults rely on human contact, with phishing and spear phishing being the most common instances.
Advanced Persistent Threats (APTs)	An unauthorized threat actor acquires extended access to a system in this sort of assault. APT necessitates extensive system knowledge.

The power sector is among the most frequently targeted industries and one of the first to implement safeguards to respond to cyber threats. As threats continually get more sophisticated, an increasing effort to manage risk is required (Livingston et al., 2018, p.2). Attackers are fast to take advantage of the increasingly globalized and digitized world. It is very important to continuously monitor the threat and risk picture and adapt to what is occurring in other countries and what could happen in Norway (Azam, 2017, p.19). According to observations by NSM's, threat actors frequently exploit known vulnerabilities. From the time a vulnerability is discovered by threat actors and for malware to be installed is becoming progressively shorter. Identifying these kinds of attacks is time critical, and businesses need to automate and simplify the process of implementing new security updates (Azam, 2017, p.25).

There is a significant challenge to handle cyber-attacks and cybercrimes aimed at the power sector. Threats against this sector cannot be entirely removed, only mitigated. The mitigation process requires time and resources, downtime and has economic and psychological consequences for the sector, all of which might harm the company's performance and the national economy (Venkatachary et al., 2017, p.250). As more components get connected to the grid in a distributed model, the trend of cyber-attacks will become more complex and continue to increase. Protecting these systems from cyber-attacks is crucial to avoiding non-availability, minimizing disruptions and losses, avoiding downtime, maximizing availability and revenues (Venkatachary et al., 2017, p.259). Cyber-attacks have the potential to destroy computer systems, which can have fatal consequences. As a result, it is critical that the power sector is safeguarded from cyber-attacks and cyber threats, which can result in information theft, security problems, interruptions, and in the worst-case scenario, an outcome in which nature or human life is endangered (Azam, 2017, p.3). Kirkebø & Ljøsne specifies that such incidents have occurred on a large scale in Norway, where ineffective routines related to the acquisition of supplies caused unauthorized personnel to acquire access to services (Kirkebø & Ljøsne, 2018, p.6).

2.4 Dependency on the Supply Chain

A SC is a collection of different organizations that assist businesses to achieve their goals (Yeboah-Ofori & Islam, 2019, p.1). It consists of interconnected nodes that collaborate to provide good services (Simon & Omar, 2020, p.162). SC is becoming increasingly globalized as a result of companies wanting to reduce electrical component, software, and firmware costs (Liang et al., 2018, p.45). Ghadge et al. states that SC is the backbone of the evolving technological ecosystem. Internet of things, additive manufacturing, virtual reality, artificial intelligence and blockchain intended to reflect, expand, alter, and innovate the relationship between SC partners (Ghadge et al., 2019, p.224). SC in larger enterprises is usually significantly sophisticated, with a great number of partners and products. A cyber security company revealed that one of their clients' supply networks involve more than 5000 organizations (Kshetri & Vaos, 2019, p.7).

Power companies are to a major extent forced to rely on suppliers, and only segments of the security are possible to verify (Hagen et al., 2020, p.6). The growing reliance on complex value and SC makes it difficult to provide a comprehensive understanding of the whole vulnerability surface (NSM, 2020, p.24). These value chains have become increasingly crucial in maintaining Norwegian societal functions (NSM, 2020, p.8). According to Haver et al. extensive digital value chains, complex systems, increasing usage of autonomy, combined with mutual dependencies on suppliers both nationally and internationally and an increasing amount of threat actors, makes it challenging for both organizations and authorities to manage their risks and vulnerabilities (Haver et al., 2021, p.6).

The number of devices connected to the internet is growing, and cloud solutions are becoming more ubiquitous (Departementene, 2019, p.6). According to a report from Riksrevisjonen, these new technologies, foreign suppliers and the various systems that are connected to the internet enlarge the likelihood of experiencing cyber-attacks against the power sector. Hence the need for reduced costs and increased access to competence. ICT-related functions are increasingly being outsourced to external suppliers, particularly in low-cost countries (Departementene, 2019, p.6). National threat assessments reveal that CI in the power industry are particularly vulnerable to intelligence and advanced network operations (Riksrevisjonen, 2021, p.4). Norwegian business values are not only stored within national borders but are frequently integrated internationally. Company structures that are split into branches across national borders is resulting in complexity and complicates the ability to have a security overview (NSM, 2020, p.26).

Quantitative research provided by NVE identifies that of 88 power organizations, 40% are reliant on the information technology provider to address events in their systems, including operational and administrative systems. 34% states that they are significantly dependent on the supplier. Whereas 25% mention that they are to a small degree dependent on the supplier (Azam, 2017, p.9). A condition report regarding information security from the power sector verifies that the sector is largely dependent on their suppliers (Kirkebø & Ljøsne, 2018, p.5). According to *"Meld. St. 25 (2015–2016) Kraft til endring - Energipolitikken mot 2030,* (Power for change - The energy policy towards 2030)", there is a risk that the power sector may become overly dependent on suppliers. It is critical that the power sector send clear signals to suppliers that ICT security is a significant priority, and that suppliers constantly enhance competence in ICT operations and ICT security (Riksrevisjonen, 2021, p.10).

Multiple businesses in the power sector use the same supplier of ICT systems. If a single company loses their ability to deliver power in the distribution or regional grid, it will only affect a limited area. However, a successful attack against a third-party supplier or a widely used system within the power sector would affect a variety of companies and larger areas. Several of these organizations are highly rely on their suppliers to manage and recover operational control systems (Riksrevisjonen, 2021, p.10). It is stated that the reliance on suppliers must be addressed for both preventative security and emergency planning (Kirkebø & Ljøsne, 2018, p.13). There is a risk that suppliers do not have dimensioned contingency for incidents that affect several companies simultaneously (Riksrevisjonen, 2021, p.10). The majority of suppliers stated that they have control over ICT security one layer down the SC. The others pointed out that it would be too resource intensive to follow up on security all the way down in the SC (Kirkebø & Ljøsne, 2018, p.21).

The SC allows for new types of risk that are independent of physical products or physical locations (Ghadge et al., 2019, p.224). Risks can arise in every stage of the supplier products and service life cycles (software, firmware, and hardware), covering procurement, deployment, operation, and maintenance (Liang et al., 2018, p.44). To effectively handle SC cyber risks, openness and trust-based relationships with the SC network are required (Ghadge et al., 2019, p.232).

According to quantitative research provided by Kshetri & Vaos, 72% of companies lack full visibility into their SC (Kshetri & Vaos, 2019, p.7).

2.5 Vulnerabilities and Attacks Against the Supply Chain

Today's global SC are vulnerable to a variety of threats, any of which might cause a company's operations to be temporarily disrupted (Simon & Omar, 2020, p.161). A SC attack is a malicious action exploiting vulnerabilities in ICT, including hardware, software, and firmware, with an intention of disrupting or surveilling by utilizing cyber resources (Heinbockel, Laderman, & Serrao, 2017, p.9). These kinds of attacks exploit the target system to acquire control, execute and maintain presence in the system (Heinbockel et al., 2017, p.18). Hackers have been able to access bigger companies that rely on software by targeting smaller software suppliers (Kshetri & Vaos, 2019, p.6). According to NSM, SC attacks will become increasingly prevalent (NSM, 2020, p.12). Cyber security issues are one of the rising hazards in the SC, and they must be handled as part of any wider SC risk management plan (Simon & Omar, 2020, p.161). SC cyber-attack are on the rise (Yeboah-Ofori & Islam, 2019, p.1). Estimates provided by Kshetri & Vaos have suggested that SC`s account for 80% of all cyber-attacks and insecure SC have increased the amount of conventional cyber-attacks (Kshetri & Vaos, 2019, p.6).

The dependency on third-party suppliers have increased the likelihood of threats in multiple layers of the SC (Liang et al., 2018, p.45). Observations made by NSM show that businesses further down the value chain are affected by security threatening activity (NSM, 2020, p.14). A successful cyber-attack against a third-party supplier can cause significant delays in production and supply, shipments, and deliveries across the SC. Additionally, it can have a negative influence on an organization's overall financial performance and shareholder value (Simon & Omar, 2020, p.161). In 2015, 46 cyber-attacks were reported in the power sector, the majority of which targeted the IT systems of utilities and suppliers (Yeboah-Ofori & Islam, 2019, p.2). The intention of these kinds of activities could be harming the target itself or be a part of a larger attack with a goal further up in the value chain (NSM, 2020, p.14). Cyber-attacks might occur anywhere along the SC. There have been several incidents when organizations have been harmed as a result of a breach via a third-party supplier (Simon & Omar, 2020, p.161). Threat actors focus on exploiting the various SC network levels to infiltrate large organizations. Malware insertion is a trending method applied to gain access to hardware via backdoors (Kshetri & Vaos, 2019, p.6).

KraftCERT has handled incidents involving manufacturers and suppliers in the power sector and believes SC attacks to be a huge danger (NSM, 2020, p.14). The well-known American company SolarWinds has been exposed to such an attack.

Late December 2020, threat actors managed to apply a sophisticated and comprehensive cyber operation establishing a backdoor in one of SolarWinds systems. The backdoor was included into an update which they distributed to 18 000 businesses globally. This backdoor enabled the threat actors to exploit the entrance to the system for further compromising the customers. The affected system was a network surveillance system, which commonly has access into the businesses infrastructure, which significantly increased the severity. After acquiring access to a variety of businesses, the threat actors pinpointed specific targets. This attack resulted in extensive consequences for those who were exposed, including US government agencies and large technology companies such as Microsoft (NSM, 2021, p.25). As more systems are outsourced, the less control you have. This increases the need to rely on your suppliers. The SolarWinds incident serves as a warning that even a reputable monitoring solution and provider may be hacked (Haver et al., 2021, p.14).

Due to the integration and interconnections of numerous suppliers that are interrelated to fulfill business goals, cyber security in the SC has become a major challenge (Yeboah-Ofori & Islam, 2019, p.22). Data, credentials, source code, applications, networks, and infrastructures are increasingly shared with "trusted" SC partners (Kshetri & Vaos, 2019, p.6). This adds complexity to an organization, and it can become more challenging to manage (Ghadge et al., 2019, p.224). The increased interconnection has brought new vulnerabilities, risks, threats, and attacks that threat actors may exploit (Yeboah-Ofori & Islam, 2019, p.4). One of the challenges that is introduced as a result of the increased interdependencies is the lack of third-party audit mechanisms and cascading cyber threats (Yeboah-Ofori & Islam, 2019, p.1). Modeling and analyzing these threats can provide valuable insight which are necessary to develop security measures to protect the SC (Yeboah-Ofori & Islam, 2019, p.4). Additionally, there is a lack of tools and technologies that can preserve the whole SC, ensuring that all software and firmware are verified for trustworthiness before being deployed in critical OT systems such as the power sector's energy delivery system (Liang et al., 2018, p.44). The table underneath lists the six most pervasive and prominent SC vulnerabilities, provided by research from Haver et al. (see table 2).

Table 2 The most important vulnerabilities (Haver et al., 2021, p.36)

ID	Pervasive and prominent supply chain vulnerabilities
1	Lack of risk and threat understanding among the actors in the supply chain
2	Lack of understanding and compliance with regulatory requirements at the KBO units

3	Lack of competence and / or capacity / ability to make sufficient demands on suppliers
4	Lack of competence and / or capacity / ability to follow up requirements set in the supply chain
5	Lack of identification of, information sharing about, and closure of digital vulnerabilities in equipment and systems among the actors in the supply chain
6	Lack of competence and / or capacity / ability to detect and handle ICT security incidents at the actors in the supply chain

According to KraftCERT, the threat description emphasizes the importance of securing communication and delivery from suppliers (NVE, 2017, p.25). Trust in any SC is a complicated issue that is difficult to measure and achieve (Kshetri & Vaos, 2019, p.7). To scale the process of securing the SC, a top-down system-level framework should be devised ahead of time to lead the formalization of the whole SC security (Liang et al., 2018, p.44). To deal with more sophisticated cyber threats, SC needs to be more transparent about security and integrate security resources (Ghadge et al., 2019, p.232). Cyber security is a significant problem for SC since a cyber-attack on one organization in the SC network might harm another (Simon & Omar, 2020, p.161). Yeboah-Ofori and Islam states that modeling cyber-attacks in a SC is a method of gaining knowledge and awareness of the opponent's methods of operation, strategies, techniques, and processes (Yeboah-Ofori & Islam, 2019, p.3).

2.6 Literature Discussion

The literature review has provided us with a deeper understanding of our problem domain and RQs. Through the analysis, we have gained an extensive comprehension of the position the Norwegian power sector has in our society and how critical this infrastructure is. Salvi et al. confirm, the power sector is one of the most important and complex sectors which large parts of society depends on (Salvi et al., 2021, p.6). If Norway's power supply fails, large parts of society will come to a halt (NSM, 2020, p.8). Furthermore, we can draw parallels from the fact that digitalization has contributed to the exposure of critical infrastructure to challenges it has never faced before. Kirkebø and Ljøsne states that the power sector has become more susceptible to cyber threats as a result of digitalization (Kirkebø & Ljøsne, 2018, p.12). This can also be confirmed by NSM through a comprehensive threat assessment of Norway, published in 2020 (NSM, 2020, p.8). Handling cyber threats and cybercrime targeted at the power sector is a serious concern. Threats to this sector can only be mitigated, not eliminated (Venkatachary et al., 2017, p.250).

Through the literature review we have identified that the SC is vulnerable to cyber-attacks but there are limited amounts of research on this topic. Threat actors could take advantage of “trusted” suppliers to acquire access to targeted systems higher in the value chain. Kshetri an Vaos states that the challenge of trust in the SC is unlikely to disappear anytime soon (Kshetri & Vaos, 2019, p.10). The SC are increasingly interconnected, resulting in lack of third-party audit mechanisms and cascading cyber threats (Yeboah-Ofori & Islam, 2019, p.1). We have recognized that there is a research gap related to the procurement of suppliers in the Norwegian power sector. According to Liang et al. there is a lack of tools and technologies that can preserve the entire SC, ensuring that all software and firmware are verified for trustworthiness before being implemented into critical systems within the power sector (Liang et al., 2018, p.44). According to qualitative research provided by Haver et al. certain countries, such as Germany and Turkey, require suppliers in power sector to be certified in accordance with international standards such as ISO 27001 and ISO 27002 on management systems for information security or equivalent (Haver et al., 2021, p.29).

Competence is necessary in procurements and administrative procedures. It is necessary to make the proper decisions so that the organizations can acquire the appropriate equipment, technology, and enter requirements into tender procedures and contracts to the supplier (NVE, 2017, p.30). It is up to the organizations themselves to assess risk and introduce risk reducing measures. Cyber security is regulated in private law contracts between supplier and customer, and between supplier and subcontractor (Haver et al., 2021, p.6). The figure underneath has been developed to summarize the challenges related to procurement of suppliers, identified through the literature. Each challenge is connected with the related process (see figure 3).

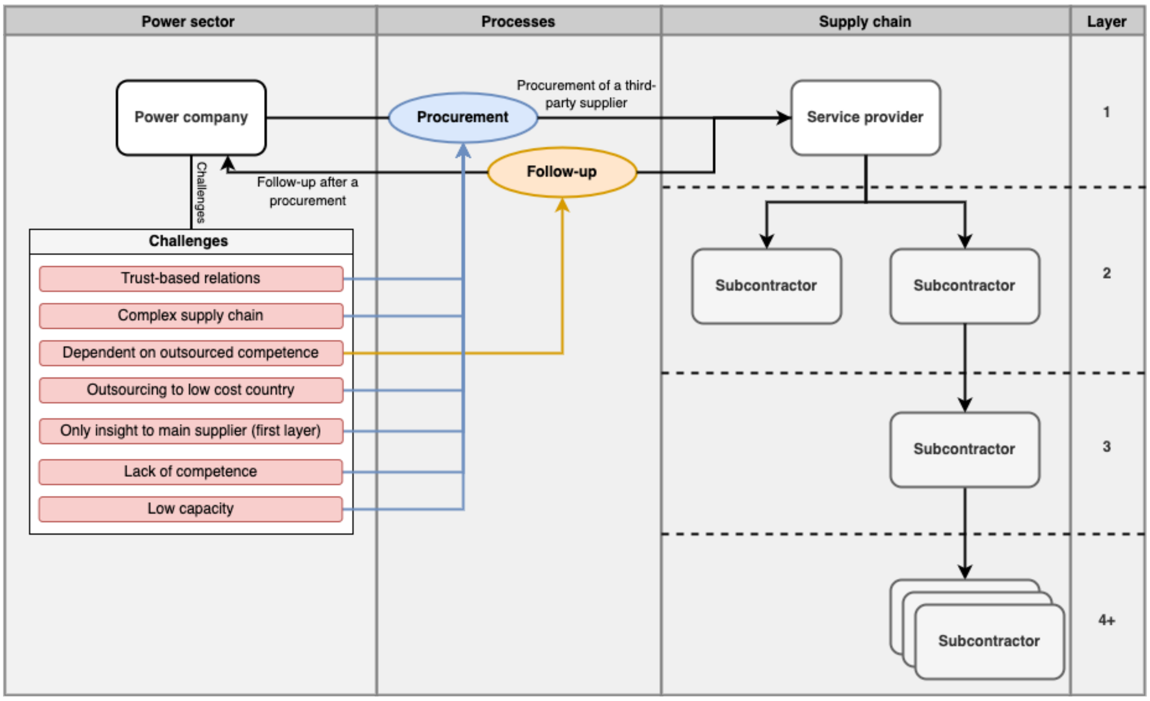


Figure 3 Identified challenges from literature

This forms our foundation to further research the procurement of third-party suppliers in the Norwegian power sector. What challenges exist in current procurement and how can the management in the Norwegian power sector make better decisions in the procurement of third-party suppliers?

3 METHODOLOGY

The following chapter examines the methodologies utilized to retrieve the data to perform the empirical analysis. The chapter initiates an in-depth explanation of conducting a systematic literature review. Subsequently, the process of selecting qualitative research methodology is explained, including reasoning behind our choices. The procedure of collecting data with the appliance of semi-structured interviews is then elaborated, with explanations of how the data has been analyzed.

3.1 Literature Review

An essential part of academic research is the process of conducting a systematic literature review (Xiao & Watson, 2019, p.93). The process of a SLR intends to enhance our capability to investigate literature in a systematic and efficient manner. The quality of the literature review is exceptionally reliant on the material gathered for the review (Xiao & Watson, 2019, p.103). Fundamentally, knowledge has been developed based on previously completed work. The conduction of our literature review has helped to gain a greater understanding of the depth of the existing work by evaluating relevant literature and identifying gaps to further investigate (Paré, Trudel, Jaana & Kitsiou, 2015, p. 183).

The literature review is a process which consists of multiple steps. These steps can be broken into three major stages: Planning the review, conducting the review, and reporting the review (Xiao & Watson, 2019, p.102). Within these stages, they are frequently recurring several similar steps from multiple sources. "A Guide to Conducting a Standalone Systematic Literature Review" by Okoli (Okoli, 2015, p.884), "The shape of digital transformation: a systematic literature review" by Emily, Mondher & Imed (Emily, Mondher & Imed, 2015, p.432) and "*Procedures for Performing Systematic Reviews*" by Kitchenham (Kitchenham, 2004, p.3).

The eight phases outlined below organize the process of performing an SLR and strive to improve our understanding of the problem domain (see figure 4).

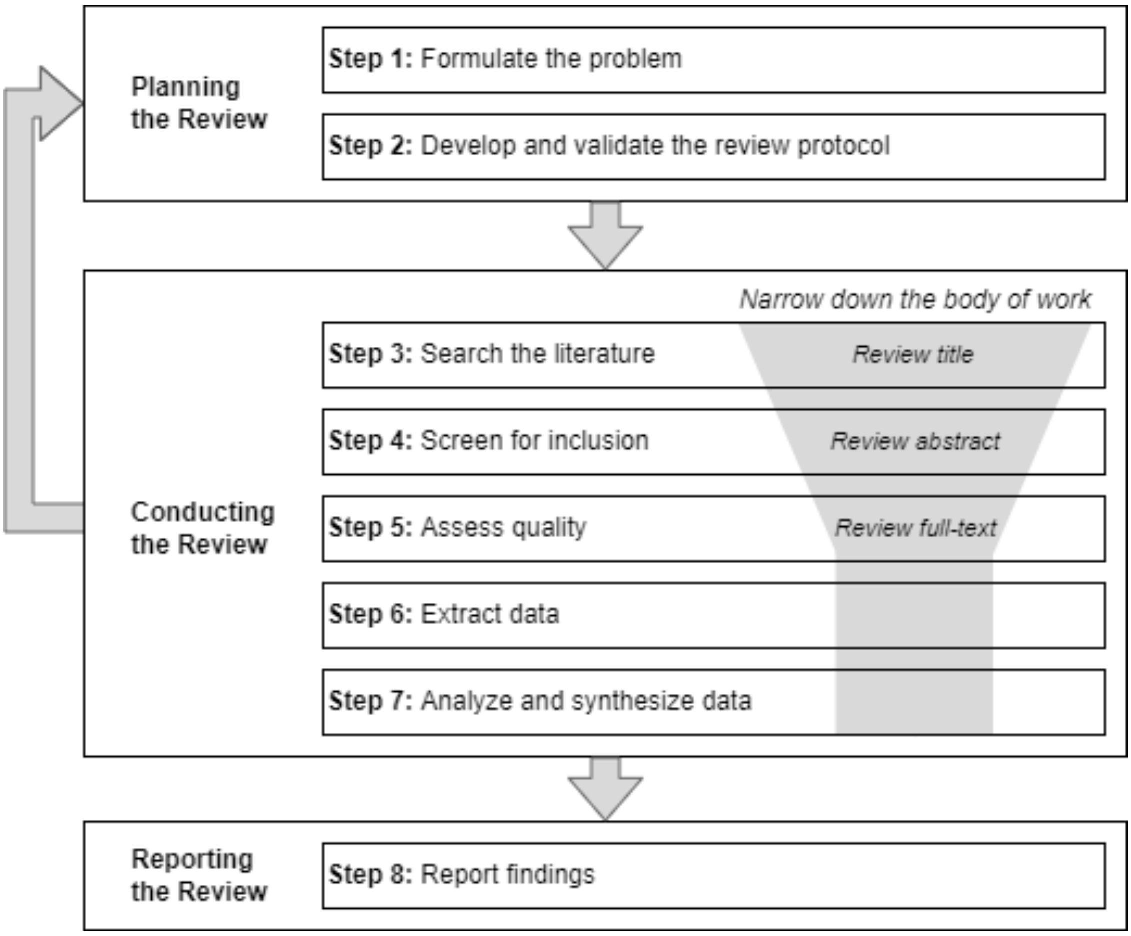

Planning
the Review
Step 1: Formulate the problem
Step 2: Develop and validate the review protocol
Conducting
the Review
Narrow down the body of work
Step 3: Search the literature
Review title
Step 4: Screen for inclusion
Review abstract
Step 5: Assess quality
Review full-text
Step 6: Extract data
Step 7: Analyze and synthesize data
Reporting
the Review
Step 8: Report findings

Figure 4 Process of SLR (Xiao & Watson, 2019, p. 103)

3.1.1 Planning the Review

Step 1: Formulate the problem

The initial step in our SLR is identifying the purpose, where we will mainly examine our topic and make an endeavor to answer our problem domain. Defining research questions limits the scope of our study, reducing the likelihood of retrieving irrelevant information. The entire literature review process is driven by our RQs (Kitchenham & Charters, 2007, p.3). Defining appropriate RQs can be an iterative process (Xiao & Watson, 2019, p.103). Our experience through the literature review process confirms that after acquiring a broader knowledge of the topic, the RQs have frequently evolved.

Table 3 shows our initial RQs, in addition to the current RQs that the iterative process has contributed to develop (see table 3).

Table 3 Research questions

	Initial	Current
RQ1:	How does the fast-evolving digitalization affect cyber security in the power sector?	Why is cyber security in current procurements of third-party suppliers in the Norwegian power sector challenging?
RQ2:	How has the power sector changed as a result of digitalization?	How can the management in the Norwegian power sector make better decisions in the procurement of third-party suppliers?

Step 2: Develop and validate the review protocol

The development and validation of the review protocol is a tool which has simplified the review procedure for us as researchers. The protocol includes guidelines for including and excluding literature for our review. This has intended to provide consistency in the literature review. To reduce the risk of research bias, the pre-determined protocol has been applied (Kitchenham & Charters, 2007, p.12). This has intentionally increased our efficiency and reduced redundant work (University of South Florida, 2021). With the protocol's assistance, we have been able to stay on track, avoid heading in the wrong direction. It has helped us to systematically find sources related to our problem domain (see appendix A).

3.1.2 Conducting the Review

Step 3: Search the literature

The collected resources have a considerable impact on the quality of the literature review. We have utilized three main methods for finding literature. These methods refer to electronic databases, forward searching and backward searching (Xiao & Watson, 2019, p.103). Additionally, our stakeholders have provided relevant research materials. Our literature was mainly collected through electronic databases. Because no database contains the total amount of published research papers, our systematic literature search has included multiple electronic databases (Xiao & Watson, 2019, p.103). The review protocol in the appendix presents our search strategy, which contains selected electronic databases, the defined keywords and different year of publication criteria for the research areas (see appendix A). After the collection of literature through multiple databases, the method of conducting backwards searching was applied. The intention of applying this method was to obtain deeper knowledge of the theory and supplement our findings (Okoli, 2015, p.894).

Step 4: Screen for inclusion

The procedure of screening each article after compiling our references has been done to determine whether it should be included for data extraction and analysis (Xiao & Watson, 2019, p.105). After developing our review protocol in a prior step, we defined eligibility criteria for the literature that further has been included in the process (see appendix A). In the search for literature, we screened a total of 56 research papers and reports. As the intention of the screening process has been to weed out resources that have been inapplicable to our research questions and defined criteria's, the number of articles were reduced (Xiao & Watson, 2019, p.105).

Step 5: Assess quality

To assess the quality of the literature, we created two tables which define our exclusion and inclusion criteria's (see appendix B & C). The initial task we did was reviewing the title of an article or report to identify if it was applicable for our topic and research questions. If the title of the article was relevant, we took a more in depth look at the abstract. Subsequently, a full text review was conducted if the criteria were approved.

Step 6: Extract data

Data extraction was the process where we structured primary studies in an organized manner using a table. The following information has been listed in the literature inclusion criteria which are found in the appendix (see appendix C). The table includes title of article, author, year, synthesize type and summary.

Step 7: Analyze and synthesize data

Organizing the data was the next step after the data extraction process. This process forms a collating and summarization of our included primary studies (Kitchenham, 2004, p.18). We chose to include the synthesis type in the *Literature Inclusion Criteria* table where we have specified which form of methodology the primary sources have used (see appendix C). This provides an overview of which methods the researchers have applied to investigate the various topics. Additionally, we got an overview of the types of data that are expected to be included, numerous data or textual description of behavior and experiences.

3.1.3 Reporting the Review

Step 8: Report findings

The acquisition of literature has been a comprehensive task which has required a sufficient amount of documentation. To visualize our process in a structured manner we created a flow-chart which displays the task of weeding out literature. The figure below explains the process of having the total number of identified records, narrowed to our included studies (see figure 5).

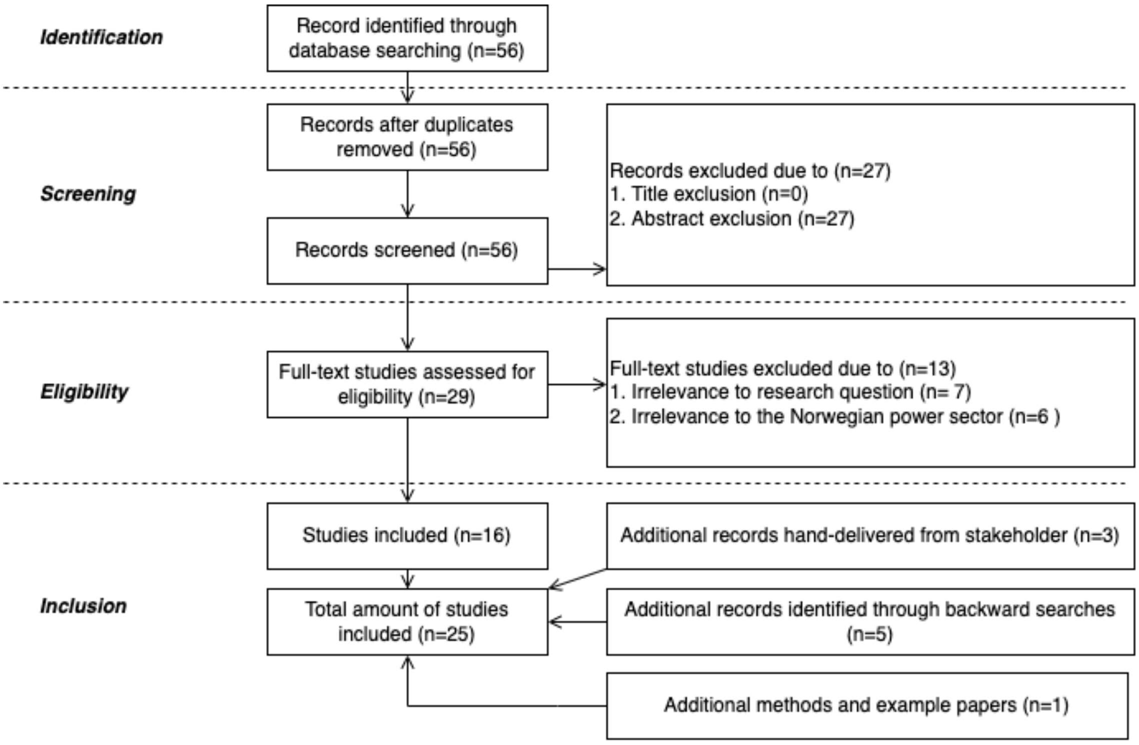

Identification
Record identified through database searching (n=56)
Screening
Records after duplicates removed (n=56)
Records screened (n=56)
Records excluded due to (n=27)
1. Title exclusion (n=0)
2. Abstract exclusion (n=27)
Eligibility
Full-text studies assessed for eligibility (n=29)
Full-text studies excluded due to (n=13)
1. Irrelevance to research question (n= 7)
2. Irrelevance to the Norwegian power sector (n=6)
Inclusion
Studies included (n=16)
Additional records hand-delivered from stakeholder (n=3)
Total amount of studies included (n=25)
Additional records identified through backward searches (n=5)
Additional methods and example papers (n=1)

Figure 5 Report findings flow chart (Xiao & Watson, 2019, p. 108)

3.2 Research Approach

According to Hafiz, the conduction of a case study should be considered when the focus of the study is to answer "how" and "why" RQs (Hafiz, 2008, p.545). As our RQs is specifically aimed at these kinds of questions, we decided to conduct a case study research method during our thesis. The aim is to cover contextual conditions because we concluded that they are relevant to our study (Hafiz, 2008, p.545). The goal of a case study is to gain as much knowledge about a specific event, person, or process (Njie & Asimiran, 2014, p.36). There are two distinct types of research that can be applied in our case study: quantitative and qualitative (Amaratunga, Baldry, Sarshar & Newton, 2002, p.19). As data collection is a necessary component in our case study, the choice of an appropriate approach and research method is essential. Each approach has its intended purpose and advantages.

A qualitative research approach gives insight into people's experiences using research methodologies such as focus group discussions, interviews, observation, and content analysis. Being able to communicate with participants during the study process is one of the benefits of conducting qualitative research. This process allows us as researchers to ask questions, talk and observe participants to develop a deeper understanding of the defined area which is explored. By using this method, it is possible to obtain an extended knowledge foundation based on real world experiences (Hennink, Hutter & Bailey, 2020, p.10).

The process of choosing a suitable research approach has been structured by identifying the differences between each approach. The table underneath summarizes the differences between both approaches (see table 4).

Table 4 Research approach difference (Khasawneh, 2009, p.67)

	Qualitative	**Quantitative**
Objectives	Description, exploration, and discovery	Description, explanation and prediction
Type of research	Exploratory	Descriptive
Focus	Examining the phenomenon's breadth and depth	Specific theories are being tested
Measurement	Researcher as instrument, “insider view“	Psychological / physiological instruments, “outsider view“
Approach	Flexible, natural setting	Highly controlled, experimental setting
Data collection	Unstructured, semi-structured or structured	Structured techniques
Sample	Purposive (evolving), small sample size	Statistical (predetermined) sample, large sample size
Data analysis	Coding, categories, themes: basic element of analysis is words/ideas	Statistical inference / statistical estimation: basic element of analysis is numbers

Outcome	Develop an initial understanding and sound base for further decision making	Used to recommend a final course of action

3.3 Research Design

The objective with the case study is to examine the challenges in the procurement of third-party suppliers in the Norwegian power sector and identify how the management can make better decisions with the procurement of third-party suppliers. This highlights our target group which mainly are managers with decision-making privileges and personnel that possess knowledge of cyber security. As our defined target audience is rather narrow, the use of quantitative methods can have limitations in relation to the sample size of respondents. Additionally, our objective requires more in-depth research that explores our problem domain with the intention of discovering valuable knowledge, which is possible to achieve by conducting qualitative research. This forms the foundation for making the decision to carry out qualitative research through this case study, as this approach is most suitable for our project. The study follows an inductive approach, where iterations of data collection have been made. This approach has been utilized to consolidate raw textual data into a simplified summary format, which aims to provide a systematic process for analyzing qualitative data which intentionally produce a reliable and accurate result (Thomas, 2006, p.237). Our aim of applying the inductive approach is to allow research findings to emerge from frequent and dominant themes inherent from the transcription, excluding restraints imposed by more structured methodologies. Our three main purposes underlying the appliance of the general inductive analysis approach are as the following:

1. Simplifying and compromising transcription from the SSI`s into a brief summary format
2. Establish parallels between our RQs and the empirical findings derived from the transcription, and assure these links are apparent and justified in context of the problem domain.
3. Explain the underlying structure of the experiences and processes evident by the transcriptions, to develop a figure

(Thomas, 2006, p.238).

3.4 Data Collection

To be able to collect facts and gain insights and understanding of opinions, attitudes, experiences, processes, behaviors and predictions, interviews have been used as our data collection tool of choice (Rowley, 2012, p.261). There are three main types of interview structures: unstructured, semi-structured and structured interviews (Harrell & Bradley, 2009, p.25). Each interview structure has their advantages. Based on a report provided by Harrel & Bradley, we developed a summarization of the various structures to identify which one that suits our data collection process the most (see table 5).

Table 5 Interview structures (Harrell & Bradley, 2009, p.26-28)

Unstructured interview	**Semi-structured interview**	**Structured interview**
- Minimum control of how the respondent answers. - Large variations in the direction of the conversation, significantly varying from each respondent. - The interviewer has only slightly control over the discussion's direction. - Free-flowing interview session. - Time consuming.	- Uses a guide with questions and topics. - Utilizes some standardized questions to ensure that the correct material is fully covered. - Conversational form of data collection. - Used to delve deeply into a defined topic and understand provided answers.	- High degree of control of how respondents answer. - Fixed questions that are asked in a defined order. - Respondents will be asked identical questions, in the defined order. - Limited explanations if questions or terms are not understood. - Used in larger samples to generalize a larger population.

The conduction of SSI has been our method of choice because of two primary considerations. The first being that this method of data collection is well suited for exploring perceptions and opinions of interviewees regarding our topic with the help of two-way communication. Conducting SSI`s allow us as interviewers the ability to ask follow-up questions, further clarifying the responses (Barriball & While 1994, p.330). The second consideration is that this method is suitable to delve deeply into our topic and to thoroughly understand the answers that are provided (Harrell & Bradley, 2009, p.27).

3.4.1 Research Subjects

Defining our target group has been necessary to be able to answer our RQs. The research subjects that have been selected are IT personnel with decision-making privileges, desirable in relation to the acquisition process of suppliers, including personnel that possess cyber security competence within the power sector. These two target groups have the most suitable foundation for being able to elaborate on our RQs. Additionally, we have focused on retrieving an even distribution on the various segments within the power sector which include power production, support system, TSO and DSO. The aim of defining our research subject in advance has been to narrow our target group, simplifying the process of identifying interviewees.

The duration of each interview has been set to approximately 30 minutes, which is most common for SSI`s (DiCicco-Bloom & Crabtree, 2006, p.315). Our goal has been to conduct between 8-12 interviews, which will be feasible to complete within our time frame. However, a factor that can affect the number of interviews is saturation. Saturation in our data collection means that no additional information is being found, where we can develop new knowledge (Saunders, Sim, Kingstone, Baker, Waterfield, Bartlam, Burroughs & Jinks, 2018, p.1895). When information from previous interviews starts to repeat, may indicate that we gathered a sufficient amount of information.

In order to protect our interviewees privacy during data collection, we chose to anonymize the data that were retrieved during the interviews. The intention with anonymize was also to give reassurance to the interview subjects so they can tell their story from their perspective without getting reactions and to get the most honest answers and opinions. The anonymization of our participants was decided at an early stage of the project, where we also have clarified this in our consent form that has been sent out in advance to the interviewees (see appendix E). The table below presents our various interview subjects, their representative organization function in addition their defined reference code (see table 6) .

Table 6 Research subjects' role

Role	**Organization function**	**Reference code**
Cyber Security Advisor	Support system	CSA-SS
IT responsible	Production & DSO	IT-PDSO
IT responsible	DSO	IT-DSO
Cyber Security Advisor	TSO	CSA-TSO

Chief Information Security Officer	DSO	CISO-DSO
Cyber Security Advisor	TSO	CSA-TSO
Chief Information Security Officer	Production & DSO	CISO-PDSO
Chief Executive Officer	Support system	CEO-SS
IT responsible	Production	IT-P
Chief Security Architect	Support system	CSA-SS

The defined organizational functions associated with the interviewees are classified as follows: *Support systems* are companies that add value to the Norwegian power sector and that are not directly linked to power production or distribution. *DSO* are companies that are only connected to distribution. TSO`s are in charge of controlling and operating the transmission grid. *Production* are companies that explicitly deal with power production. The pie chart below depicts the percentage distribution of organizational functions within the Norwegian power sector, which our interview subject is associated with (see figure 6). Our aim has been to retrieve an equal distribution of the various segments of the power sector in order to get the most holistic view of the industry, exploring and identifying experiences and opinions related to multiple point of view of procurement in SC.

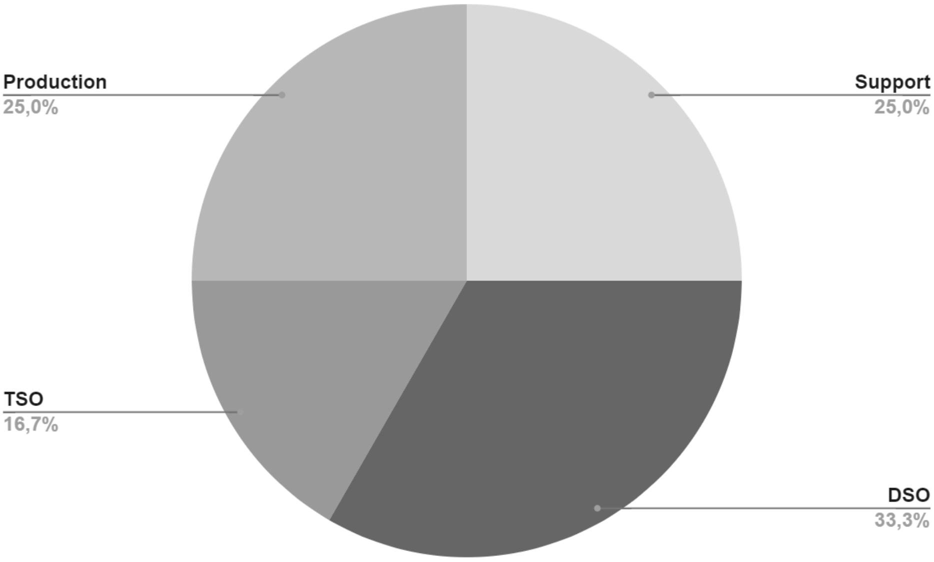


Figure 6 Distribution of the various included organization functions

3.4.2 Semi-Structured Interviews

To conduct our SSI`s, we have developed an interview guide which contributes to the objectivity and trustworthiness of the studies and makes the results more plausible (Kallio, Pietilä, Johnson & Kangasniemi, 2016, p.2954). Our interview guide has been based on a five-phase qualitative SSI guide provided by Kallio et al. (see figure 7).

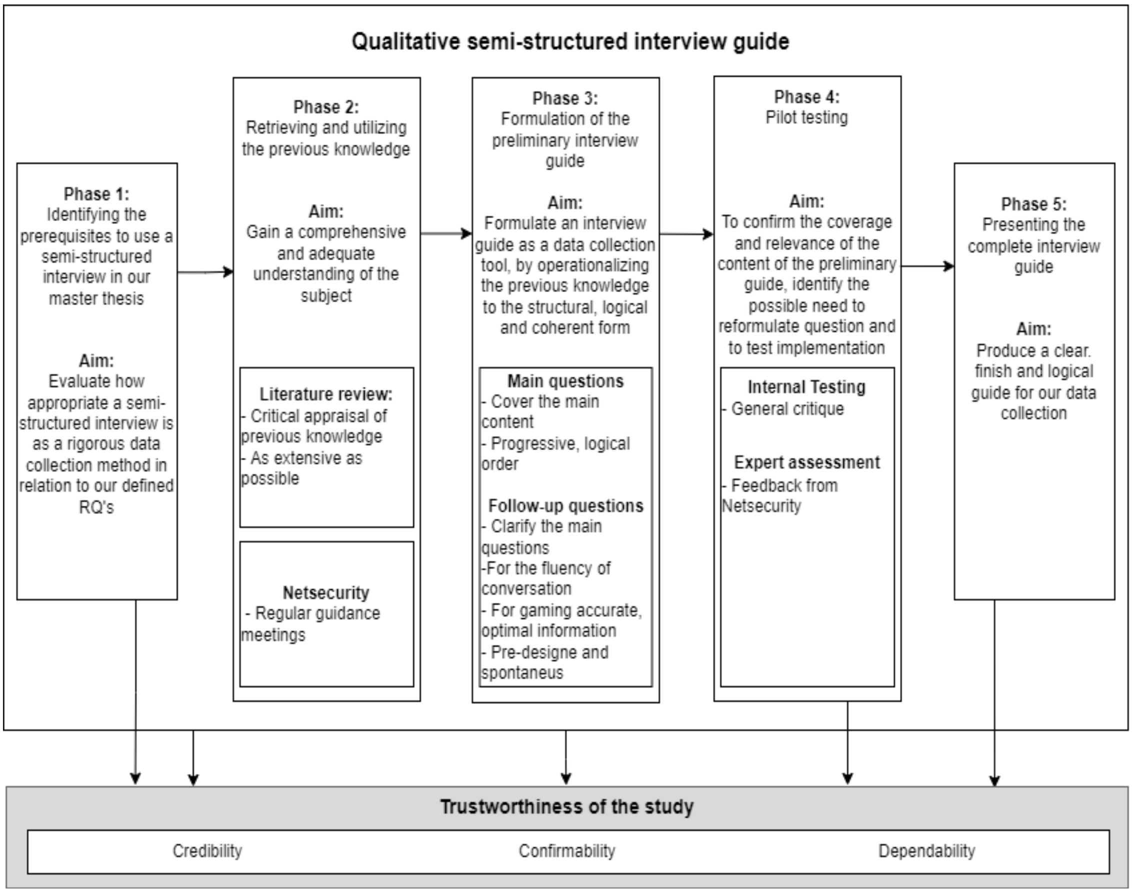

Qualitative semi-structured interview guide
Phase 1: Identifying the prerequisites to use a semi-structured interview in our master thesis
Aim: Evaluate how appropriate a semi-structured interview is as a rigorous data collection method in relation to our defined RQ's
Phase 2: Retrieving and utilizing the previous knowledge
Aim: Gain a comprehensive and adequate understanding of the subject
Literature review: - Critical appraisal of previous knowledge - As extensive as possible
Netsecurity - Regular guidance meetings
Phase 3: Formulation of the preliminary interview guide
Aim: Formulate an interview guide as a data collection tool, by operationalizing the previous knowledge to the structural, logical and coherent form
Main questions - Cover the main content - Progressive, logical order
Follow-up questions - Clarify the main questions -For the fluency of conversation - For gaming accurate, optimal information - Pre-designe and spontaneus
Phase 4: Pilot testing
Aim: To confirm the coverage and relevance of the content of the preliminary guide, identify the possible need to reformulate question and to test implementation
Internal Testing - General critique
Expert assessment - Feedback from Netsecurity
Phase 5: Presenting the complete interview guide
Aim: Produce a clear. finish and logical guide for our data collection
Trustworthiness of the study
Credibility
Confirmability
Dependability

Figure 7 Semi-structured interview guide (Kallio et al., 2016, p.2962)

According to Kallio et al., it is important that we have a good grasp of the substance of the research (Kallio et al., 2016, p.2959). This is done by acquiring knowledge through our SLR in phase 2. Prior knowledge has helped to create a foundation for our interview question. The aim of this guide has been to develop questions that have functioned as our standardized interview tool in our data collection process. The interview guide is described as a collection of questions that guides dialog during the interview toward our research topic (Kallio et al., 2016, p.2960). The defined interview questions were developed based on our new knowledge retrieved from the SLR. These questions have been formulated as our preliminary SSI guide. In total, 19 questions were developed in phase 3 which vary from cyber security challenges, how the acquisition process is today, what kind of insight the organizations have and what requirements are needed to the collaboration and acquisition process of other suppliers (see appendix D). After the creation of our questions for the interviews, pilot testing was conducted in phase 4. The aim of testing has been to confirm the coverage and relevance of the preliminary guide to identify the need to make changes to the questions, reducing the probability of getting misunderstood. This was completed by an expert assessment conducted by our stakeholders. After the review was completed, we were able to make informed changes and adjustments to the interview questions, improving the quality of the interview guide (Kallio et al., 2016, p.2960).

3.4.3 Potential Issues with Conducting Semi-Structured Interviews

There are a variety of challenges and limitations that may arise when conducting SSI's. Table 7 highlights the issues, limitations and solutions associated with the qualitative methodology. Several of the challenges described below are well-known issues that may occur when conducting qualitative research (Queirós, Faria & Almeida, 2017, p.379; Barriball & While, 1994, p.332). The following issues and limitations which may emerge are included to prepare solutions in advance of occurrence, to prevent unnecessary use of time and resources.

Table 7 Issues/limitation and potential solutions within qualitative research approach

Issues and limitation	Solutions
Unclear/bad answers When we ask questions, the interviewee replies with misleading or unclear responses. It is hard to obtain detailed information.	We can solve this by having well formulated questions, so that the interview subject clearly understands what we are asking about.
Time constraints/lack of time The interviewee may have a schedule that limits the amount of time we have to do the full interview.	Develop well-defined questions that can be answered effectively.
Not answering/refuse to be interviewed The person that has been contacted to participate in the interview could potentially not respond or refuse to be interviewed.	Contact several potential participants to increase the likelihood of retrieving a suitable amount of interview subject.

Feeling apprehensive about being interviewed Interview subject could feel apprehensive regarding the interview.	Explain the process in fine detail to participants that may find it apprehensive being interviewed. Share interview questions with participants in advance to make it possible to prepare for what is being asked in the interview.
Not wishing to answer certain questions during the interview Participants may find it inappropriate to answer certain questions.	Conduct multiple interviews to gather an equal number of respondents to the defined questions.
Refusing to have the interview audio taped Interview subjects may find it inappropriate to answer questions if the interview is audio taped.	Specify what the information will be used to, how long it is being stored and on what medium it is stored at. In situations where this occurs, ask the participant if it is better to only write notes during the interview.
Not showing up Participants may agree to be interviewed but do not show up for the scheduled meeting.	Start the interview process early and plan to potentially conduct more interviews if necessary.

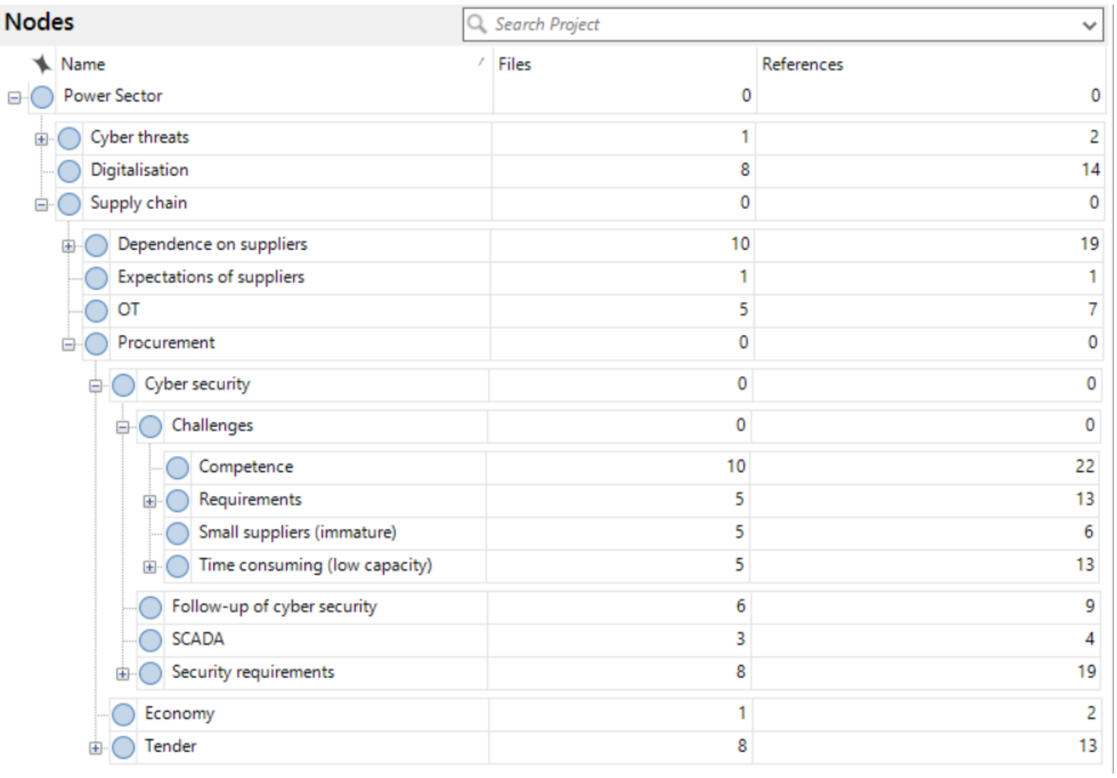
3.5 Data Analysis

After completing 10 SSI`s in different segments within the Norwegian power sector, the process of analyzing the obtained data began. Our initialization was to prepare the collected data to be analyzed, this was conducted by transcribing the interviews. Each interview has been sound recorded with a dictaphone application from UiO, an application that has been approved for usage in academic research purposes and complies with guidelines set by Norwegian Center for Research Data (NSD) for data processing, to ensure that an identical replication of the contents of each interview were available which facilitates our analysis (Barriball & While, 1994, p.332).

To efficiently organize the retrieved data from the SSI`s, the tool NVivo 12 has been utilized. NVivo is a complex analysis tool for qualitative research that helps to organize different types of data, code and systematic analyzes and form conclusions (UiO, 2020). Our need of processing unstructured data from our SSI`s made it appropriate to apply this tool. This increased the efficiency of our workflow as manual tasks became more autonomous. However, the analysis was still conducted manually by us as researchers. Subsequently, we have used a process provided by the National Science Foundation (NSF) to structure our analysis of the SSI`s. The goal of our data analysis has been to identify and understand meaningful patterns that will help us answer our RQs (NSF, 1997).

All acquired data originating from our SSI`s needed to be organized and reduced in a meaningful manner. According to the NSF, data reduction is the first of three elements of qualitative data analysis. Data reduction aims to focus, simplify, and transform our data, making it more manageable (NSF, 1997). NVivo 12 was utilized to code the raw data from our SSI`s, simplifying the process of excluding irrelevant information. To identify the most relevant data, our RQs were used to filter the information. Data that has relevance to our questions was included, and irrelevant data were excluded.

Data display is the second element of qualitative data analysis. This element goes a step beyond data reduction to provide "an organized, compressed assembly of information that permits conclusion drawing" (NSF, 1997). The process of displaying data has assisted our research to visualize the collected information systematically, in order to draw valid conclusions (Miles & Huberman, 1994, p.91). By utilizing NVivo, identifying higher order categories and themes that emerged from the retrieved data were visualized through nodes, displaying systematic patterns and interrelationships in the data (see figure 8).



Name	Files	References
Power Sector	0	0
Cyber threats	1	2
Digitalisation	8	14
Supply chain	0	0
Dependence on suppliers	10	19
Expectations of suppliers	1	1
OT	5	7
Procurement	0	0
Cyber security	0	0
Challenges	0	0
Competence	10	22
Requirements	5	13
Small suppliers (immature)	5	6
Time consuming (low capacity)	5	13
Follow-up of cyber security	6	9
SCADA	3	4
Security requirements	8	19
Economy	1	2
Tender	8	13

Figure 8 NVivo data analysis

Figure 8 shows how our data has been categorized through themes by nodes represented within the “Name” column. Files refers to the number of interviews related to a specific node. References represent the total amount of interrelationships between data from our interviews and identified nodes.

The third element of our qualitative data analysis is conclusion drawing and verification. Our conclusion drawing has involved an evaluation of the analyzed data to assess how it contributed to answering the RQs. Subsequently, validation has been the process that has entailed audit of the data as many times as necessary to verify our conclusion (NSF, 1997). To verify and cross-check our conclusion, our stakeholders which possess specialist knowledge regarding cyber security within the Norwegian Power Sector, have provided their perceptions, experiences, and knowledge to enhance the integrity of our conclusion drawing from our qualitative research analysis. Validation of the conclusion with assistance of an expert ensures higher integrity to our study, verifying that data are credible, defensible, justifiable, and capable of withstanding alternative interpretations (NSF, 1997).

4 EMPIRICAL FINDINGS

The following chapter presents the findings originating from the data analysis of the SSI`s. The chapter includes dependency on suppliers, various challenges within the procurement of suppliers and cyber security requirements and measures which are set to procurements. The purpose of the empirical findings is to answer our RQs, with quotes that illustrate the findings provided by our ten informants.

4.1 Dependency on an Increasingly Digitalized Supply Chain

The majority of the interviewees have noticed change caused by digitalization. The remaining believe the power sector has undergone a natural development. CSA-TSO mention that: *"The digitalization has made it more difficult to handle more connections than previously, making it more demanding to achieve control."* This increases the dependency of knowledge provided by suppliers. Critical systems are getting more interconnected resulting from more utilization of IoT sensors and instrumentation which enlarge the overall attack surface. New systems are being formed as entrepreneurs create new businesses that integrate into an established market and other products and services are now accessible as a result of digitalization. IT-DSO state that: *"It is not possible to operate efficiently in today's society without cloud services."*

Companies in the power sector have a greater connection to some of their suppliers, enlarging their dependence on certain suppliers. Suppliers has comprehensive responsibilities and defined tasks to complete. CSA-SS highlight this by stating: *"There is a reason why suppliers are utilized. They have an important task to complete, and if the supplier cannot deliver, then something is wrong or not working properly."* All interviewees state that they are dependent on suppliers to operate IT and/or OT systems, where multiple of the suppliers are providing value in terms of development of new functionalities, patching or providing competence and support. Other kinds of suppliers offer services such as system monitoring and detection.

Downtime in crucial systems provided by suppliers is much more extensive as they have expert knowledge, which is not always available in-house. Cyber-attacks against the SC can affect the delivery of the product or potentially cause downtime. Critical systems are often duplicated to enhance the cyber resilience against successful attacks, reducing the likelihood of experiencing downtime. The majority of the interviewees mention that cyber-attacks against a supplier have considerable consequences related to downtime. However, IT-P highlight that: *"Downtime is not necessarily the worst consequence. Creating a backdoor like the SolarWinds incident is much worse."* Malware with the ability to spread is a problem that might have many extensive consequences across various segments if it spreads to the remainder of the operation controls.

4.2 Challenges with Procurement of Suppliers

Results from our qualitative research have provided valuable insight into challenges the Norwegian power sector is facing regarding their SC and procurement of suppliers. The figure below has been developed to illustrate the variety of challenges in the procurement and follow-up of third-party suppliers, which are identified through our data analysis (see figure 9).

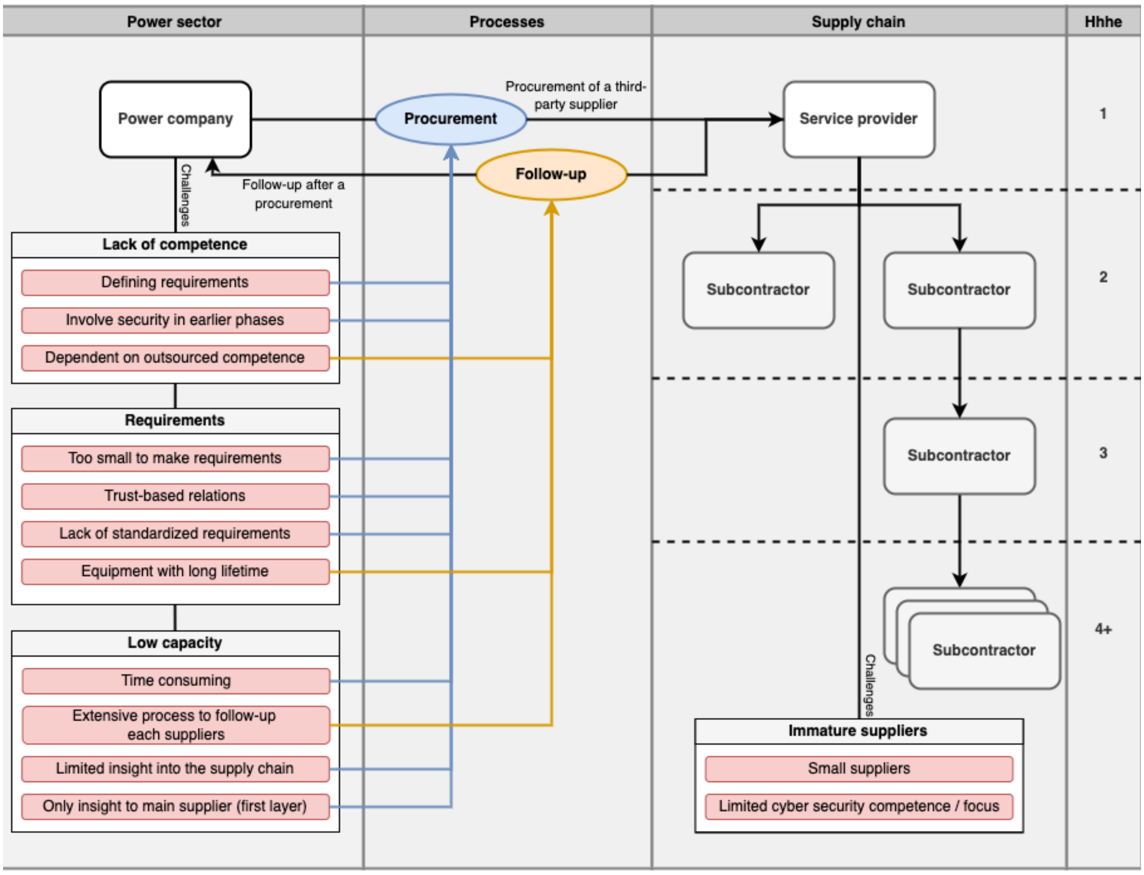

Power sector
Processes
Supply chain
Hhhe
Power company
Procurement
Procurement of a third-party supplier
Service provider
1
Follow-up
Follow-up after a procurement
Challenges
Lack of competence
Defining requirements
Involve security in earlier phases
Dependent on outsourced competence
Subcontractor
Subcontractor
2
Requirements
Too small to make requirements
Trust-based relations
Lack of standardized requirements
Equipment with long lifetime
Subcontractor
3
Low capacity
Time consuming
Extensive process to follow-up each suppliers
Limited insight into the supply chain
Only insight to main supplier (first layer)
Subcontractor
4+
Challenges
Immature suppliers
Small suppliers
Limited cyber security competence / focus

Figure 9 Challenges in procurement and follow-up of suppliers

The figure is divided into three main columns: *power sector*, *processes,* and *supply chain*. The first column, *power sector*, visualizes the challenges that are identified through our conducted data analysis. These challenges have subcategories which will be further explained. The second column, *processes*, show each process and what challenges that are interconnected. The third column, *supply chain,* illustrates the structure of a SC including subcontractors, divided into layers. Additionally, challenges that are directly related to the service provider and subcontractor are included.

4.2.1 Lack of Competence

The majority of our participants express concern about lack of internal cyber security expertise. Services that have nothing to do with local IT operations or cyber security are frequently ignored and may go under the radar in several procurements. As an example, provided by CEO-SS:

> *If someone buys a cloud-based HR system or personnel system, the assessment is mostly addressed by the department that acquires the system. The security requirements that are set for other IT systems could potentially be left out.*

This can create vulnerabilities for any company within the power sector, based on lack of cyber security assessments in the procurement. Interviewees mention that cyber security is included too late in the procurement of a supplier. IT-P confirms this by stating that: *"Cyber security surely needs to be more involved in the projects at an earlier stage. It is often included too late."* According to 50% of our interviewees, incorporating cyber security at an early stage might contribute to improving cyber security in the procurement. IT-P mention that: *"After the procurement of a supplier, the cyber security functions a bit like a brake pad in many cases. Particularly in smaller projects where the procurement perhaps happens a bit more uncontrolled."*

Research participants mentioned that they do not want to have all competence in-house, but rather control it. It is a balancing act to have control and manage processes internally and rely on competence in what the supplier can offer. CISO-DSO stated that they have a philosophy where they use partner networks to always have a high level of competence, but also to scale in breadth for a greater robustness in relation to capacity. However, CISO-PDSO stated that: *"Internal IT competence is to a large extent scaled down since most experts are becoming potatoes after 4-5 years."* Expert competence is rather retrieved through outsourcing to dynamic environments which constantly strive to acquire up-to-date knowledge. If an incident occurs, the organization may face significant difficulties since it is frequently regulated in such a manner that it is dependent on the competency of the supplier.

4.2.2 Requirements Definition

The competence challenges make it demanding to define an adequate set of cyber security requirements for the procurement of a supplier. *"It is demanding to define clear requirements if you do not have sufficient internal competence."* The data analysis highlights that there is a lack of overall standardization of cyber security requirements for procurement of suppliers within IT and OT systems in the Norwegian power sector. The majority of our interviewees refer to the power contingency regulations, which are regulations on security and contingency in the power supply. CSA-TSO mention that:

> *Today, there is no set of requirements that you absolutely must be able to satisfy. However, we use the power contingency regulations in the procurement, and it is interpreted. It is not extensive enough to cover all procurement areas.*

An informant mentioned that there are checklists provided by NVE for ICT security in procurements and outsourcing in the Norwegian hydroelectric power sector which may be applied, but this is not a requirement. Multiple informants mention that they must obtain the necessary information to assess, as well as set requirements for the suppliers themselves. The process of defining cyber security requirements is an extensive task which includes comprehensive lists of requirements. These requirements are not always as easy to understand and can be misunderstood.

Trust-based relations to supplies are frequently mentioned in conversations with our informants. These relations are often based on prior contracts, which form a foundation for trust. In some cases, it is mentioned that it is easier to build trust-based relations if the supplier has delivered similar services to other customers in the power sector.

Audits are a part of defined requirements for the majority of the informants, but they mention that the Norwegian power sector has a potential for general improvement in this area. To maintain a defined level of security and threat knowledge across the SC it is critical that companies operating in the Norwegian power sector include audits into their requirements. Most of the informants mention that it is challenging to define requirements, also in relation to conducting audits to larger suppliers, based on the fact that most of the Norwegian power companies are small customers to certain suppliers on a global scale. Additionally, some of the Norwegian power companies experience that large suppliers can appear contradictory if they believe that the requirements are too strict. CISO-PDSO highlighted by stating:

> *Many large global suppliers do not provide the opportunity to make audits or have our own requirements. The suppliers have standard agreements. Take it or leave it. We are too small to have any influence.*

4.2.3 Low Capacity

The SC can be confusing and unknown to several companies in the Norwegian power sector. Not all personnel are equally familiar with this issue. 70% mention that they lack insight into how their supplier's subcontractor is securing their services. CSA-SS mention that: *"We have insight into the first supplier, but no more than that."* Extensive SC`s make it challenging and close to impossible to have control over all suppliers. IT-DSO mention that: *"Subcontractors have the same requirements as suppliers. However, in practice we are unable to follow up. We have no control at that layer."*

Certain suppliers are large and have a significant number of subcontractors. This causes some of the Norwegian power companies to rely on the supplier to have control of which subcontractors they utilize, the components they provide and how they are put together. IT-DSO mention that: *"We do not have the capacity to handle it as we would like. At least not with direct audit or follow-up, it is too demanding."* IT-DSO mention that procurements which are considered critical or especially important are requested for insight further into the SC. This is rarely the case through all individual subcontractors. In some cases, this is only carried out once due to lack of capacity. Agreements and contracts often include requirements in relation to conducting audits, but multiple informants mention that the process of follow-up the SC is significantly resource demanding and time consuming.

4.2.4 Digital Readiness of the Supplier

The digitalization has introduced a variety of new suppliers and systems which are rather small compared to well-established ones. 50% of the interviewees mentioned that suppliers are to a varying degree focused on cyber security. Some of the interviewees mention that smaller suppliers have a lower level of cyber security maturity. IT-P mentions that: *"My impression about cyber security around these small suppliers is that security is not high on their list, there is something we have to impose."* This might be due to the fact that smaller suppliers in some cases lack the knowledge, competence and resources related to cyber security that other larger suppliers may possess. CSA-SS highlighted this by saying: *"Smaller suppliers are more immature and need much closer follow-up. They are not as mature in terms of cyber security as the larger companies."*

Informants highlight another point of view by mentioning that there are some highly cyber security mature companies that buy equipment from very small companies in Norway that do not possess IT personnel. These cases may require the main supplier to help the individual subcontractor to enhance their competence. CEO-SS mention that: *"The largest threats are simply the width of attacks that are coming now. A company of two people is as vulnerable as one with 1,500 employees."* Multiple informants state that several suppliers lack threat understanding. In multiple cases, suppliers which do not focus on enhancing their threat understanding and general cyber security competence constitutes the weakest link.

4.3 Cyber Security Requirements and Measures

All interviewees utilize comprehensive sets of requirements in the procurement. Being competent at defining requirements is considered as an essential task for obtaining the proper supplier. However, lack of cyber security requirements is mentioned as a process problem. CEO-SS mentioned that: *"All parts of an organization should have a relation to cyber security, possibly also in the hiring process."* Visualized in the figure underneath is the relationship that *requirements* have towards the power company and procurement of suppliers (see figure 10). The various aspects of the figure form the structure for the following chapters. The yellow requirement-boxes, certification, and extensive contracts, represent neither positive nor negative aspects but rather neutral points. The green boxes, geographical location, and the power contingency regulations, are positive requirements.

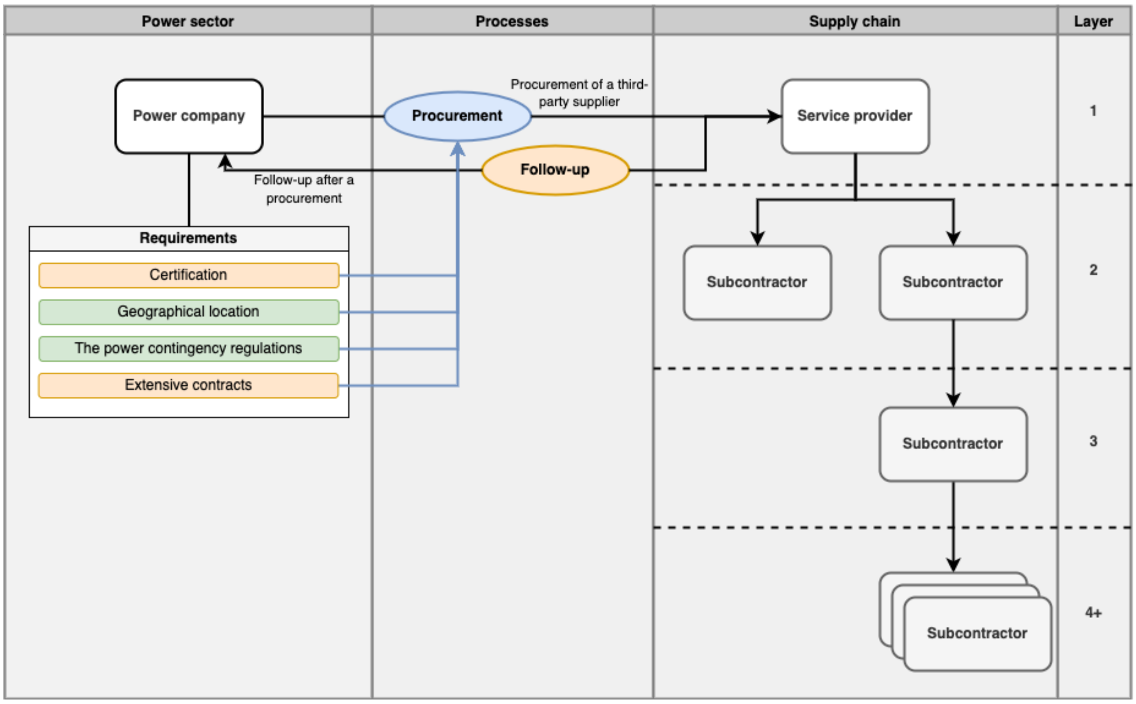


Figure 10 Requirements and measures with procurement of suppliers

4.3.1 Certification

The interviewees provided mixed answers to whether a certification in accordance with international security standards would help in the procurement. The majority of the interviewees believed a supplier would be more attractive if they were certified. CISO-DSO mentioned that: *"When we get suppliers who certify themselves, it is easier to gain trust, because it indicates that they have a system and internal control to ensure that they comply with good practice on information security."* None of the participants utilize defined requirements that suppliers must follow international standards or have completed cyber security certifications. However, it is considered as a positive factor in a procurement if the suppliers utilize certificates or follow international standards. Some companies have included certification in their ICT checklists based on recommendations provided by NVE. Having specific requirements related to certification may exclude potential supplies. CSA-TSO mention that having certifications can cause false security. CEO-SS highlighted this by saying:

> *It can lead to false security. Certifications are showing that you have thought about different things, but there are no audits checking the actual work that is being done in accordance with what has been said.*

Certification is seen as verification of accomplishment. However, it frequently covers a restricted topic. Even though certifications have been completed, it is not assured that it covers the areas that are desired. This is confirmed by CEO-SS, who said*: "It has something to say that they are certified, but it is not enough."* The good may become its own enemy. In the sense that the emphasis will be meeting a large number of requirements rather than providing true security.

4.3.2 Geographical Location

When it comes to procurement, most of our participants mention that geographical location is important. The majority of informants state that they have requirements regarding data storage within EU, EØS and NATO countries. CSA-SS states:

> *The first thing we look at is geographical location. Is it a sales solution or cloud solution, where do they stand? Where are their IT technologies located? Who has access to the system? What consequences can it have for internal systems? Where do we connect them?*

Some informants mention that they prefer to collaborate with Norwegian and Nordic suppliers. An IT responsible mentioned that they do not necessarily have these kinds of requirements, but rather ask if the data is being stored in a sensible location. Additionally, they do not go in depth to identify if suppliers have an overview of their own third-party vulnerabilities. Companies who utilize suppliers from other countries have strict requirements, especially on critical systems which affect the ability to have light in the bulb. These kinds of suppliers cannot be countries that Norway does not have security policy cooperation with. CISO-PDSO mention that:

> *The power contingency regulations state that you must have suppliers from the EU, EØS or NATO, which is a bit challenging. One thing is the first layer, the service provider, but is it relevant when things are produced globally.*

4.3.3 The Power Contingency Regulations

The power contingency regulations are frequently referred to by our interviewees. These regulations, in addition to the energy act, relate to the entire Norwegian power sector. It states that the supplier must be familiar with the power contingency regulations and must operate in accordance with it. The regulations include requirements regarding cyber security, and it has specific requirements related to procurement in chapter 6, § 6-5. Procurements. CSA-TSO highlighted this by saying:

> *In accordance with the power contingency regulations, it says that our organization must have control. You must sign a security agreement, and the so-called security agreement is what you use to regulate conditions down the supply chain.*

However, CSA-TSO and IT-P stated that there are not as strict security requirements for companies that are of a smaller size, such as unclassified power plants. *"Small power plants that are unclassified do not have the same requirements. Many small power suppliers have more types of solutions where you can nearly operate the power plant from the couch using an iPad."*

4.3.4 Extensive Contracts

Extensive agreements and contracts are developed in the procurement of suppliers. These contracts are comprehensive documents which are sent back and forth between power companies and suppliers. The defined requirements are objectively evaluated to what extent they meet the demands set in the contracts. CSA-TSO mentioned that: *"Meaningless or irrelevant answers can lead to further investigation in advance of a procurement, making the process more demanding and on some occasions frustrating for both parties."* Another informant mentioned that suppliers need to provide a list of which subcontractors they use, varying from the type of access and insight the supplier intends to have.

The responsibility for cyber security is imposed on the supplier through contracts. All of the respondents stated that they only focus on the first layer in the SC, but they urge contracts to be reflected down the SC. CSA-TSO mention that: *"If a supplier uses subcontractors, it is the main supplier's responsibility to ensure that the subcontractor complies with the requirements provided in the contract."* It is frequently questioned if the supplier's compliance with the requirement has been revised subsequently. The degree to which this is followed up varies significantly.

5 DISCUSSION

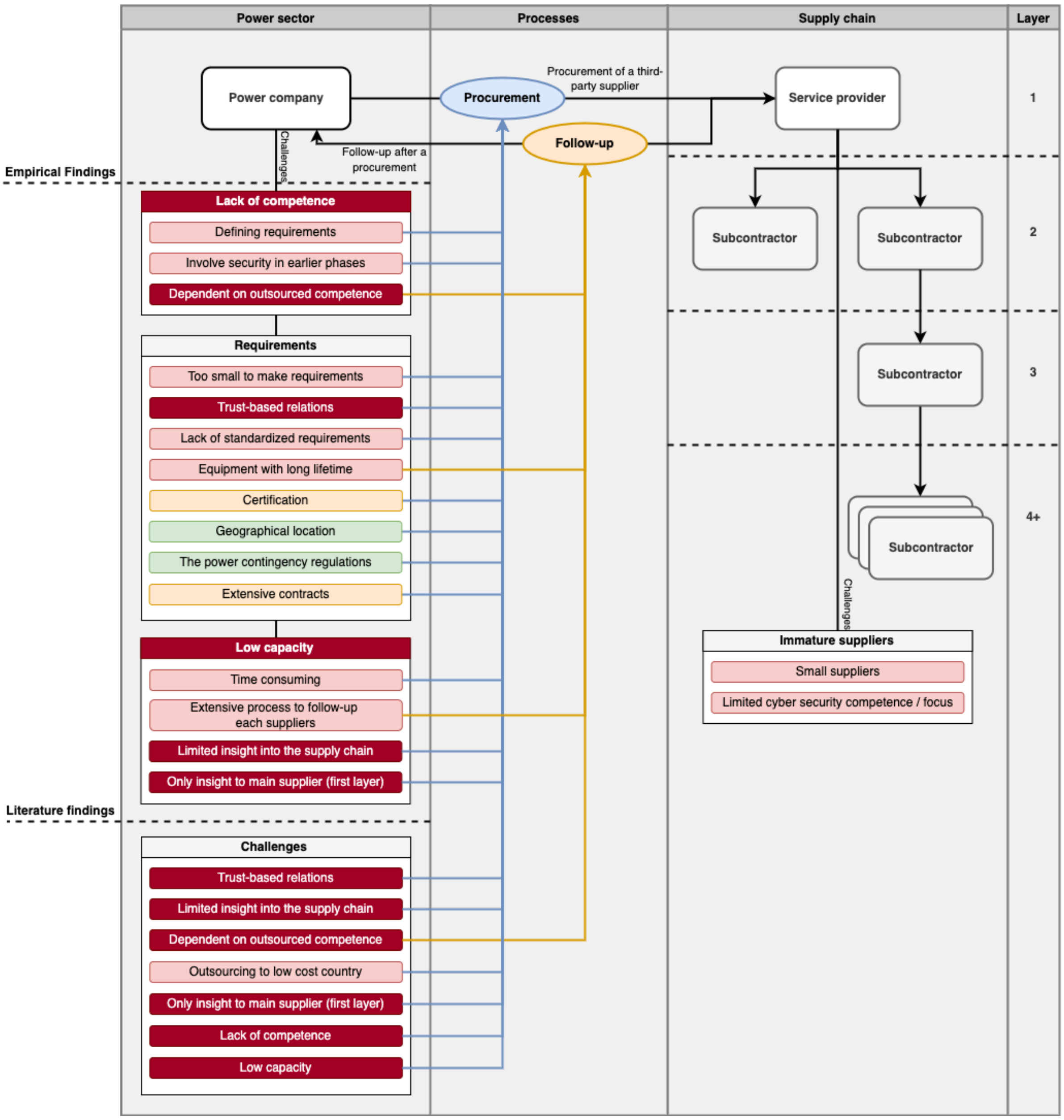
The following chapter discusses the literature findings from the background and related work upon the empirical findings retrieved through our qualitative research, where differences and similarities are examined. The intention is to answer our problem statement regarding how digitalization has changed the procurement of third-party suppliers of IT and OT technologies, focusing on cyber security, in the Norwegian power sector. Subsequently, answering our RQs.

RQ 1: Why is cyber security in current procurements of third-party suppliers in the Norwegian power sector challenging?

RQ 2: How can the management in the Norwegian power sector make better decisions in the procurement of third-party suppliers?

The figure below illustrates our findings from both the literature review and empirical findings which are discussed in this section. Underneath the first dotted line in the power sector column is our empirical findings, while the literature findings are visualized below the second dotted line. We used a dark red hue to highlight similar challenges to make it easy to compare the findings. These challenges represent similarities that are repeated in the literature finding and our empirical findings (see figure 11).

Figure 11 Supply chain procurement challenges


Power sector
Processes
Supply chain
Layer
Power company
Procurement
Procurement of a third-party supplier
Service provider
1
Follow-up
Follow-up after a procurement
Challenges
Empirical Findings
Lack of competence
Defining requirements
Involve security in earlier phases
Dependent on outsourced competence
Subcontractor
Subcontractor
2
Requirements
Too small to make requirements
Trust-based relations
Lack of standardized requirements
Equipment with long lifetime
Certification
Geographical location
The power contingency regulations
Extensive contracts
Subcontractor
3
Subcontractor
4+
Challenges
Immature suppliers
Small suppliers
Limited cyber security competence / focus
Low capacity
Time consuming
Extensive process to follow-up each suppliers
Limited insight into the supply chain
Only insight to main supplier (first layer)
Literature findings
Challenges
Trust-based relations
Limited insight into the supply chain
Dependent on outsourced competence
Outsourcing to low cost country
Only insight to main supplier (first layer)
Lack of competence
Low capacity

5.2 Dependency on an Increasingly Digitalized Supply Chain

The increased attack surface that has resulted from digitalization has increased the possibilities for exploitation (Livingston et al., 2018, p.2). Our empirical findings highlight that multiple interviewees have noticed change caused by digitalization. However, an insignificant number of participants mentioned that the sector has undergone a natural digital development. The growing interconnectivity of organizations and systems, as well as the widespread usage of digital communication, increases the danger of experiencing cyber-attacks (Vozikis et al., 2020, p.2). Interviewees confirm that digitalization has made it more difficult to handle more connections, making it increasingly demanding to achieve control, resulting in an increased dependency to the supplier. Increased interconnections to the control system are expected in the future (Haver et al., 2021, p.15). This indicates that a future affected by digitalization resulting in more interconnectivity, would likely make it more demanding to achieve control in the SC.

The number of new suppliers offering innovative digital and technological solutions is increasing (Haver et al., 2021, p.10; Azam, 2017, p.10). Our empirical findings confirmed this as entrepreneurs establish new enterprises that integrate into the existing market, enabling new systems to emerge as a result of digitization. Data originating from our data collection process identifies that it is not possible to operate efficiently without modern technologies. It is conceivable that the use of new technologies and services will be a natural part of the development of the SC, further enlarging the dependency on the supplier. However, the reliance on suppliers has increased the danger of cyber-attacks (Liang et al., 2018, p.45). The increased dependence on digital systems raises overall vulnerability, needing a higher level of security (Hagen et al., 2020, p.3). Companies in the power sector have a closer connection with some of their suppliers, increasing their reliance on them.

Downtime is a consequence which may arise as a result of a successful cyber-attack which could result in extensive consequences. This explicit problem area is insignificant in our literature findings. However, our empirical findings highlight that downtime is not necessarily the worst consequence. Enabling access to critical systems can cause much more extensive outcomes, as malware may be deployed which can spread to multiple segments of the SC and operation controls. The SolarWinds case is an example of this kind of attack, where a backdoor to their systems were included in an update which were distributed to 18 000 businesses globally, enabling threat actors to exploit the entrance and further compromise customers (NSM, 2021, p.25). This signals that similar events may occur in the future, affecting a further interconnected SC.

Control systems which previously have been physically separated are evolving into more remote-controlled systems, as they provide efficient operation and data to provide new services. As a result, these systems, like traditional ICT systems, are even more vulnerable to conventional cyber-attacks (NVE, 2017, p.5). These functionalities provide value in the SC but expose the sector for cyber-attacks in an increasingly extensive landscape of cyber threats.

5.3 Challenges with Procurement of Suppliers

To a considerable extent, power companies are dependent on suppliers, and only parts of cyber security can be verified (Hagen et al., 2020, p.6). All participants in the study confirm that they are dependent on suppliers to operate IT and/or OT systems. Suppliers add value through the development of new functionality, patching, and providing competence and support. However, interviewees highlight that there is significant concern about the lack of in-house cyber security expertise. The Norwegian power industry lacks ICT security knowledge, posing a significant risk to cyber security (Riksrevisjonen, 2021, p.8). The issue with obtaining in-house knowledge is that these personnel may be assigned to a variety of responsibilities, resulting in a more general emphasis rather than specific cyber security expertise. Certain companies within the power sector prefer to obtain expert competence through outsourcing to adaptive environments which continually seek to possess up-to-date knowledge. The extent to which an outsourcer's expertise understands what a company in the power sector needs is critical in procurement evaluations. In-house cyber security expertise may have a more holistic understanding of needs that the power sector possesses. A collaboration between in-house cyber expertise which provides the holistic view and outsourced cyber expertise which could possess more specified competence may result in more thoughtful cyber security requirements set in the procurement. The challenge of implementing cyber security earlier in the procurement is one of the consequences which can be linked to the lack of in-house cyber security competence.

It is essential that the power sector provide clear signals to suppliers that ICT security is a high priority, and that suppliers continue to improve their ICT operations and security skills (Riksrevisjonen, 2021, p.10). Procurement and administrative processes both require expertise. Making the right decisions allows companies to acquire the necessary equipment and technology, as well as put requirements into procurements and contracts with suppliers (NVE, 2017, p.30). The competence challenges make defining an adequate set of cyber security requirements for supplier procurement challenging. Our empirical findings identify a lack of overall standardization of cyber security requirements which apply in the procurement of suppliers, which differ from our literature findings which did not include research regarding standardized requirements. This might be due to the fact that developing these kinds of requirements, which apply to all companies within the Norwegian power sector, is an extensive task. Internal differences can make it difficult to comply with standard requirements. However, having general guidelines which may be applied in the process of defining cyber security requirements for the procurement could result in better, more secure procurements. It is possible to utilize current ICT security checklists provided by NVE, although it is not currently required.

Certain companies within the Norwegian power sector experience challenges regarding defining requirements towards larger suppliers in procurements. This issue is not identified in our literature review, but rather frequently highlighted in our empirical findings. Some suppliers do not allow companies to conduct audits or set their own requirements but apply standard agreements. Power companies state that they are far too insignificant to make demands. Larger suppliers possess significant amounts of customers in variable sizes. The challenge of defining cyber security requirements and requirements regarding audits toward these large suppliers is difficult. If all customers provide their own cyber security requirements towards a larger supplier, may result in way too extensive cyber security requirements. Compliance with all these cyber security requirements may be too difficult to achieve in practice.

The power contingency regulations apply to the Norwegian power sector, however there is a concern with how it can be interpreted. Different levels of competence may result in varied degrees of compliance outlined in this regulation. Due to a lack of internal expertise, defining clear procurement requirements is challenging. This is one of the pervasive and prominent SC vulnerabilities highlighted by NVE (Haver et al., 2021, p.3). Establishing cyber security requirements early in the procurement is significantly important because the contracts and agreements that include them are frequently reflected down the SC. Subcontractors must meet the same standards as main suppliers, emphasizing the need of clearly articulating ICT security requirements.

The majority of the power industry relies heavily on transparency and trust in its SC relationships (Ghadge et al., 2019, p.232). Our informants commonly reference trust-based relationships with suppliers. Trust in the SC is unlikely to disappear anytime soon (Kshetri & Vaos, 2019, p.10). These relationships are frequently founded on previous contracts, which form the basis for trust. Trust relations in SC is a complex issue which is challenging to measure and achieve (Kshetri & Vaos, 2019, p.7). In some circumstances it is simpler to establish trust-based relationships if the supplier has previously provided similar services to other clients in the power sector. This complies with the literature findings and our empirical findings.

It is difficult to obtain a clear understanding of the vulnerability landscape because of the increasing reliance on complicated SC`s (NSM, 2020, p.24). The majority of the research subjects highlight that they lack insight into how their supplier`s subcontractor is securing their services. The majority of our interviewees state that they only have insight into the first layer of suppliers. The lack of capacity to follow up requirements set in the SC is one of the pervasive problems that our literature review and empirical findings identifies (Haver et al., 2021, p.36). Controlling and conducting frequent audits of all suppliers is demanding and difficult, if not impossible, due to extensive SC`s. Following up the requirements set in the SC demands a significant number of resources. Interviewees pointed out that this process would be too resource intensive, following up on cyber security down the entire SC. Most of the interviewees state that they do not have the resources to handle audits as efficiently as they want. Increased capacity might result in improved procurement due to detailed evaluations in advance and enabling the ability to conduct more frequent audits. However, we see that there are variations in sizes of power companies. Enhancing the capacity by hiring in-house cyber security expertise may be significantly resource demanding for certain power companies.

5.4 Cyber Security Requirements and Measures

Countries like Germany and Turkey, require suppliers in the power sector to be certified in line with international standards such as ISO 27001 and ISO 27002 on information security management systems or similar (Haver et al., 2021, p.29). In Norway, these standards are not mandatory for suppliers, although they do count positively toward procurement if they have certificates. Most participants agreed that a certified supplier will be more attractive. Based on NVE's guidelines, some power companies have included certification in their ICT checklists. However, certifications might create a false sense of security. Having certifications indicates that a variety of factors have been considered, but there are no audits confirming that the tasks are carried out in line with what has been stated.

Since power companies want to reduce costs on electrical components, software, and firmware, SC`s is becoming increasingly globalized (Liang et al., 2018, p.45). External providers are increasingly being used to perform ICT-related services, particularly in low-cost countries (Departementene, 2019, p.6). An insignificant amount of interviewees mentioned that outsourcing to low-cost countries is a cost reduction measure which is applied. Geographic location is essential to our participants. However, other informants state that they are not looking specifically for these requirements, but rather want to know if the data is stored in a sensible location. The majority of respondents said they have data storage obligations within EU, EØS, and NATO nations. This might become an issue as business values and company structures are branching across national borders, resulting in more complex SC`s which complicates the ability to have a security overview (NSM, 2020, p.26). Companies that use supplies have stringent requirements, particularly for crucial systems that influence the ability to have light in the bulb. These suppliers cannot come from countries with whom Norway has no security policy cooperation.

Private law contracts govern security between suppliers and customers, as well as between suppliers and subcontractors (Haver et al., 2021, p.6). These extensive contracts contain cyber security requirements which are sent back and forth between power companies and suppliers. The cyber security requirements that are defined in these contracts rely on internal competence within each power company, in addition to similar competence possessed by the supplier. Disparities in cyber security expertise between these links could lead to misunderstandings, resulting in extensive resource needs. This might cause both parties to be frustrated, take up unnecessary time, and result in higher expenses.

5.5 Practical Contributions

The report provides insight into current challenges the Norwegian power sector faces related to cyber security in the procurement of third-party suppliers. Additionally, we identify how the management within the power sector can make better decisions in the procurement of third-party suppliers. These findings contribute to develop an extensive awareness of the challenges related to cyber security in procurement of third-party suppliers within the Norwegian power sector, which can be a step towards a safer SC. Our study identifies issues related to lack of competence, which makes it demanding to define requirements to procurement. Low capacity complicates the process of following-up the SC and conducting frequent audits. Immature suppliers introduce new services resulting from digitalization which cause vulnerabilities in the increasingly digitalized SC. Additionally, the empirical findings have highlighted that cyber security should be included earlier in the procurements of third-party suppliers, which contribute towards an overall more secure SC.

5.6 Further Research

Based on our conclusions, researchers should consider identifying the specific competence needed to develop improved cyber security expertise, aimed at defining cyber security requirements towards procurements. Subsequently, develop a cyber security training program which intends to enhance employees within the Norwegian power sector`s threat understanding and cyber security competence. It could be considered to research the need for standardized cyber security requirements, which all companies within the Norwegian power sector could apply in their procurement of any third-party supplier. If the research indicates a need for these kinds of standardized cyber security requirements, the development of easy-to-understand requirements which do not require expert knowledge to be understood should arise.

5.7 Limitations

This section presents the variety of limitations that have been encountered, as well as how they may have impacted the project. The chapter includes reflections related to having a broad problem statement, inadequate sample size in addition to time constraints.

5.7.1 Broad Problem Statement

As our thesis focuses on both IT and OT systems, our data collection process has provided valuable insight into the differences and variety of challenges in each system. However, including both systems has potentially made the study more general. By selecting one of them could potentially increase the usefulness of our research. Additionally, the research which has been conducted includes a variety of segments from the Norwegian power sector, including production, support system, TSO, and DSO. The report provides research samples from each of the different segments which gives a holistic view of the entire sector. However, focusing on a single segment would narrow our research considerably, simplifying the process of conducting further research for power companies related to the specified segment.

5.7.2 Inadequate Sample Size

Saturation was encountered during our data collection process, which initiated the time that was selected to end the data collection process. Conducting more interviews could enrich the study, making it possible to further develop the interview guide to acquire more specific answers and details. However, time constraints required an even distribution of resources throughout the project timeframe. As our study has aimed to provide insight into procurement challenges in the Norwegian power sector by conducting qualitative research, statistical generalizations were absent.

5.7.3 Time Constraints

The project time frame has required a distribution of our time to the various parts of the thesis. Acquiring interview subjects was one of the most time-consuming processes which required a significant amount of time. Additionally, several hours that were put into this process were lost since multiple potential interviewees did not answer our request of participating in the research project. Throughout the report, both project members have worked in the same section, which has not been the most time efficient approach. However, feedback that has been received regularly indicated that the quality originating from this work method produces high quality content. This has eliminated the need to re-write sections of the report multiple times, which can be significantly demanding and time consuming.

6 CONCLUSION

This thesis has aimed to identify how digitalization has changed the procurement of third-party suppliers of IT and OT, focusing on cyber security, in the Norwegian power sector. Based on our study, it can be concluded that current procurements of third-party suppliers in the Norwegian power sector is challenging. Additionally, there are measures which can be applied in order to make better decisions with procurement of third-party suppliers. The results indicate that there is a need for more cyber security competence within the Norwegian power sector, enabling better and safer procurements. Our research clearly illustrates the need for enhanced capacity related to following up cyber security in the SC and conducting audits within the Norwegian power sector, but also raises the question of whether this is practically feasible for all companies in this sector. Our empirical findings differ from our literature findings regarding power companies which are too small to make cyber security requirements towards larger suppliers. Additionally, our study highlights the issue of not including cyber security earlier in the procurement.

Companies within the Norwegian power sector should consider applying competence enhancing measures related to cyber security and enlarge in-house cyber security capacity. These measures may result in more secure procurements and reduce the likelihood of experiencing successful cyber-attacks against the SC. Increased competence and capacity could contribute with defining improved cyber security requirements for the procurement and more capacity to conduct audits. Our research indicates that SC`s will further become more interconnected and globalized over national borders, affected by digitalization, increasing the need for enhanced cyber security competence and capacity.

REFERENCES

Achilles. (2019). Transparente leverandørkjeder, ansvarlig sourcing og ansvarlighet. Retrieved from: https://www.achilles.com/no/industry-insights/transparente-leverandorkjeder-ansvarlig-sourcing-og-ansvarlighet/

Agee, J. (2009). Developing qualitative research questions: A reflective process. *International journal of qualitative studies in education*, 22(4), 431-447. https://doi.org/10.1080/09518390902736512

Amaratunga, D., Baldry, D., Sarshar, M., & Newton, R. (2002). Quantitative and qualitative research in the built environment: application of "mixed" research approach. *Work study*, 17-31. https://doi.org/10.1108/00438020210415488

Azam, N. (2017). Informasjonssikkerhetstilstanden i energiforsyningen, 74, 1-29. Retrieved from: https://publikasjoner.nve.no/rapport/2017/rapport2017_74.pdf

Barriball, K. L., & While, A. (1994). Collecting data using a semi-structured interview: a discussion paper. *Journal of Advanced Nursing-Institutional Subscription*, 19(2), 328-335. https://doi.org/10.1111/j.1365-2648.1994.tb01088.x

Cassotta, S., & Sidortsov, R. (2019). Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North. *Energy Research & Social Science*, 51, 129-133. https://doi.org/10.1016/j.erss.2019.01.003

Departementene. (2019). Nasjonal strategi for digital sikkerhet. Retrieved from: https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/nasjonal-strategi-for-digital-sikkerhet.pdf

DiCicco-Bloom, B., & Crabtree, B. F. (2006). The qualitative research interview. *Medical education*, 40(4), 314-321. https://doi.org/10.1111/j.1365-2929.2006.02418.x

Emily, H., Mondher, F., & Imed, B. (2015). The shape of digital transformation: a systematic literature review. *MCIS 2015 proceedings*, 10, 431-443. Retrieved from: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1038&context=mcis2015#page=438

Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2019). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, 223-240. Retrieved from: https://www.emerald.com/insight/content/doi/10.1108/SCM-10-20180357/full/html?casa_token=lqXZG0mDlDkAAAAA:gPATHoGItpwx0I7W5qeLh4MuCM1N64_dqTOB9R0pHNylggiscyPRonPg-gIexlxYgAeOqxHrgTiZVRvVutGoszE6JVnqGdtbxH1vO2PZma4CpmPlRsvU

Hafiz, K. (2008). Case study example. *The qualitative report*, 13(4). 544-559. Retrieved from: https://www.academia.edu/18565714/Case_study_ecmple?bulkDownload=thisPaper-topRelated-sameAuthor-citingThis-citedByThis-secondOrderCitations&from=cover_page

Hagen, J., Houmb, S. H., Smevold, L. E., Kalstad, N., & Nygård, A. R. (2020). Utvikling av cybersikkerhetskompetanse for kraftbransjen. 3-18. Retrieved from: https://www2.deloitte.fr/formulaire/pdf/Deloitte_managing-cyber-risk-2020.pdf

Haver, K., Valdal, A.K, Vernholt, T. & Wiencke, H.S. (2021). Norges vassdrags- og energidirektorat (NVE), Veikart for NVEs oppfølging av IKT-sikkerhet i leverandørkjeden, 1-52. Retrieved from: https://proactima.com/2022/01/proactima-bistar-nve-med-veikart-for-a-styrke-ikt-sikkerheten-i-kraftforsyningen/

Harrell, M. C., & Bradley, M. A. (2009). Data collection methods. Semi-structured interviews and focus groups. *Rand National Defense Research Inst santa monica ca*. Retrieved from: https://apps.dtic.mil/sti/pdfs/ADA512853.pdf

Heinbockel, W. J., Laderman, E. R., & Serrao, G. J. (2017). Supply Chain Attacks and Resiliency Mitigations. *The MITRE Corporation*, 1-30. Retrieved from: https://www.mitre.org/sites/default/files/pdf/PR_18-0854.pdf

Hennink, M. M., Hutter, I., & Bailey, A. (2020). Qualitative research methods. *London: SAGE Publications Ltd*, 10. Retrieved from: https://www.worldcat.org/title/qualitative-research-methods/oclc/1153392954?referer=di&ht=edition

Horne, M. (2019). Photos of the 2003 Blackout: When the Northeast Went Dark. Retrieved from: https://www.history.com/news/2003-blackout-new-york-city-photos

Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). Systematic methodological review: developing a framework for a qualitative semi-structured interview guide. *Journal of advanced nursing, 72*(12), 2954-2965. https://doi.org/10.1111/jan.13031

Khasawneh, M, H,. (2009). An exploration of consumer response towards sponsored search advertising (SSA) from a consumer behavior perspective, 67. Retrieved from: https://www.researchgate.net/publication/267954145_AN_EXPLORATION_OF_CONSUMER_RESPONSE_TOWARDS_SPONSORED_SEARCH_ADVERTISING_SSA_FROM_A_CONSUMER_BEHAVIOUR_PERSPECTIVE

Kirkebø, E., & Ljøsne, M. (2018). IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen. *Technical Report 90, Norges vassdrags-og energidirektorat (NVE)*, 2018. (In Norwegian). Retrieved from: https://publikasjoner.nve.no/rapport/2018/rapport2018_90.pdf

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University*, 33(2004), 1-26. Retrieved from: http://www.elizabete.com.br/rs/Tutorial_IHC_2012_files/Conceitos_RevisaoSistematica_kitchenham_2004.pdf

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering. Vol 2.3 EBSE Technical Report*. EBSE-2007-01, Software Engineering Group, School of Computer Science and Mathematics, Keele University, Keele, UK. Retrieved from: https://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=%EF%A3%BF?doi=10.1.1.117.471&rep=rep1&type=pdf

Kshetri, N., & Voas, J. (2019). Supply chain trust. IT Professional, 21(2), 6-10. 10.1109/MITP.2019.2895423

Kumar, V. S., Prasad, J., & Samikannu, R. A. (2018). A critical review of cyber security and cyber terrorism – threats to critical infrastructure in the energy sector. *Int. J. Critical Infrastructures, Vol. 14, No. 2.* 101-119. https://www.doi.org/10.1504/IJCIS.2018.091932

Lamba, A. (2018). *Protecting "Cybersecurity & Resiliency" of Nation's Critical Infrastructure Energy, Oil & Gas (Vol. 10, Issue 12), 76865-76876.* Retrieved from: https://dx.doi.org/10.2139/ssrn.3535434

Liang, X., Shetty, S., Tosh, D., Ji, Y., & Li, D. (2018). Towards a reliable and accountable cyber supply chain in energy delivery system using blockchain. *In International Conference on Security and Privacy in Communication Systems*, 43-62. Retrieved from: https://link.springer.com/chapter/10.1007/978-3-030-01704-0_3

Livingston, S., Sanborn, S., Slaughter, A., & Zonneveld, P. (2018). Managing cyber risk in the electric power sector. Deloitte. As of, 1-17. Retrieved from: https://www2.deloitte.fr/formulaire/pdf/Deloitte_managing-cyber-risk-2020.pdf

Miles, M. B., & Huberman, A. M. (1994). Qualitative data analysis: An expanded sourcebook. Sage, 1-338. Retrieved from: https://vivauniversity.files.wordpress.com/2013/11/milesandhuberman1994.pdf

National Science Foundation (NSF). (1997). Analyzing Qualitative Data. Retrieved from: https://www.nsf.gov/pubs/1997/nsf97153/chap_4.htm

Njie, B., & Asimiran, S. (2014). Case study as a choice in qualitative methodology. *Journal of Research & Method in Education*, 4(3), 35-40. Retrieved from: https://apprendre.auf.org/wp-content/opera/13-BF-References-et-biblio-RPT-2014/Case%20Study%20as%20a%20Choice%20in%20Qualitative%20Methodology.pdf

NSM. (2020). Helhetlig digitalt risikobilde 2020. Retrieved from: https://nsm.no/regelverk-og-hjelp/rapporter/helhetlig-digitalt-risikobilde-2020/det-digitale-risikobildet/

NSM. (2021). Nasjonalt digitalt risikobilde 2021. Retrieved from: https://nsm.no/getfile.php/137495-1635323653/Filer/Dokumenter/Rapporter/NSM_IKT-risikobilde_2021_ny_B_enkeltside.pdf

Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. *Communications of the Association for Information Systems*, 37, 879-910. https://doi.org/10.17705/1CAIS.03743

Paré, G., Trudel, M.C., Jaana, M. & Kitsiou, S. (2015). Synthesizing Information Systems Knowledge: A Typology of Literature Reviews. Information & Management 52:183–99. https://doi.org/10.1016/j.im.2014.08.008

Queirós, A., Faria, D., & Almeida, F. (2017). Strengths and limitations of qualitative and quantitative research methods. *European Journal of Education Studies,* 369-387. Retrieved from: https://zenodo.org/record/887089#.YjxX_ufMJD8

Riksrevisjonen. (2021). *Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen Dokument 3:7 (2020–2021).* Retrieved from: https://www.riksrevisjonen.no/globalassets/rapporter/no-2020-2021/nves-arbeid-med-ikt-sikkerhet-i-kraftforsyningen.pdf

Rowley, J. (2012). Conducting research interviews. Management research review, 260-271. https://doi.org/10.1108/01409171211210154

Salvi, A., Spagnoletti, P., & Noori, N. S. (2021). Cyber-resilience of Critical Cyber Infrastructures: integrating digital twins in the electric power ecosystem. C*omputers & Security*, 102507. https://doi.org/10.1016/j.cose.2021.102507

Saunders, B., Sim, J., Kingstone, T., Baker, S., Waterfield, J., Bartlam, B., Burroughs, H., & Jinks, C. (2018). Saturation in qualitative research: exploring its conceptualization and operationalization. *Quality & quantity*, 52(4), 1893–1907. https://doi.org/10.1007/s11135-017-0574-8

Simon, J., & Omar, A. (2020). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research*, 282(1), 161-171. https://doi.org/10.1016/j.ejor.2019.09.017

Thomas, D. R. (2006). A general inductive approach for analyzing qualitative evaluation data. *American journal of evaluation*, 27(2), 237-246. https://doi.org/10.1177/1098214005283748

Universitetet i Oslo (UiO). (2020, 7. Oktober). NVivo. Retrieved from: https://www.uio.no/tjenester/it/forskning/datafangst-og-analyse/nvivo/mer-om.html

University of South Florida. (2021). Develop a Systematic Review Protocol. Retrieved from: https://guides.lib.usf.edu/c.php?g=848629&p=607376

Venkatachary, S. K., Prasad, J., & Samikannu, R. (2017). Economic impacts of cyber security in energy sector: A review. *International Journal of Energy Economics and Policy*, 7(5), 250-261. Retrieved from: https://www.proquest.com/docview/2610088010?pq-origsite=gscholar&fromopenview=true6

Vozikis, D., Darra, E., Kuusk, T., Kavallieros, D., Reintam, A., & Bellekens, X. (2020). On the importance of cyber-security training for multi-vector energy distribution system operators. *In Proceedings of the 15th International Conference on Availability, Reliability and Security*, 1-6. https://doi.org/10.1145/3407023.3409313

Xiao, Y., & Watson, M. (2019). Guidance on Conducting a Systematic Literature Review. *Journal of Planning Education and Research,* 39(1), 93–112. https://doi.org/10.1177/0739456X17723971

Yeboah-Ofori, A., & Islam, S. (2019). Cyber security threat modeling for supply chain organizational environments. *Future internet*, 11(3), 63. https://doi.org/10.3390/fi11030063

APPENDIX

Appendix A. Review Protocol

Team Information

Researchers	Brage Fagstad & Knut Andreas Aas
Date	19.01.2022
Institution	University of Agder, Kristiansand

Background

The background for the review protocol is to investigate the role of cyber security in digitalization focusing on the Norwegian power sector. Our objective is to obtain knowledge related to the following problem domain:

> *"Has digitalization affected cyber security in the Norwegian power sector and what cyber security challenges this sector is facing?"*

Note: This is our initial problem statement, which most likely evolves after more knowledge is acquired.

Objective

Our objective is to gain greater knowledge of the various aspects of our problem domain. This is to be able to acquire a knowledge foundation which identifies research gaps within our focus area and develop research questions. These will further be investigated through quantitative and/or qualitative research approaches. This intends to enhance the integrity of the report, highlighting a problem domain that most likely needs more research.

Search Strategy

Electronic Databases
Google Scholar ScienceDirect Springer
Keywords
Critical infrastructure Cyber Security Digitalization/Digitalization

Energy sector Norwegian Power Sector Supplier Supply chain attack Supply chain
Year of Publication
Critical infrastructure: Not published later than 2015 Cyber security: Not published later than 2015 Digitalization: Not published later than 2010 Supply chain: Not published later than 2016
Stakeholders
Netsecurity AS will function as our stakeholders throughout the project. They have provided high quality research materials which will be used to investigate our problem domain. The material that they have provided is: Hand-delivered: 1. Riksrevisjonen. Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen. 2. NVE. Hagen, J., Houmb, S. H., Smevold, L. E., Kalstad, N., & Nygård, A. R. (NVE). Utvikling av cybersikkerhetskompetanse for kraftbransjen. 3. NSM. Helhetlig digitalt risikobilde 2021.
Reference Searches
Backward searching will be performed to supplement knowledge to the project.

Eligibility Criteria

Inclusion Criteria	Exclusion Criteria
Title: Relevance to problem domain	Title: Not related to problem domain
Abstract: Includes a simplified overview of what the report/article contains	Abstract: Poorly written which make it difficult to understand what the report/article contains
Full text: Content of the report/article is related to the topic	Full text: Content of the report/article is irrelevant
Peer-reviewed: Only the newest journals	
Publication language: English or Norwegian	Publication language: Not in English or Norwegian
Setting: Related to Power sector in Norway	Setting: Not related to our problem domain

Appendix B. Literature Exclusion Criteria

Date of search	Author and Title	Title exlusion	Abstract exclusion	Full-text exclusion	Comment
20.01.2022	Kumar, A.v., Pandey, k.k., & Punia, D.k. Cyber security threats in the power sector: Need for a domain specific regulatory framework in India	✓	✗	✗	Setting - out of scope, cannot be related to the Norwegian power sector.
21.01.2022	Riksrevisjonen. Riksrevisjonens undersøkelse av digitalisering i statlige virksomheter	✓	✓	✗	Setting - out of scope. Irrelevant to our research questions.
21.01.2022	PST. PST National Threat Assessment 2021	✓	✗	✗	Setting - out of scope, not including the power sector.
21.01.2022	Park, C., & Kim, M. Characteristics Influencing Digital Technology Choice in Digitalization Projects of Energy Industry	✓	✗	✗	Setting - out of scope, cannot be related to the Norwegian power sector.
21.01.2022	Carlson, J. Cybersecurity Power Industry Locks Down	✓	✓	✗	Setting - out of scope. Irrelevant to our research questions.
21.01.2022	IKT-Norges. bærekraftskartlegging: Datasikkerhet aller viktigst	✓	✗	✗	Setting - out of scope, does not mention the power sector and digitalization
21.01.2022	Brown, M., Woodhouse, S. & Sioshansi, F. Consumer, Prosumer, Prosumer: How Service Innovations will Disrupt the utility business model	✓	✗	✗	Setting - out of scope. Irrelevant to our research questions.
24.01.2022	Silvestre, M. L., Favuzza, S., Sanseverino, E. R., & Zizzo, G. How Decarbonization, Digitalization and	✓	✗	✗	Setting - out of scope. Irrelevant to our research questions.

	Decentralization are changing key power infrastructures				
24.01.2022	Gribanov, Y., & Shatrov, A. Modular digitalization of the energy sector	✓	✓	✖	Setting - out of scope, cannot be related to the Norwegian power sector.
24.01.2022	Dorokhova, M. The digitalization of energy systems: towards higher energy efficiency	✓	✖	✖	Setting - out of scope. Irrelevant to our research questions.
24.01.2022	Zinaman, O., Miller, M., & Bazilian, M. The Evolving Role of the PowerSector Regulator	✓	✖	✖	Setting - out of scope, cannot be related to the Norwegian power sector.
24.01.2022	Sachdeva, M. L., & Sodha, N. S. Cyber security disaster management for power sector	✓	✖	✖	Setting - out of scope, cannot be related to the Norwegian power sector.
24.01.2022	Fuentes, S., Villafafila-Robles, R., Olivella-Rosell, P., Rull-Duran, J., & Galceran-Arellano, S. Transition to a greener Power Sector: Four different scopes on energy security	✓	✓	✖	Setting - out of scope, cannot be related to the Norwegian power sector.
24.01.2022	Zhang, Z. Cybersecurity policy for the electricity sector: the first step to protecting our critical infrastructure from cyber threats	✓	✖	✖	Setting - out of scope. Irrelevant to our research questions.
24.01.2022	Leszczyna, R. A review of standards with cybersecurity requirements for smart grid	✓	✖	✖	Setting - out of scope. Irrelevant to our research questions.
24.01.2022	Kaster, P. and Sen, P.K. Power Grid cyber	✓	✓	✖	Setting - out of scope. Irrelevant to

	security: Challenges and impacts,"				our research questions.
24.01.2022	Venkatachary, S. K., Prasad, J., & Samikannu, R. Cybersecurity and cyber terrorism - in energy sector – a review	✓	✓	✖	Setting - out of scope, cannot be related to the Norwegian power sector.
24.01.2022	Smith, D. C. Enhancing cybersecurity in the energy sector: a critical priority	✓	✖	✖	Setting - out of scope. Irrelevant to our research questions.
24.01.2022	Venkatachary, S. K., Prasad, J., Samikannu, R., Alagappan, A., & Andrews, L. J. B. Cybersecurity infrastructure challenges in IoT based virtual power plants	✓	✖	✖	Setting - out of scope. Irrelevant to our research questions.
24.01.2022	Parn, E.A & Edwards, D. Cyber threats confronting the digital built environment	✓	✖	✖	Setting - out of scope. Irrelevant to our research questions.
24.01.2022	Barichella, A. Cyber-security in the Energy Sector: a Comparative Analysis between Europe and the United States	✓	✓	✖	Setting - out of scope. Irrelevant to our research questions.
24.01.2022	Daria, G., & Massel, A. Intelligent System for Risk Identification of Cybersecurity Violations in Energy Facility	✓	✖	✖	Setting - out of scope. Irrelevant to our research questions.
24.01.2022	Sun, C.C., Hahn, A. & Liu, C.C. Cyber security of a power grid: State-of-the-art.	✓	✖	✖	Setting - out of scope. Irrelevant to our research questions.
24.01.2022	Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, M. K. A Review of Cybersecurity Incidents in the Water Sector	✓	✓	✖	Setting - out of scope. Irrelevant to our research questions.

24.01.2022	Dagoumas, A. Assessing the Impact of Cybersecurity Attacks on Power Systems	✓	✖	✖	Setting - out of scope. Irrelevant to our research questions.
24.01.2022	Yohanandhan, R. V., Elavarasan, R. M., Manoharan, P., & Mihet-Popa, L. Cyber-Physical Power System (CPPS): A Review on Modeling, Simulation, and Analysis With Cyber Security Applications	✓	✖	✖	Setting - out of scope, cannot be related to the Norwegian power sector.
24.01.2022	Alekseev, A. N. Digitalization of the Russian energy sector: State-of-the-art and potential for future research	✓	✖	✖	Setting - out of scope, cannot be related to the Norwegian power sector.
24.01.2022	Gluschke, G., Casin, M. H., & Macori, M. Cyber security policies and critical infrastructure protection	✓	✓	✖	Setting - out of scope, cannot be related to the Norwegian power sector.
24.01.2022	Rajavuori, M., & Huhta, K. Investment screening: Implications for the energy sector and energy security	✓	✖	✖	Setting - out of scope. Irrelevant to our research questions.
24.01.2022	Hossein Motlagh, N., Mohammadrezaei, M., Hunt, J., & Zakeri, B. Internet of Things (IoT) and the Energy Sector	✓	✖	✖	Setting - out of scope. Irrelevant to our research questions.
24.01.2022	Twohig, S. Cyber Security Management Model for Critical Infrastructure	✓	✓	✖	Setting - out of scope, cannot be related to the Norwegian power sector.
24.01.2022	Le, T. D., Anwar, A., Loke, S. W., Beuran, R., & Tan, Y. GridAttackSim: A Cyber Attack Simulation Framework for Smart Grids	✓	✓	✖	Setting - out of scope, cannot be related to the Norwegian power sector.

24.01.2022	Canaan, B., Colicchio, B., & Ould Abdeslam, D. Microgrid Cyber-Security: Review and Challenges toward Resilience	✓	✖	✖	Setting - out of scope, cannot be related to the Norwegian power sector.
24.01.2022	Kelemen, M., Szabo, S., Vajdová, I., Bekesiene, S., & Hošková-Mayerová, Š. Cybersecurity in the Context of Criminal Law Protection of the State Security and Sectors of Critical Infrastructure	✓	✓	✖	Setting - out of scope. Irrelevant to our research questions.
15.02.2022	Overland, I. EU Climate and Energy Policy: New Challenges for Old Energy Suppliers	✓	✖	✖	Setting - out of scope. Irrelevant to our research questions.
15.02.2022	Urpelainen, J & Yang, J. Global patterns of power sector reform, 1982–2013	✓	✖	✖	Setting - out of scope. Irrelevant to our research questions.
16.02.2022	Duncan, R. How to secure your supply chain	✓	✖	✖	Setting - out of scope. Irrelevant to our research questions.
16.02.2022	Schneier, B. Every part of the supply chain can be attacked.	✓	✖	✖	Setting - out of scope. Irrelevant to our research questions.
16.02.2022	Ayuninggati, T., Harahap, E. P., & Junior, R. Supply Chain Management, Certificate Management at the Transportation Layer Security in Charge of Security.	✓	✖	✖	Setting - out of scope. Irrelevant to our research questions.
17.02.2022	Unsal, D. B., Ustun, T. S., Hussain, S. M., & Onen, A. Enhancing cybersecurity in smart grids: false data injection and its mitigation. Energies	✓	✓	✖	Setting - out of scope. Irrelevant to our research questions.

Appendix C. Literature Inclusion Criteria

Date of search	Author and Title	Synthesis Type(s)	Summary
21.01.2022	Riksrevisjonen. Riksrevisjonens undersøkelse av NVEs arbeid med IKT-sikkerhet i kraftforsyningen.	Qualitative & Quantitative	Report related to NVE by The Norwegian Office of the Auditor General's, investigating NVE's work with IT security in the Norwegian power sector.
21.01.2022	Livingston, S., Sanborn, S., Slaughter, A., & Zonneveld, P. (Deloitte). Managing cyber risk in the electric power sector.	Theoretical Report	Deloitte writes about threats in the Power sector and what vulnerabilities the sector may face. They are also examining the steps that power companies can take regarding cyber risks.
21.01.2022	Hagen, J., Houmb, S. H., Smevold, L. E., Kalstad, N., & Nygård, A. R. (NVE). Utvikling av cybersikkerhetskompetanse for kraftbransjen.	Theoretical Report	NVE report related to the development of cyber security competence within the Norwegian power sector.
21.01.2022	Kirkebø, E. & Ljøsne, M. (NVE). IKT-sikkerhet ved anskaffelser og tjenesteutsetting i energibransjen.	Qualitative	NVE writes about digitalisation in the power sector and their challenges when it comes to cyber security. NVE also writes about the importance of cyber security.
21.01.2022	Azam, N. (NVE). Informasjonssikkerhetstilstanden i energiforsyningen.	Quantitative	The NVE report focuses on the information system security within the Norwegian energy supply.
21.01.2022	NSM. Helhetlig digitalt risikobilde 2020.	Theoretical Report	NSM addresses the risk picture of 2020 where they talk about typical attacks that are carried out due to digitalisation.

21.01.2022	Departementene. Nasjonal strategi for digital sikkerhet.	Theoretical Report	The Norwegian departments report focus on digitalisation, cyber security in critical societal functions and in Norwegian infrastructure.
21.01.2022	Lamba, A. Protecting “Cybersecurity & Resiliency” of Nation`s Critical Infrastructure Energy, Oil & Gas.	Qualitative	The research article provides information regarding protecting cyber security and resiliency of the nation's critical infrastructure energy, oil and gas.
21.01.2022	Venkatachary, Prasad & Samikannu. Economic Impacts of Cyber Security in Energy Sector: A Review	Quantitative	The journal contains information regarding the impacts of cyber security in the energy sector globally.
21.01.2022	NVE. Informasjonssikkerhetstilstanden i energiforsyningen 2017	Quantitative	NVE writes in a 2017 journal that digitalisation has led to the power industry being more exposed to digital attacks than before. The report provides a picture of the security situation in the energy sector.
21.01.2022	Vozikis, D., Darra, E., Kuusk, T., Kavallieros, D., Reintam, A. & Bellekens, X. On the Importance of Cyber-Security Training for Multi-Vector Energy Distribution System Operators.	Theoretical Report	The research paper consists of the importance of cyber security training in multi vector energy distribution system operators.
21.01.2022	Cassotta, S. & Sidortsov, S. Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North	Qualitative	The article includes cyber threats to critical infrastructure in the Nordic countries and approaches to protection
21.01.2022	NSM. Nasjonalt digitalt risikobilde 2021	Theoretical Report	NSM addresses the risk picture of 2021 where they talk about typical attacks that are

			carried out due to digitalisation.
24.01.2022	Salvi, A., Spagnoletti, P. & Noori, N.S. Cyber-resilience of Critical Cyber Infrastructures: Integrating digital twins in the electric power ecosystem	Research article	The article includes upon cyber-resilience of critical cyber infrastructures. Additionally, the integration of digital twins to the electric power ecosystem.
24.01.2022	Campbell, R. J. Cybersecurity issues for the bulk power system.	Theoretical Report	The report includes vulnerabilities in the power sector, and how critical this sector is if anything happens
24.01.2022	Kumar, V. S., Prasad, J., & Samikannu, R. A critical review of cyber security and cyber terrorism – threats to critical infrastructure in the energy sector	Research article	The article contains a critical point of view on the security of the power sector and the what threats critical infrastructure is facing
24.01.2022	Bailey, T., Maruyama, A., & Wallance, D. The Importance of Strong Cyber Security industrial Environments	Theoretical Report	This report is about the reasons why the power sector has poor cyber security
24.01.2022	Horne, M. Photos of the 2003 Blackout: When the Northeast Went Dark.	Example papers	Example of a blackout in the northeast and the following consequences.
17.02.2022	Yeboah-Ofori, A., & Islam, S. Cyber security threat modeling for supply chain organizational environments.	Research article	The article is about understanding the supply chain and which threat it brings.
17.02.2022	Simon, J., & Omar, A. Cybersecurity investments in the supply chain: Coordination and a strategic attacker.	Research article	The article is about challenges to the supply chain and investment in the supplier.
17.02.2022	Liang, X., Shetty, S., Tosh, D., Ji, Y., & Li, D. Towards a reliable and accountable cyber supply chain in energy delivery systems using blockchain.	Research article	The article presents how supply chains in the energy sector can be reliable with the help of blockchain.
17.02.2022	Kshetri, N. & Voas, J. Supply Chain Trust	Research article	The article is about supply chain trust. Including vulnerabilities and

			challenges, service providers and customers.
17.02.2022	Heinbockel, W. J., Laderman, E.R., Serrao, G.J. Supply Chain Attacks and Resiliency Mitigations	Technical report	The report provides information regarding supply chain attacks and resiliency mitigations and recommends different techniques for cyber resiliency.
17.02.2022	Ghadge, A., Weiß, M., Caldwell, N.D., Wilding, R. Managing cyber risk in supply chains: a review and research agenda	Research article	The article provides insights in the process of managing cyber risk in the supply chain.
03.03.2022	Haver, K., Valdal, A.K, Vernholt, T. & Wiencke, H.S. Norges vassdrags- og energidirektorat (NVE), Veikart for NVEs oppfølging av IKT-sikkerhet i leverandørkjeden	Qualitative	The article provides insights in the decision-making process in the supply chain as well as shortcomings with this process today

Appendix D. Interview Guide

Initial questions:

1. What role do you have in your organization?
2. How long have you worked in the company?
3. Do you have experience with IT security?
4. What type of IT threats and challenges do you face today?
5. Do you rely on third-party suppliers to provide your services?

   - If yes, how?

The selection process:

6. Which ICT security challenges are there in the process of selecting third-party suppliers in the Norwegian power sector?
7. How has digitalization affected the process of selecting third-party suppliers of IT and OT systems/services?
8. How is ICT security being considered before the selection of third-party suppliers of IT and OT systems/services?
9. What kind of ICT security considerations are made and applied in advance of a potential collaboration with new third-party suppliers? (E.g., risk assessments)?
10. How can you make a better decision with the procurement of third-party suppliers?
11. Which ICT issues are considered in the selection process of third-party suppliers of IT and OT systems/services?
12. How is ICT security being regulated through contracts and agreements down in the supply chain?
13. Do you have insight into how third-party suppliers are security their system, product and/or services?
14. Do you have requirements or expectations related to the third-party supplier that follow international security standards (E.g., ISO 27001/27002)?

Operating third-party interactions:

15. How do you follow up the ICT security down the supply chain?
16. What are the consequences if a third-party IT / OT supplier goes down?
17. What do you do to have redundancy in your systems/services if a third-party supplier is shut down?

- Do you have an action plan if situations such as a shutdown occur?

Final question:

18. How do you rate your maturity in IT security (from 1-5)?
19. Do you know anyone that potentially could be a resource in our research that we should contact?

Appendix E. Consent Form

Vil du delta i forskningsprosjektet "The Role of Cyber Security in Digitalization focusing on the Norwegian Power Sector"

Dette er en forespørsel til deg om å delta i et forskningsprosjekt hvor formålet er å identifisere om digitalisering har økt sårbarheter i den Norske kraftsektorens/energisektorens leverandørkjeder. I dette skrivet gir vi deg informasjon om målene for prosjektet og hva deltakelse vil innebære for deg.

Formål

Prosjektets formål er å identifisere hvordan digitalisering har påvirket cybersikkerheten innenfor den Norske kraftsektoren. Vårt mål er å identifisere hvilke utfordringer bransjen står overfor relatert til tredjepartsleverandører av IT og OT tjenester, og hvilken påvirkning digitaliseringen har hatt på anskaffelsen av nye leverandører.

Oppgaven er en masteroppgave innenfor Cybersikkerhet, ved Universitetet i Agder. Dette skal være en forskningsrapport som vi vil svare på følgende forskningsspørsmål:

- How has digitalization affected the power sector management's decision making for acquiring third-party suppliers?
- How can the management in the Norwegian power sector make better decisions in the procurement of third-party suppliers?

Forskningsrapportens periode strekker seg fra 10. Januar 2022 til 3. Juni 2022. Opplysningene skal kun brukes i akademisk sammenheng, for å best mulig kunne besvare forskningsspørsmål og problemstillingen.

Hvem er ansvarlig for forskningsprosjektet?

Universitetet i Agder, avdeling Kristiansand er ansvarlig for prosjektet.

Hvorfor får du spørsmål om å delta?

Utvalgets populasjon er begrenset til fagpersonell som innehaver relevant kompetanse, som intensjonelt vil sikre svært høy integritet i innhentet informasjon. Utvalgskriterier er at personell som deltar i intervju har kunnskap om IKT, cybersikkerhet, leverandørkjeden og/eller innen den Norske kraftsektoren.

Hensikten med å tilegne seg opp til 20 responser er for å danne et solid faglig grunnlag for å kunne ha en svært høy grad av integritet på den innhentede informasjonen.

Hva innebærer det for deg å delta?

Deltakelse på intervju:

Dersom du velger å delta i prosjektet ved å ta del i et intervju, vil dette ta deg ca. 30 minutter. Spørsmålene vil være relatert til digitalisering, datasikkerhet og tredjepartsleverandører i den norske kraftsektoren. Vi vil også spør etter hva slags rolle du har i din representative organisasjon. Det ønskelig å gjennomføre intervjuet over nett med hensyn til effektivitet og smittevern. Dine svar fra intervjuet blir registrert elektronisk, og anonymisert.

Vi tar lydopptak/skjermopptak av intervjuet for å sikre oss mest mulig nøyaktig informasjon. Disse vil bli slettet ved endt prosjekt.

Det er frivillig å delta

Det er frivillig å delta i prosjektet. Hvis du velger å delta, kan du når som helst trekke samtykket tilbake uten å oppgi noen grunn. Alle dine personopplysninger vil da bli slettet. Det vil ikke ha noen negative konsekvenser for deg hvis du ikke vil delta eller senere velger å trekke deg.

Ditt personvern – hvordan vi oppbevarer og bruker dine opplysninger

Vi vil kun bruke opplysningene om deg til formålene vi har fortalt om i dette skrivet. Vi behandler opplysningene konfidensielt og i samsvar med personvernregelverket.

De som har tilgang ved behandlingsansvar er veiledere ved Universitetet i Agder, samt prosjektgruppen.

Tilgangskontroll er begrenset til prosjektgruppen, som til enhver tid har innsikt i at ingen uvedkommende får tilgang til personopplysninger. Enkeltpersoners navn vil ikke bli brukt i prosjektet, da denne informasjonen er irrelevant for forskningen.

Hva skjer med opplysningene dine når vi avslutter forskningsprosjektet?
Opplysningene anonymiseres når prosjektet avsluttes/oppgaven er godkjent, noe som etter planen er 3. Juni 2022. All personlig informasjon vil bli slettet etter prosjektet er ferdigstilt, og oppgaven er karaktersatt. Dette vil innebære at lydopptak/skjermopptak, intervjunotater o.l. blir fjernet.

Dine rettigheter
Så lenge du kan identifiseres i datamaterialet, har du rett til:

- Innsyn i hvilke personopplysninger som er registrert om deg, og å få utlevert en kopi av opplysningene
- Å få rettet personopplysninger om deg
- Å få slettet personopplysninger om deg,
- Å sende klage til Datatilsynet om behandlingen av dine personopplysninger.

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

På oppdrag fra Universitetet i Agder, Kristiansand har NSD – Norsk senter for forskningsdata AS vurdert at behandlingen av personopplysninger i dette prosjektet er i samsvar med personvernregelverket.

Hvor kan jeg finne ut mer?
Hvis du har spørsmål til studien, eller ønsker å benytte deg av dine rettigheter, ta kontakt med:
Student ved Universitetet i Agder. Brage Fagstad. Mail: brage.fagstad@hotmail.com
Student ved Universitetet i Agder. Knut Andreas Aas. Mail: knut-andreas97@hotmail.com
Veileder ved Universitetet i Agder. Marko Ilmari Niemimaa. Mail: marko.niemimaa@uia.no
Veileder ved Universitetet i Agder. Paolo Spagnoletti. Mail: paolo.spagnoletti@uia.no
Vårt personvernombud: Johanne Warberg Lavold. Mail: personvernombud@uia.on

Hvis du har spørsmål knyttet til NSD sin vurdering av prosjektet, kan du ta kontakt med:
NSD – Norsk senter for forskningsdata AS på e-post
(personverntjenester@nsd.no) eller på telefon: 55 58 21 17.

Med vennlig hilsen
Brage Fagstad & Knut Andreas Aas

Samtykkeerklæring

Jeg har mottatt og forstått informasjon om prosjektet *The Role of Cyber Security in Digitalization focusing on the Norwegian Power Sector*, og har fått anledning til å stille spørsmål.

Jeg samtykker til:

- å delta i intervju
- taleopptak av intervjuet (via UiO Nettskjema Diktafon)
- at mine opplysninger behandles frem til prosjektet er avsluttet

----

(Signert av prosjektdeltaker, dato)