jamk.fi

Cyber Security Management in Energy Supply

Cyber Security Roadmap for Elenia

Elina Dauchy

Master's thesis
May 2021
Technology
Degree Programme in Information and Communication Technology
Master's Degree Programme in Cyber Security

jamk.fi

Description

Author(s)	Type of publication	Date
Dauchy, Elina	Master's thesis	May 2021
		Language of publication: English
	Number of pages 141	Permission for web publication: x

Title of publication

Cyber Security Management in Energy Supply

Cyber Security Roadmap for Elenia

Degree programme

Degree Programme in Information and Communication Technology, Cyber Security

Supervisor(s)

Hautamäki Jari; Kotikoski Sampo

Assigned by

Elenia Verkko Oyj; Paananen Heikki

Abstract

Electricity distribution company Elenia is planning cyber security roadmap for the years 2023–2025. The first objective was to study the meaning of cyber security in the future by identifying the foreseeable factors affecting the energy sector in the coming years. The second aim was to evaluate the adequate level.

The methods used were mixed methods with qualitative and quantitative methods combined. The emphasis was on qualitative methods with content analysis, interview, and the Delphi method. With the Delphi method opinions of experts were collected for roadmap recommendations. Theoretical background consists of foreseeable changes of the energy sector, the actual maturity level of the energy sector, threats, trends, megatrends, and scenarios.

It was found that the requirements of the suppliers and devices are in a significant role. Instead of setting requirements only for the critical infrastructure, the requirements should also apply to suppliers and devices to address the system wide cyber security question. The consumers and consumer devices are also part of the system. It would be beneficial for the national economy to define a national level official digital authority and set clear and precise requirements for the critical infrastructure. This way the lack of cyber security resources and competence would become visible, measurable, and resolvable.

Recommendations for the key development areas for cyber security in electricity distribution are awareness management, competence management, risk management, and active management of the cyber security towards a desirable future by taking part in legislative reforms both European and national wide. The actions should also cover the partnerships.

Keywords/tags (subjects) Awareness, cyber security, cyber strategy, Delphi method, knowledge management, management, regulation, risk management, strategy

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Dauchy, Elina	Opinnäytetyö, ylempi AMK	Toukokuu 2021
		Julkaisun kieli Englanti
	Sivumäärä 141	Verkkojulkaisulupa myönnetty: x

Työn nimi

Cyber Security Management in Energy Supply

Cyber Security Roadmap for Elenia

Tutkinto-ohjelma

Degree Programme in Information and Communication Technology, Cyber Security

Työn ohjaaja(t)

Hautamäki Jari; Kotikoski Sampo

Toimeksiantaja(t)

Elenia Verkko Oyj; Paananen Heikki

Tiivistelmä

Sähkönjakeluyhtiö Elenia on toteuttamassa kyberturvallisuuden tiekarttaa vuosille 2023–2025. Tavoitteena oli tutkia kyberturvallisuuden merkitystä tulevaisuudessa tunnistamalla sähkönjakeluun keskeisesti vaikuttavat ennakoitavissa olevat toimialan muutokset. Toisena tavoitteena oli arvioida kyberturvallisuuden riittävää tasoa sähkönjakeluliiketoiminnassa.

Tutkimusmenetelmät olivat sekä laadullisia että määrällisiä painottuen laadulliseen sisällönanalyysiin, haastatteluun ja keskeisimpänä Delfoi-menetelmään, jonka avulla kerättiin asiantuntijanäkemyksiä ja mielipiteitä suositusten pohjaksi. Teoreettinen viitekehys koostuu energia-alan ennakoitavissa olevista muutoksista, nykytilan maturiteetin tarkastelusta ja uhkakuvista, trendeistä ja megatrendeistä sekä skenaarioista.

Tutkimuksessa huomattiin, että toimittajien ja laitteiden vaatimukset ovat keskeisessä asemassa ja sen sijaan, että vaatimuksia asetettaisiin vain kriittisen infrastruktuurin toimijalle, vaatimukset tulisi kohdistaa myös laitteisiin ja toimittajiin, jotta koko systeemitasoisen kokonaisuuden kyberturvallisuus olisi ratkaistu. Huomioitavaa on, että myös kuluttajat ja kuluttajaratkaisut ovat osana systeemiä. Kansantaloudellisesti ei ole kannattavaa asettaa vaatimuksia vain yrityksille vaan digitaalisen maailman virkavallan rooli olisi määriteltävä, ja asetettava selkeät vaatimukset kriittisen infrastruktuurin toimijoille. Tällä tavoin kyberturvallisuuden osaamisvaje saadaan näkyväksi, mitattavaksi ja ratkaistavaksi.

Suositukset osa-alueista, joihin sähkönjakeluliiketoiminnassa tulisi kyberturvallisuuden kehitysaskeleet kohdistaa ovat tietoisuus, osaaminen ja riskienhallinta sekä aktiivinen vaikuttaminen lainsäädäntöön ja tulevaisuuden suunnitteluun. Toimenpiteet tulisi ulottaa kattamaan oman toiminnan lisäksi koko kumppaniverkosto.

Avainsanat (asiasanat) Delfoi-menetelmä, johtaminen, kyberturvallisuus, kyberstrategia, lainsäädäntö, riskienhallinta, strategia, tietoisuus, tietoturvallisuus

Contents

Figures

Tables

Abbreviations

AI	Artificial Intelligence
CIA	Confidentiality, Integrity, Availability
COVID-19	Coronavirus Disease 2019, severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2)
DSO	Distribution System Operator
Enisa	The European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation (EU) 2016/679
ISAC	Information Sharing and Analysis Centre
ISMS	Information Security Management System
IT	Information Technology
NC ER	Network Code on Electricity Emergency and Restoration (EU) 2017/2196
NCSC-FI	National Cyber Security Centre Finland, Kyberturvallisuuskeskus
NESA	National Emergency Supply Agency, Huoltovarmuuskeskus
NIS	Directive of Security of Network and Information Systems (EU) 2016/1148
NIST	National Institute of Standards and Technology
OT	Operational Technology
SoA	Statement of Applicability
SUPO	Finnish Security and Intelligence Service, Suojelupoliisi
Traficom	Finnish Transport and Communications Agency, Liikenne- ja viestintävirasto
TTPs	Tactics, Techniques, and Procedures (used by the attackers)

1 Introduction - From the COVID-19 to a Cyber-COVID?

The writing of this thesis takes place during very exceptional times. Coronavirus disease 2019 (later COVID-19) crisis has turned our lives upside down during the year 2020 in an unpredictable way. Uncertainty of the business continuity followed by massive unemployment has set our society face to face with a new reality. For those, whose employment has not been endangered, this crisis has demostrated that the old structures and ways of working can be challenged. Working on site at the office is no longer a requirement, the workplace can be as well one's home. During the crisis people has become highly dependent of internet and digital services. The future will show if this is the new normal.

From the cyber security perspective this new setup requires more focus on the securing the remote work and assuring that the employees are respecting the company's information security policies while working. Managers have an increasingly significant role in such an exceptional situation, and emotional intelligence is needed to detect as early as possible the potential deviations.

After closing the office door, we all tranform ourselves from employees to private individuals. But have this transformation really taken place each morning the other way round since many of us we have been working from home having to take care of the children alongside the working duties?

Before the crisis, the household´s preparedness was faint. If we ask now if the people are more prepaired to face such a containment again, the answer would be yes. Yes, we are prepared and have enough emergency supplies to stay at again home for several weeks.

According to Kunnaskari and Peltonen (2018) Finns are resilient and willing to help one another in crisis situations like prolonged energy outages. From this point of view we have essential conditions in place to tolerate crisis. (57.)

During the crisis white hat hackers united their forces to collaborate and protect free of charge, especially the health care sector (Kyber VPK n.d.). This was a good example of how in such an exceptional situation people come to together and unify their forces for the common good.

Since Ukraine cyber security attacks, major cyber security incidents have been avoided in the energy sector. The cyber threats are constantly evolving like the COVID-19 virus. How will the future change the situation?

Due to the COVID-19 crisis several small and medium size enterprises in all sectors have met problems while big multinational companies gain profit from the crisis (Financial Times 2020). The impact of the crisis on the cyber security service and consultancy companies has not been under much discussion. Does the crisis affect the cyber security sector, how did the cyber security companies manage the crisis, and would there be a drop or an increased demand in cyber security services and consultancy now or soon? Did smaller cyber security companies lose their customers or was there an increased demand for cyber security services? The impact of the crisis on the cyber security sector at the national level is not covered in this thesis since observations during longer periods are needed. Will this crisis endanger, or will it increase the national cyber security level, the results will be known in the future? The COVID-19 crisis is a good example of unforeseen changes in which our society should be prepared to and be flexible.

1.1 Research Questions and Approach

The background of this thesis is the existing implementation of ISO/IEC 27001:2013 certified information security management system (later ISMS) of the commissioner Elenia Verkko Oyj. With a certified ISMS and a first three-year cyber security roadmap already implemented, the future of the cyber security development for a distribution system operator (later DSO) should be thoughtfully planned. Basic elements of cyber security have already been implemented including cyber security governance, cyber strategy, and regulatory requirements.

The aim of this thesis is divided in two goals. First aim is to look in the future which are the possible visions of the cyber security of the electricity distribution. What kind of world awaits us and how should we be prepared? The second aim is to study the actual cyber security requirements of the distribution system operators. What is required today and what is a reasonable level? The results of the thesis provide the commissioner with visions of probable futures and a basis to be implemented in the

continuous development of the thesis' commissioner´s cyber security management in form of cyber security roadmap proposal.

Thesis do not cover the General Data Protection Regulation requirements (later GDPR), information security management system (later ISMS) theory, nor implementation of an ISMS but instead concentrates on the continous development requirements: the longterm cyber security roadmap. We should be prepared to counter the future threats and make the the right choices to confront what is yet to come in the continuously evolving world.

This thesis goes through the European and Finnish guidelines and regulations applied to electricity distribution. Also, the trends and threats from European and Finnish sources are presented to give the most correct situational picture.

The research questions of this thesis are:

1. What is the meaning of cyber security in the electricity distribution business in the future?
2. What is the reasonable level of cyber security for a DSO?

The research questions are answered using both qualitative and quantitative research methods. The answers to the first research question will be given using content analysis of the theoretical background, interviews, and a Delphi panel. The second research question is answered based on the analysis of the regulation and legislative requirements set to DSOs including the results of the Delphi panel.

Elenia´s strategic goals are defined for the next five years. A three-year plan to achieve strategic aims is defined but predicting beyond the near future is challenging. The energy sector and cyber security are both rapidly evolving. Due to this constant evolution, the cyber security threats which will be encountered during the forthcoming years, can´t be predicted without anticipation. The Delphi method is perfect to study a phenomenon which is not yet known and can have diverse manifestations.

1.2 Structure of the Thesis

First part of the thesis introduces the commissioner including commissioner's ISMS and cyber security strategy. Reseach methods of the thesis are presented followed by the previous studies and the key concepts. The changes of the energy sector are described next and emphasized to give the reader a good understanding of the disruption which has started to occur in the DSO's business. The fifth chapter describes the societal meaning of the energy including the prospects which can be seen today. The fifth chapter also gives insights to actual smart grid risk landscape and introduces probable futures in form of security of supply scenarios.

Before the actual research conduction, chapter six presents cyber security trends, threats, and risks which will be incorporated in the evaluation of the changing landscape. The trends are collected from several sources including global risk landscape, reports of Finnish authorities and global cyber security suppliers. The future megatrends according to Finnish Innovation Fund Sitra will be presented.

The theoretical background continues in the chapter seven and introduces the Finnish cyber security strategy and the national and international regulation of the DSO´s. The theoretical background is followed by the research and the research results in chapters eight and nine. Finally, the conclusions and recommendations for future research are given.

1.3 Elenia

The commissioner of this thesis is Elenia Verkko Oyj. Elenia Verkko Oyj is part of the Elenia Group. Elenia Verkko Oyj is the second largest DSO in Finland supplying services to 430 000 customers in Central Finland, Kanta-Häme, Pirkanmaa, Päijät-Häme and South and North Ostrobothnia. Services consist of connecting new customers to the electricity network, supplying the customers with electric power, ensuring the electricity network operations including maintenance and safety with appropriate investments, monitoring the operations of the electricity network, handling the outages and serving customers with information, metering electricity consumption and providing the hourly data to customers and power vendors,

enabling efficient electricity market and power vendor changes, invoicing customers and developing smart grid and e-services. (Elenia n.d.a.)

1.3.1 Cyber Environment of Elenia

Figure 1 presents the various stakeholders who together make up the cyber environment of Elenia. Elenia is a group of companies working in close collaboration with their partners and the electricity market parties. The partners are performing the maintenance, construction, and outage handling of the electricity network in the field. To manage field operations, efficiently functioning material handling, work order management and coordination are vital. Information system providers are also in a significant role in the functioning of the system. The consumer and enterprise customers are naturally the most important stakeholder groups. In the third stakeholder perimeter are the authorities, municipalities, shareholders, investors, landowners, media, job applicants, students, and the sub-contractors of all partners. As one can see, the cyber environment is composed of several stakeholders which is important to understand when defining the cyber security roadmap.

Figure 1. Elenia´s Stakeholders (Elenia n.d.b.)

1.3.2 Elenia´s Cyber Strategy

Elenia is a provider of essential services, which sets requirements to ensure the electricity supply in normal and exceptional circumstances. The criticality of the electricity sets requirements and responsibilities also for information and cyber security. The continuity of the operations is assured by effective cyber security management. (Elenia 2019a.)

Elenia's cyber strategy is Elenia group wide and is based on business strategies. The cyber security strategy was published in 2019. Elenia's strategy states the importance of cyber security which is ensured by a separate cyber security roadmap. (Ibid.)

The strategy emphasizes the security of supply as being the primary concern in normal and exceptional conditions. The following strategic aims are the core of the strategy:

- Proactively reduce the probability of a cyber security incident
- Handle the possible incidents and exceptional circumstances to minimize the business impact of the incident
- Secure the uninterrupted functioning of vital information networks and systems
- Prevent data loss and unauthorised use of information, information networks and systems
- Establish information security practices as modus operandi for the entire company (Elenia 2019a.)

In addition to the aims, there are four strategic alignments. These alignments are cyber security of business operations, security of supply, partnership management and security of personnel. Business operations emphasize enabling business development and digitalization. Enterprise architecture must include cyber security and the design, implementation and continuous operations should include cyber security. Cyber security is linked to enterprise risk management and external competence and partnerships are used to audit the cyber security implementation. Security of supply aligns the importance of automation and IoT as the primary areas of cyber security. Partnerships are in a significant role in business operations and the cyber security knowledge and awareness of the partners must be assured. Security of the personnel highlights the importance of the knowledge and awareness of employees. Employees should have the necessary competence in assuring the cyber

security of the complex systems both in the business operations and in business development. Strategy emphasises that the information security is handled according to the ISO/IEC 27001 standard and the company is compliant with the general data protection requirements. (Ibid.)

For the creation of the first cyber security roadmap, a gap analysis based on several information security frameworks and best practices was carried out in 2018. Based on the gap analysis, a roadmap was created consisting of ten different development areas which were

- Cybersecurity strategy and governance model,
- Data security and data processing,
- System and network security,
- Third party security,
- Security event monitoring and threat mapping,
- Business continuity and incident management,
- End-User device management,
- Physical security and
- Identity & access management. (Ibid.)

1.3.3 Elenia's Information Security Management System

Elenia's management has decided to implement and certify an information security management system in compliance with the ISO/IEC 27001:2013 standard. The decision was taken after the electricity market act was updated with the requirements of the directive on security of network and information systems (later NIS directive).

According to the NIS directive (Directive (EU) 2016/1148), a DSO must ensure the risk management of the networks and information systems they are using. Electricity market act (L 9.8.2013/588, 28 §, 29 a §) also requires the compliance with the requirements of the security of supply, according to which cyber security must be continuously and systematically monitored and developed, the risk management methodology documented and described as a part of a mandatory preparedness plan. The ISO/IEC 27001 standard has been chosen for Elenia's ISMS framework since it is a globally recognised information security management system standard.

The scope of Elenia's information security management system includes the people, information systems, processes and the services provided by Elenia group's electricity distribution, energy supply, energy sector customer service solutions, project management, construction, partner management and group services. Physical office locations are included in the ISMS scope. (Elenia 2019b.)

The ISO/IEC 27001 standard requires continuous development of ISMS. The compliance is audited by an external accredited body on a yearly basis and the recertification takes place every third year. ISMS is part of Elenia's certified management systems. The other relevant certified management systems are electricity network management ISO 55001, electricity network management PAS 55, occupational health and safety management system OHSAS 18001 and environmental management system ISO 14001. Management systems assure quality and provide a solid foundation in Elenia's business. Elenia fulfilled the ISO/IEC 27001:2013 standard's requirements in March 2020 and received the ISO/IEC 27001:2013 certificate in April 2020.

2 Research Methods

To study the importance of cyber security in electricity distribution it is crucial to understand the actual business environment and the forthcoming changes which may affect the sector. When the landscape and relevant topics of the future are known, the importance of cyber security and the required actions can be decided.

The theoretical background of the thesis consists of the future landscape of electricity distribution supplemented by trends, threats, and risks gathered from different sector specific publications, security of supply and cyber security articles, studies, and journals. As described in Figure 2, a **content analysis** and synthesis of DSOs changing business environment and the most important change drivers is made using **PESTLE analysis** tool to highlight the most relevant topics under each PESTLE factor. Two individual **semi-structured interviews** (N=2) will be conducted to evaluate the PESTLE results against the opinions of specialists from the energy sector. Based on the interviews, Delphi panel scenarios will be created using **content analysis**. Interest group and specialists of both the cyber security and energy sector

specific cyber security representatives will be invited to answer **Delphi panel** (N=22) questions anonymously to collect meaningful arguments from the panellists. The answers of the panel will be analysed and a proposal for the cyber security roadmap for the thesis´ commissioner will be given using **content analysis** combined with quantitative answers to the Delphi questions. A combination of research methods is chosen to guarantee the reliability of the research.

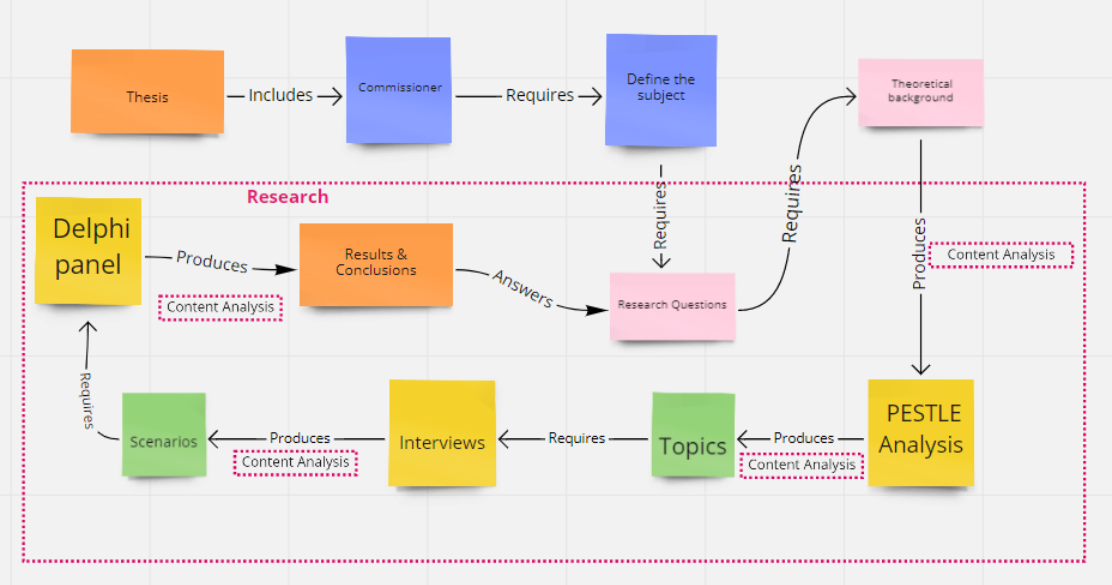


Figure 2. Thesis' Process, Research Part Emphasized

In this chapter the research methods of the thesis are presented. Mixed method is used. The conduction of the research is described in chapter 8.

2.1 Mixed Method

Both qualitative and quantitative methods are used. The qualitative methods are emphasized, quantitative analysis is used in Delphi panel questionnaire reporting. According to Creswell (2009), after Tuomi and Sarajärvi (2018), a research combining the two methods is called a mixed method research. Using both methods together is fertile and is assuring that the factors which may be missed with the use of only method, are covered. (Tuomi & Sarajärvi 2018, 56–58.) The use of quantitative

analysis together with qualitative analysis of the interview responses and Delphi panel results will give reliable recommendations.

According to Valli and Aarnos (2018) when planning for the data collection, the methods should be selected in a way that the results enable an analysis and examination of both the larger context and individual cases. The reliability of the collected data is important, how well the collected data stands for and covers the research topic, could it be transposed to another similar target group. The data should be collected so that general conclusions can be made. In quantitative method the majority is important, with qualitative methods the analysis of the researcher is the key. (22–24.)

The collection of the data differs in the quantitative and qualitative methods. Qualitative methods include interview, survey, observations, and data collection from different documentation. These collection methods can be used alone or combined depending on the available resources for the research. (Tuomi & Sarajärvi 2018, 62.) In this thesis three different methods are used: data collection from the theoretical background using PESTLE analysis for initial topics, interview to validate and evaluate the initial topics and thirdly a single round Delphi panel. Qualitative research method perfectly suits the needs to collect and highlight the opinions of the experts in the field of study.

2.1.1 PESTLE Analysis

PESTLE analysis is a tool to understand the political, economic, sociocultural, technological, legal, and environmental aspects which could be either disrupting or creating opportunities. PESTLE is a mnemonic of the first letters of each of these issues. The changes of the future will affect us, the question is how. The PESTLE model helps in framing the subject, asking, and answering the right questions to analyse the possible outcomes of the changes. (Warner 2010, 27–29.)

A lot of information sources can be found about trends and threats. This information needs to be structured to be useful and exploitable in research. In the PESTLE model, the information is approached from six different environments. P as political are the political changes expected to affect the sector of the research. The E as economic

incorporates the economic issues. The S like socio-cultural changes include the changing values, beliefs, and demographic structures. T like technologies which can influence the future of the sector. L stands for legal and regulatory changes and finally E for environmental trends. In addition to the identification and description of the trends, they must be analysed, why and how each trend matters. (ibid., 29–39.)

2.1.2 Content Analysis

Content analysis can be used as a single method but also as a theoretical framework. Downe-Wambolt (1992), referenced by Bengtsson (2016), describes the content analysis as being an objective and systematic way to make sound conclusions from written, visual, or verbal data to depict a specific phenomenon. When planning the research, the credibility and logicality of the content analysis decisions must be considered.

According to Tuomi & Sarajärvi (2018, 78–89.) it is important to carefully select the data meaningful for the research. Essential is to make clear what is wanted to be found out, how and from whom and select an adequate number of informants to answer the research questions to obtain confident results. The usual number of informants is 1 to 30. The informants must be made aware of the confidentially and the voluntariness of the study including the possibility to withdraw their participation and data during the process. (Bengtsson 2016.)

Usually there are several interesting findings which come up from the collected data and the researcher must narrow and choose the meaningful content. According to Tuomi & Sarajärvi (2018) the analysis can be divided in four parts; first decide the meaningful content, secondly select the content, and separate it from the rest of the data, thirdly classify, create themes of typify the data and finally make an analysis. Usually the classifying, creating types or themes are erroneously mistaken to be the analysis. The data classification can be used as a qualitative analysis if the content is classified, and the number of occurrences is counted. (Tuomi & Sarajärvi 2018, 87–89.)

As described in the data analysis process presented in Figure 3, the researcher should read the collected data through to understand the sense. Then the data can be

separated into smaller units called meaning units. Each separate meaning unit is coded. (Berg 2001; referenced by Bengtsson 2016.) Inductively created codes and inductive reasoning are the process of developing conclusions from the data and combining it with the theory. Codes are created during the analysis to answer the research questions. Inductively created codes can change during the process whereas deductively created codes are defined before the analysis and remain the same. To assure the reliability during the process, coding should be performed repeatedly according to Downe-Wambolt (1992) referenced by Bengtsson (2016). When the meaning units are identified, they are condensed to identify categories. Condensation means that the number of words of each meaning unit is reduced without losing the meaning. This process is needed if the data is collected from an interview and latent analysis is used. Manifest analysis means that the researcher uses the words of the informants, and references to the text are made. (Burnard 1991; referenced by Bengtsson 2016.)

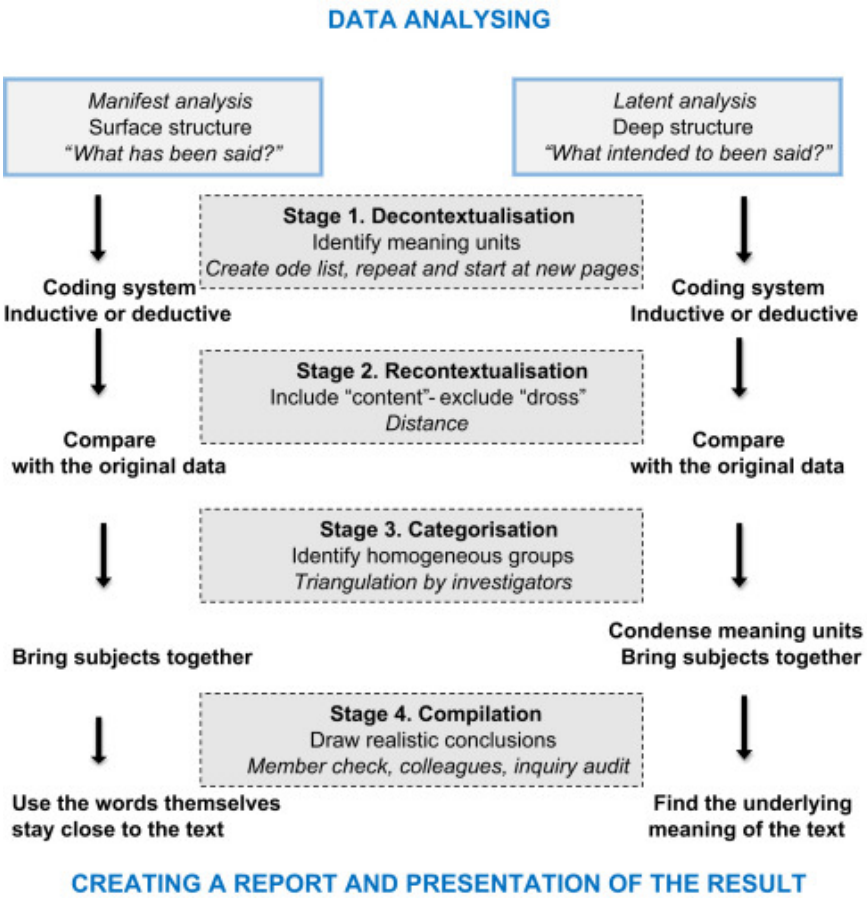


Figure 3. Data Analysis process in Content Analysis (Bengtsson 2016.)

Validity of the qualitative study means that the same results would have been obtained if the same study was conducted by another researcher (Morse and Richards 2002; referenced by Bengtsson 2016). Different researchers may obtain different conclusions. To validate the results, another researcher could make the same analysis and the results could be discussed. This triangulation can also be performed by using different informants in the data collection to confirm the results (Denzin 1978, referenced by Tuomi & Sarajärvi 2018, 124).

The data collection in this research comprises several phases. The first phase is the theoretical background and the analysis of it using the PESTLE method. Interview of two experts is followed to confirm and validate the findings of the PESTLE analysis. Interviews are transcribed and analysed using inductive categorization process meaning the categories were created during the process and not before the study as in a deductive categorization process. Inductively created codes changed during the thesis process and different categorization is used in interview and Delphi panel analysis. Manifest analysis is used meaning that the analysis of the data is done by describing what has been said, what is obvious and visible, the opinions of the panellists are referred to in the analysis of the Delphi panel. Latent analysis is the other possibility to analyse the data. In latent analysis the underlying meaning of the data are searched. (Berg 2001; Catanzaro 1988; and Downe-Wambolt 1992; referenced by Bengtsson 2016.)

2.1.3 Semi-structured Interview

Interview is a flexible data collection method. The interviewer can clarify, repeat the questions, and have a dialog with the interviewee so that each question is answered, and the purpose of the interview fulfilled. Compared to a questionnaire sent by email or in paper form, in the interview the questions can be presented in different order to collect a largest amount of information concerning the topic. For ethical reasons and for a successful interview, the questions or at least the topics of the interview should be sent in advance to the interviewees. During the interview observations can also be made covering not only what has been said but also how it was said. Interviews are time consuming and so costly which is a weakness of this data collection method. (Tuomi & Sarajärvi 2018, 62.)

Semi-structured interview emphasizes interviewees interpretations, meanings and how the meanings are formed. Semi-structured interviews have predefined themes, and more questions can be asked to deepen the answer. The relevance originates from interaction. (Tuomi & Sarajärvi 2018, 65.)

Interview is used in this research as data collection method to validate and evaluate the topics selected by the researcher from the theorical background with PESTLE analysis. Observation is not part of the interviews, only what is said is meaningful in this study.

2.2 The Delphi Method

According to Rubin (n.d.) the purpose of forecasting the future is to broaden the variety of the future choices and give a meaning to todays´ choices. Each choice is dependent on the past choices. Our choices are connected to the available knowledge about the past and about the future. Knowledge is based on history, values, culture, the prevailing conditions, nature, and the individual experiences of each person.

The best potential future can be achieved when the possible choices, both the positive and negative ones, are recognised and when their likelihood is studied. Even though the future is the sum of the past and of future choices, it is unpredictable. We can have a vision of what lies ahead, the possible futures. The future is not predetermined, we can lead our way in a direction if we have identified possible paths. For that reason, it is important to know the possibilities, what is likely and what is desirable. (ibid.)

The Delphi method is named after a Greek place called Delphi. The name Delphi derives from the word dolphin. The son of Zeus, Apollo, was the ruler of Delphi. Apollo was famous everywhere in Greece due to his beauty and the ability to foresee the future. Apollo disguised himself in the form of a dolphin to attract the first oracles to Delphi. This is the reason the place was named Delphi. The first oracles were sailors. The futurists are seen today as the sailors and oracles of Delphi. Delphi became the centre of the future in the antique Greece where Apollo´s predictions were transmitted by the oracles interpreted by the priests. (Kuusi n.d.)

After Kuusi (n.d.) the Delphi method was first used in the United States in the 1950´ for military purposes. This technique consists of collecting the positions and opinions of specialists to find possible futures. These specialists are the oracles of today. The Delphi method can have various interpretations from a single survey to a committee.

The Delphi method is good for bringing values, new viewpoints, and ideas to planning and decision making. This method could also be used if the research is undetermined and requires an approach based on multiple research methods. Delphi method is usually applied with other research methods such as cross-effect analysis or scenario creation Kuusi (n.d.) continues. The success of the study is dependent on how well the subject and the research are defined.

Delphi method is a research technique where a group of selected specialists are answering questions in a controlled interactive process. The answers form information about the phenomenon of the research. The specialists are representing widely the knowledge about the research topic. All the answers and comments are anonymous which enables free, authentic, and varied communication and removes limitations which occur in face-to-face discussions. The social status, job or expertise of the panellist is not affecting the opinions of others when all dialogue is anonymous. There is no pressure of losing face in anonymous answers. (Linturi 2020.)

According to Hiltunen (2012) a typical study using the Delphi method consists of the following phases:

- Defining the research questions and the aim of the study
- Defining the research team for conducting the study
- Selecting the specialists and composing the panel for the survey
- Developing the survey questionnaire for the first round of the survey
- Conducting the first phase of the survey with a written questionnaire or by interviews
- Analysis of the answers of the first phase
- Developing the survey questionnaire for the second round of the survey
- Conducting the second round of the survey and analysing the results
- Reporting the results of the study

The difference between a survey and Delphi method is iterative process. A survey is collecting information once whereas in Delphi the feedback is directed back to the panellists to guide the panellist to argument again over their choices and comments.

The process is like a dialog where different opinions are presented and discussed without juxtaposition. The formation of the information is creating the basement for a possible next Delphi round. The number of rounds in a panel depends on the available resources and aims of the research. Catalyst of the Delphi round is Delphi manager. Manager is responsible for composition of the panel, questions and motivating the panellists. Manager should not manipulate the results while conducting the panel. (Linturi 2020.)

Expertise connects to interest. Therefore, it is important to select the panellist carefully and include generalists and dissidents to the panel to challenge the experts to give ground for new yet unknown occurrences, social structures, and technologies. The aim of the Delphi process is not only collecting information about the research topic but also producing information. (Ibid.) In argumentative Delphi the purpose is not to foresee a certain future but to discover specialist's thinking and assumptions. Delphi method requires also explaining reasons behind the assumptions and opinions. This argumented information is useful in decision making. It is typical that panellists' subjective opinions change during the Delphi process and the process can be a learning event to the panellists. (Linturi n.d.)

The Delphi method is widely used when forecasting the future, especially in finding the possibilities of technological advancements. Finnish parliament's committee of the future has ordered several studies where Delphi method was chosen. One of the centres of Delphi in Finland is in Mikkeli called Otavan opisto, which is organizing an education in form of workshop and individual guidance on how to apply the method. This research community is concentrating on the internet-based Delphi applications. Hiltunen (2012, 208–212.) During the thesis process the author has taken part in this education and used eDelphi online application to organise the Delphi-panel. The eDelphi online tool is flexible and easy to use with comprehensive instructions. The reporting is included in the tool and is used when reporting the results of the panel. More information about the tool can be found on the tool's homepage. Individual guidance and workshops of the education is also used in the Delphi-process.

Delphi method is useful when finding possible futures. Therefore, this method has been chosen for roadmap creation. Roadmap is by its very nature a tool to conduct

the organization towards a desirable aim, the strategy addressing the occurrences of the future.

3 Previous Studies

When creating a strategic roadmap, it is important to understand the organizational choices and mechanisms which have allowed cyber-attacks to happen by not recognizing the organization´s vulnerabilities. The previous studies have been chosen not to study the details of the past attacks but instead the strategic and management level development needs to build an adequate cyber security roadmap covering future needs.

No results appeared when searching for Finnish studies on cyber security strategy development of critical infrastructure companies. Cyber security in the critical infrastructure is clearly an area requiring more research. Several studies exist about the Finnish national cyber strategy implementation challenges. One of them is presented in this chapter. The research was enlarged to cover cyber security and strategy in general including the protection of critical infrastructure against cyber attacks. Five different studies were chosen where different approaches to cyber security, risk management and implementation of regulation were studied.

Silfversten, Jordan, Martin, Dascalu and Frinking (2020) emphasizes in the study of national state-of-art cyber security, the approach to cyber security being typically risk management-based instead of managing performance. Measuring and evaluating the outcomes would enable the creation of relevant data for decision making and policy creation. The evidence for quality and fit for purpose are challenging to find in the cyber security sector. Silfversten & al. (2020) recognizes the missing relevant, verifiable large-scale data based on which decisions could be made. Defining and understanding the cyber security problem including required effective ways to handle it, is demanding without data. Since the relevant information about methods and data is missing there is a challenge in decision making; on which criterion the decisions should be based and how to measure the performance and impact of the applied measures. (36.)

Sallos, Garcia-Perez, Bedford, and Orlando (2019) describe how IT and communication technologies have changed the economical possibilities, value creation and enabled new business models since the geographical or temporal restrictions doesn´t apply in the man-made cyber-domain after Kuehl (2009). Yet this reliance on technology is shadowed by vulnerabilities and cyber threats. These threats can endanger the security, sustainability and even the existence of companies. Despite the significant impact of these threats, cyber security is not perceived as a value creator nor as an enabler for monetisation but as a problem which cannot be solved. (Sallos et al. 2019.)

Sallos et al. (2019) proposes that knowledge would enable effective cybersecurity and risk management. According to Neef (2005), Sallos et al. (2019) state that the company's ability to manage cyber security risks is linked to its ability to manage relevant knowledge. Julisch (2013), according to Sallos et al. (2019), depicts the relation between limited knowledge and ineffectiveness of a cybersecurity strategy as being witnessed by reliance on intuition, missing security foundations, inadequate governance, or a dependence on generic knowledge of the topic. Cyber security risks should be approached as a phenomenon combining the interaction of people, processes, and technology in the context of each company's own ecosystem rather than a domain specific approach. (Ibid.)

The intellectual capital is the overall knowledge of each person in a company creating value when combined (Dumay 2013; Dumay and Garanina 2013, 21; referenced by Sallos et al. 2019). Intellectual capital consists of information, knowledge, experience, intellectual property, and intellectual material. The cyber security risks are materialised from the combination of these elements with each company's own processes and value creation chains. In this complex interplay of elements, approaching cyber security only from a technical perspective is short-sighted. The organizational relational, structural, and human capital should all be considered. The foundation of vulnerabilities and how the perturbations are faced is rising from the history of each organization, the accumulated structures, technologies in use, interaction of systems, relations, and sub-systems. Knowledge is essential when aiming for an effective and efficient cyber security defence. (Kianto et al. 2014; referenced by Sallos et al. 2019.)

According to Sallos et al. (2019) a data breach relies on the different approach to the information between the attacker and the defender. Attackers´ target is to gain information and take advantage of the possible vulnerabilities, while the defender is focused on value maximization. The attacker can put all efforts to one breach while the defender must success in defending against all breaches. The defender´s approach can be based on biases, assumptions and ignorance when evaluating the likelihood of a vulnerability and the required defence mechanisms. From the attacker's point of view, an unsuccessful attack is not a significant cost. This state creates the so-called ecosystem of cybercrime after Kraemer-Mbula et al. (2013) referenced by Sallos et al. (2019) or the underground economy after Thomas et al. (2015) referenced by Sallos et al. (2019).

Sallos et al. (2019) present the misalignment of the defence being caused by the missing link in the organization between the defence responsible and information system failures. These misalignments occur especially in the trade-off between security and accessibility or efficiency.

In several cyber security strategies and policies, information sharing is seen as a mechanism to mitigate this informational imbalance. Effective information sharing would help the defender correctly align the mitigation initiatives. Studies have proved that approaches favouring operational priorities in detriment of security are favoured. Misaligned initiatives could lead the behaviour of organizations or strategy development in the wrong direction. (Sallos et al., 2019.)

Sallos et al. (2019) continues and emphasizes that it is both the technical and context dependent local capabilities which are needed to develop cyber security knowledge and situational awareness. Whereas today, when recruiting cyber security ability, the accent is put on the graduation and learned technical skills instead of wide understanding of the societal factors, experience, and context dependent understanding.

Cyber security strategy would benefit from a knowledge-centric approach since the strategy is diversely structured. With the knowledge-based approach, cyber security would have the ability to create value. (ibid.)

Vepsäläinen (2017) has studied the future energy sector competence needs. The study presents the competences which will be needed based on the changing political, Socio-cultural, legal, and technological context of the energy sector in Finland. Also, the competences which will be less needed were part of the study.

In the field of energy production and supply, the future competence needs are the skills for managing larger entities; there are more energy sources, assets, materials, information, technology, logistics, circular economy, legal and regulatory requirements and so on. Skills to constitute an overall picture and to combine different contributory factors together are needed. Researchers and developers are also needed for studying the production, storing, buying, and transmitting energy in the changing context where carbon neutrality and renewable energy are emphasized. (ibid., 101.)

With globalization, the energy sector may interconnect to a larger network. Such a network would require increased regulation, contract management skills and so energy sector lawyers will be needed. Together with tightening requirements for the organizations, consumers could be subject to regulations based on their activity in the energy market. (Ibid., 66–67.)

A comprehensive approach to answer the consumers' needs will be emphasized instead of deep competence. Flexibility, willingness to server and competence for creating concepts are needed. Vepsäläinen (2017) presents the concept of an energy janitor whose role would be a guide in everyday energy questions. Such a person would know energy technology, has electrical engineering competence, knows the production techniques of the households, has good skills in information technology, IoT and smart grids. Such a janitor can help with the use of devices, has technological skills, energy sector certifications and willingness to serve. (102.)

Mäkinen (2016) has studied the national cyber strategy implementation program from critical infrastructure point of view. According to Mäkinen (2016) Finland´s cyber strategy implementation program is authority centric. Sector specific implementation programs including critical infrastructure are not published even though Finland was among the first countries to issue a national cyber strategy. Mäkinen (2016) also emphasised that the leadership at the national level is missing.

The cyber strategy implementation program called *Kyber 2020* was launched to implement the strategy into action, but participation is not mandatory for the critical infrastructure actors. Many of the critical infrastructure companies are owned by the private sector, therefore there is a need to increase cooperation between private and public sectors. Two examples of a successful collaboration are presented and recommended, the operating models of Estonia and the Netherlands. Finally, Mäkinen (2016) proposes a cyber security evaluation framework to be implemented including key performance indicators (later KPI) and logic modules familiar from program management to evaluate the outcome of the Kyber 2020 program. The European Union Agency for Cybersecurity (later ENISA) also recommends these tools to be used when evaluating each nation´s cyber security strategy.

Pullinen´s (2012) thesis approach to the cyber security is technical. He has studied how to protect the critical information systems against cyber attacks. Even though the management, strategy and cyber security risks are not in the focus, Pullinen (2012) describes a threat modelling example and states that needed resources should be given in information system projects to carry out threat modelling, especially in mission critical systems. Threat modelling would allow us to recognise the possible attack vectors based on which needed defence mechanisms could be correctly adjusted. Pullinen (2012) recognises that the threat modelling being not widely used, there are no research data available concerning the possible positive impact of threat modelling on the level of information system´s security.

Synthesis of the Previous Studies

Sallos et al. research recognises that even though cyber security is approached as an organizational question, it has a significant societal impact. The research reveals a possible foundation of a successful cyber security culture; the intellectual capital of each employee combined into a companywide common knowledge of the threats and the vulnerabilities. The knowledge-based approach would empower the whole organization to identify the risks continuously instead of top-down risk management activities taking place less often. Finnish National Agency of Education´s research of future competencies reveals the need for energy generalists and confirms the need for a knowledge-based approach.

Mäkinen´s thesis reveals the missing mandatory participation obligation in national program for the critical infrastructure actors. Voluntariness could lead to situations where the organizations who would benefit the most from help and guidance will not take part due to missing resources. Critical infrastructure´s interdependency is important, and each actor's cyber security practises should follow a common baseline. A framework proposed by Mäkinen could be extended to the organization level to create an exact situational picture of the cyber security maturity of each critical infrastructure organization. Finnish National Cyber Security Centre (2020) has recently launched a maturity evaluation tool called Kybermittari [Cyber meter] which could enable an independent and reliable baseline for the development needs.

Threat modelling requires both the information system functional and technical knowledge. One of the reasons why threat modelling may not be widespread and not part of every project could be the misunderstanding that cyber security is a combination of technical and business knowledge. An effective threat modelling would require several parties, the business operations responsible, architects, technical security responsible, software developers and system owner to sit in the same table and go through the use cases, threats, and to name the risks together.

The previous studies are covering the topic of cyber security strategy implementation at national or independent of sector while this thesis is approaching cyber security from the DSO perspective. General principles of cyber and information security are generic, but specific sectors have its specificities, especially national critical infrastructure whose failures to prevent and recover from cyber-attacks would affect the whole society.

The tactics, technics, and procedures (later TTPs) of the attackers are important to analyze in detail to learn from the occurred attacks and about adversaries. Author´s personal experience has showed that case examples of past occurrences are unbeatable in the awareness training. Although important, this thesis is not taking a deep dive in the past occurrences´ details, even if they give an excellent view of the evolution of the attacks but concentrates on management and strategic level actions to reach an economic, effective, efficient, and good-enough cyber security culture.

4 Cyber and Information Security

Cyber security is a state where cyber space can be trusted, and the functioning of cyber space is secured. Cyber security includes the required actions to anticipate and resist different threats and their consequences. Information security threats are causing disturbances in cyber space. Information security is a key element alongside measures taken to ensure the continuity of the operations of the physical world in case of disturbances. Information security is the confidentiality, integrity, and availability (later CIA) of the information while cyber security is the security of the digital interconnected world´s operations. (The Security Committee 2018, 31.)

Information security is how the CIA of the information is guaranteed. **Confidentiality** means that information is neither available nor published to entities which are not entitled to use the information. **Integrity** means that the data is not altered during creation, being at rest, use or transfer. **Availability** means that entities have access to the data which is meant to be accessed by them at the right time.

Information security measures are e.g., physical access control and locking system, safe document handling and disposal, encryption of data, use of certificates, firewalls, antimalware software and backups. Securing the data, data communications, hardware, software, and information systems are included in information security. Information security can also be referred to as a state where information security risks are controlled. (Ibid., 15.)

Cyber space is a place where electronic and electromagnetic spectrums are used to alter, transfer and store data in one or several digital information systems. Cyber space includes the physical structure needed to process data. Examples of cyber space are banking and payment systems, logistics of food supply, traffic, and nuclear power plant control systems. (Ibid., 21.)

According to Limnéll, Majewski, Salminen, and Samani (2015), humans are at the center of the cyber security and human element is always present; artificial world of bits and bytes is created by humans. No cyber security breaches have occurred without human’s willingness to act. Cyber security is protection and a way to ensure that we can trust the functionality of the digital world. Dynamic is the word that

describes the cyber world the best. There is no time nor geographic boundaries, and this world is global and real 24x7x365. The physical world of atoms and cyber world are intricately connected and in constant interaction. Operations in the physical world are dependent on the cyber world. A disruption in the cyber world will affect the physical world. (16, 29–30, 38–49, 76.)

Many companies refer to information security when talking about securing the data capital of the company even if cyber security would be a more proper term. Cyber security should be a concept that is wider than information security or network security. It requires constant situational awareness, dynamic security measures, collaboration, and continual development of security culture. (Ibid., 19–20, 54.)

Cyber security is a company's strategic choice and goals must be set at a strategic level. Strategic level answers the questions why and what. These goals are then realized at the technical level, but the technical level should not be the goal-setter. Technical level answers the question how. (Ibid., 79.)

Cyber security cannot be limited only to the company's own processes. The whole stakeholder network must be included. For example, a third party's system may enable unauthorized access to an organization's confidential information. To ensure that security is a key foundation towards a company's future, traditional security solutions are a good starting point, but they are sufficient only until a certain point. Cyber security demands a broader point of view. Cyber security measures should be considered in every organization since they would enable continuation of operations in situations where society's shared infrastructure collapses. To realize this goal the organization must have in place shared standards, practices, controls, reporting, situational awareness, and disruption management. (Ibid., 55–57.)

The cyber world is not only about threats and risks. Cyber security should also be an enabler for the company's possibilities and innovations. (Ibid., 85.) Cyber security should therefore be a constantly ongoing process that enables exploitation of the cyber world's opportunities in different areas of the company's actual business context and in search of new business areas (Ibid., 101).

Definition of Martin, Rashid, Chivers, Danezis, Schneider and Lupu (2019) extend the definition of cyber security in 19 different knowledge areas presented in Figure 4.

Cyberspace can be defined as a place where humans are communicating, business and art is made, and relationships are developed. Cybercrime, terrorism, and war may occur in this place. Interruptions may have impacts both in real and virtual worlds. (3–4.)

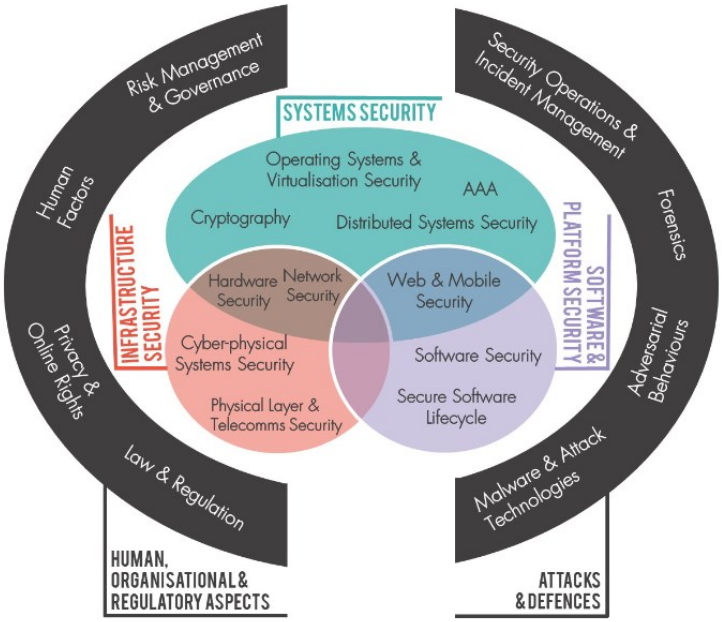


Figure 4. Cyber Security Knowledge Areas by CyBOK (Martin et al. 2019, 4.)

4.1.1 Information Security Management System

The purpose of an ISMS is to protect organization's information assets and assure the business objective fullfillement. The ISMS is approached from the risk management point of view. Depending on the sector and the size of the organization, there might be regulatory, legal, or contractual requirements which apply to the organization. Smaller organizations which do not work with personal of confidential data usually do not need a sophisticated ISMS. In these organizations information security risks can be assessed as a part of a company's risk management process. (ENISA n.d.)

The most important in developing an ISMS is the management's and stakeholder's understanding of prevalent information security risks and the need for protecting organization's information. After the commitment of the management and

stakeholders, the key elements are to setting up the necessary organizational roles and responsibilities, the people. ISMS development requires administrative people and technical knowledge for implementation to succeed. (Flyktman 2016, 36–37.)

4.1.2 ISO/IEC 27001 ISMS Framework

ISO/IEC 27001 is an international standard describing the requirements for an information security management system. The standard consists of mandatory clauses, which are

4. Context of the organization,
5. Leadership,
6. Planning,
7. Support,
8. Operation,
9. Performance evaluation, and
10. Improvements. (ISO/IEC 27001:2017, 29.)

In addition to the clauses, the standard includes annex A, a set of 114 controls the organization should implement. The implementation of all these controls is not mandatory, organizations should identify the necessary controls.

The ISO/IEC 27001 is part of the ISO/IEC 27000 standard family which includes standards setting the requirements and standards supplying guidance for the implementation and continuous development of the implemented ISMS. As presented in Figure 5, there are three standards setting the requirement: beforementioned ISO/IEC 27001, ISO/IEC 27006 requirements for the auditors who are certifying the ISO/IEC 27001 conformity and ISO/IEC 27009 for sector-specific implementation requirements for the ISO/IEC 27001. In the sector specific guidance energy sector specific standard ISO/IEC 27019 supplies guidance for the information security controls for the energy utility industry. In addition to the requirements, the family includes several standards to help in the implementation process. These standards consist of the best practices for implementing the requirements and controls. (ISO/IEC 27000:2020, 18–20, 24.)

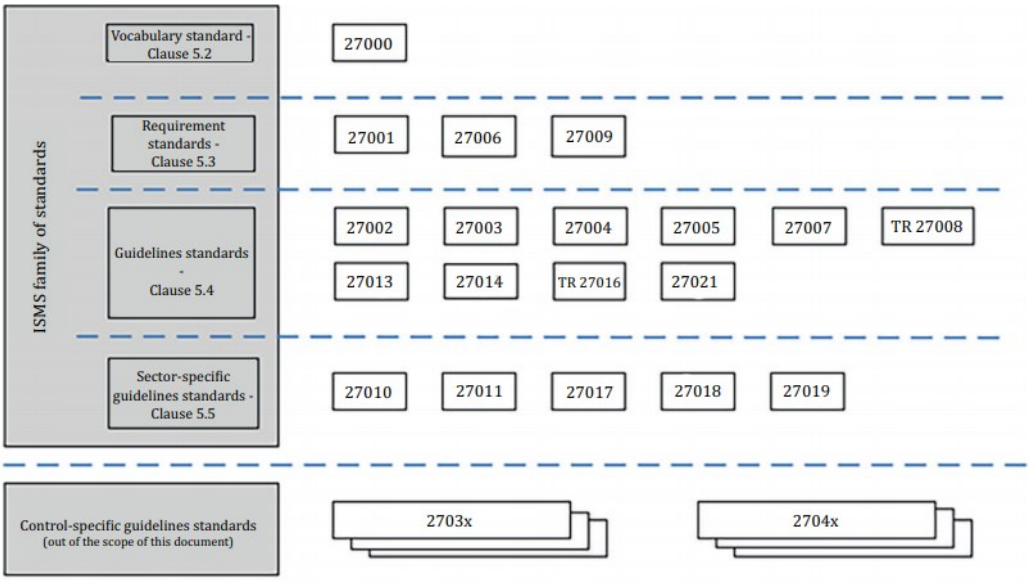


Figure 5. ISMS standard family (ISO/IEC 27000:2020, 19.)

A step-by-step implementation of an ISMS in described in Figure 6. After the management´s commitment and decision to implement an ISMS, the first step is to define the ISMS´ scope. ISMS can be applied first in a smaller part of the organization, for example the IT department. Next, the inventory of the information assets should be conducted. When the assets are known, the risks threatening the assets can be named, evaluated and a risk treatment plan created. Statement of applicability (later SoA) is a mandatory document which describes the state of the controls of annex A supplemented with the regulatory and contractual requirements. Internal audits are mandatory. When all these steps are finalised and the requirements of the standard´s clauses 4–10 are fulfilled, the organization is ready for a pre-assessment and finally, after possible corrective actions, to certify the compliance. After the certification is achieved, the continuous development of the ISMS starts.

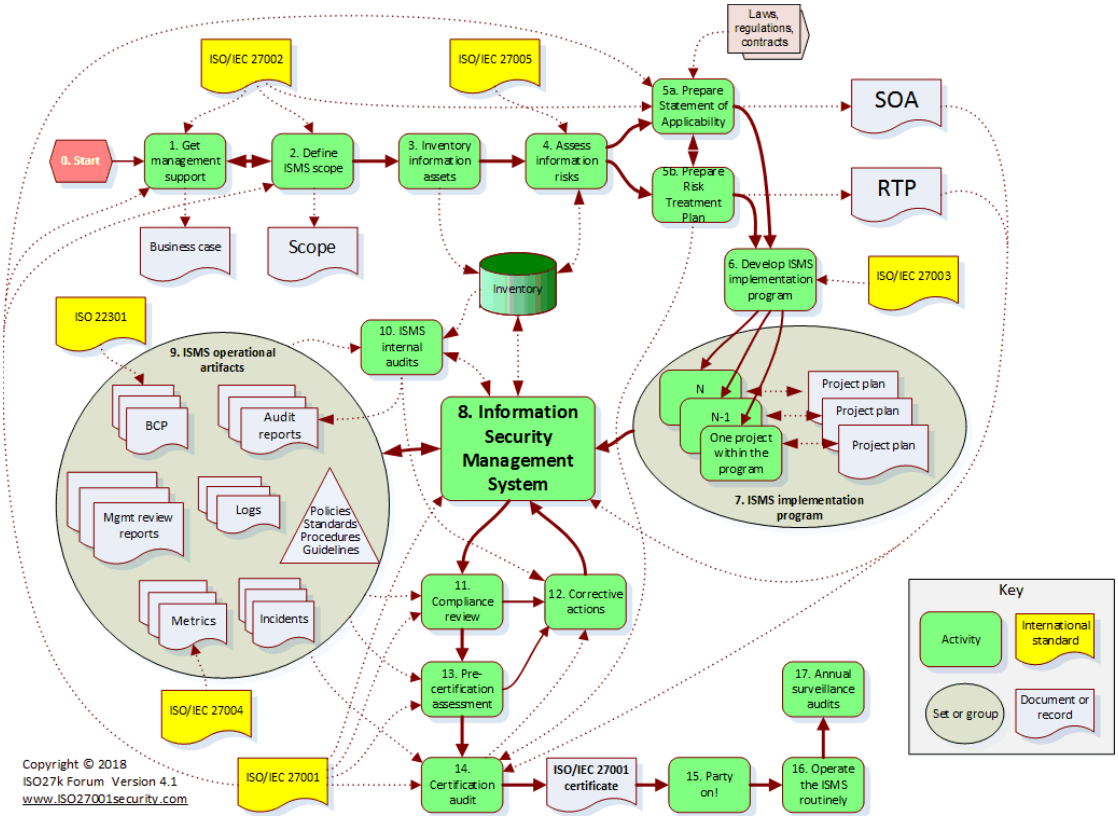


Figure 6. Step-by-step implementation of ISO/IEC 27001 (ISO27k toolkit n.d.)

4.1.3 NIST Cybersecurity Framework

The United States National Institute of Standards and Technology (later NIST) cybersecurity framework was issued in 2014. The NIST framework deepens the ISO27001 approach of people, processes, and technology to include governance, management, procedures, policies, supply chain management and training. The framework was created as a response to an executive order of United States´ former president Barack Obama to develop voluntarily a cybersecurity framework aiming to protect critical infrastructure. The approach is based on risks and cost-effectiveness. (Vacca 2017, 7.)

The framework is divided into three parts, the core, tiers of implementation, and profile. The core includes a set of outcomes and activities separated into five categories, each of which has sub-categories described in Figure 7. These security function categories are identify, protect, detect, respond, and recover. Tiers of implementation supplies context for cyber risk management and guides the

organization in the considerations of right level of the cyber security program. Tiers is also a communication tool to facilitate discussions concerning budget, priority, and risk appetite. Profile is organization specific and is used to define the desired level of cyber security. (National Institute of Standards and Technology 2018.)

IDENTIFY	Asset Management Business Environment Governance Risk Assessment Risk Management Strategy
PROTECT	Access Control Awareness and Training Data Security Information Protection Processes and Procedures Maintenance Protective Technology
DETECT	Anomalies and Events Security Continuous Monitoring Detection Processes
RESPOND	Response Planning Communications Analysis Mitigation Improvements
RECOVER	Recovery Planning Improvements Communications

Figure 7. National Institute of Standards and Technology Framework's functions and categories. (Vacca 2017, 7.)

5 Energy as an Enabler for the Society

Distribution of electricity is a fundamental necessity for the functioning of a modern society. The electricity distribution business is subject to a license and, the distribution companies are monopolies in their own distribution areas. According to the Energy Agency, there are 77 distribution network operators in Finland at the time of authoring this thesis. (Energy Authority n.d.a.)

Energy distribution business´ foremost threats for security of supply so far have been natural events like storms and snowloads. The underground cabling will assure the weatherproofness of the distribution networks and lower the impact of the weather on the security of supply. On the other hand the increased implementation of intelligent devices to the interconnected business environment sets essential importance to the cyber risk management. The need to identify the risks has been acknowledged at the national and international level.

5.1 The Future of the Electricity Distribution

According to Haapala (2020), the Finnish energy system is at a turning point. Finland has the ambition to be carbon neutral by 2035 and the fossil combustibles will be gradually abandoned. The replacing solutions to produce the necessary energy are yet at the design table together with the means to assure the security of supply of these novel solutions. The future is uncertain what comes to energy production and distribution technologies.

The sufficiency of the capacity during the energy consumption peaks is a concern says Haapala (2020). At the same time, a structural change is challenging Finland; continuously raising proportion of the energy is produced by difficultly adjustable wind and nuclear power.

National Emergency Supply Agency (later NESA) has started a program called *Energia 2030* in which the security of supply and the risk management of the future energy distribution network is studied. One of the projects included in the program is to investigate energy islands as an energy supply solution in case of a major transmission system network disruption. (Ibid.)

The program also includes preparedness exercises. Even though the energy sector has long traditions in contingency planning, the energy system changes will require more investments in preparedness planning and training. (Ibid.)

The increase in renewable energy and the production of electricity that varies according to weather conditions mean significant changes to the Finnish electricity system. Maintaining the power balance in an entity consisting of distributed resources requires an increase in automation, in which case we are talking about an

intelligent electrical system, ie an intelligent network. Cyber security is at the heart of using automation. (Ministry of Economic Affairs and Employment of Finland 2018.)

According to Ang and Utomo (2017) the cyber security threats are increasing alongside with the technological development and the increase of the automation. The use of technology already has and will change the future of the energy sector. The exchanged information has increased, more detectors are installed, and automation has increased the process efficiency. Outage times are reduced thanks to the optimization of the operations.

Cyber terrorism has appeared, and it is state sponsored. Cyber threats are a nationwide problem if the critical infrastructure is attacked. To protect the critical infrastructure the energy sector requires operational technology (later OT) and information technology (later IT) competence. Therefore the approach of the cyber security must be comprehensive. (Ibid.)

The electricity network has developed from the distribution monitoring and controlling entity to an integrated bidirectional communication system. Consumers have become energy producers with the solar panels and they are selling the produced energy back to the electricity grid. In the future the digital electricity grid will be an active network being able to collect, analyse and transform the data into an important business asset. (Ibid.)

The reliability of the energy supply is the core of the DSO business. The overhead lines will be replaced by underground cabling, which is weatherproof. According to Elenia this work has started in 2009. For Elenia the annual investments to the underground cabling is 160 million euros in 2020 including 3500 kilometres of cable. The underground cabling supply employment for hundreds of persons across the Elenia’s geographical area. The half of Elenia’s powergrid is already weatherproof. (Elenia 2020.)

The security of supply requirements is set in the Electricity Market Act. In the effective law it is said that after 2028 an electricity outage may not be longer than six hours in local detailed plan areas and 36 hours outside these areas (Partanen 2018, 20). This valid goal may change if the Electricity Market Act is updated. It would give more time to the DSO´s to implement this requirement. At the same time, the

profitability of the DSOs could be reduced. (Ministry of Economic Affairs and Employment of Finland 2021.)

The increase in renewable energy sets new requirements to the distribution network since wind and solar energy production is fluctuating. There must be a continuous balance between consumption and production in the Nordic electricity system. A storage solution is needed alongside the increase of wind and solar energy production.

Batteries will be part of smart grid development in the future. During a power outage they will guarantee the energy supply for the customers. In normal situations batteries can be used to regulate the power, meaning supplying a solution to the fluctuations of production and consumption. The battery also assures the energy supply in case of a power outage caused by storms or other damage to the power grid. The batteries are planned to be installed in locations where the overhead power lines will remain for a longer period. (Lähdeaho 2020.)

The batteries could also be a cyber security resilience control to handle an unexpected power outage. In the case of a cyber-attack targeting electricity distribution the batteries would provide the consumers with electricity and the impact of the attack would remain limited.

Innovative technology enables new possibilities for consumers. One example is a service to control energy consumption by directing the consumption to the lower priced night hours. This service enables cost-efficiency. According to Juujärvi (2021) also the green values are promoted when using the service, since the night-time electricity production is made with less carbon dioxide emitting fuels.

5.1.1 Smart Grid Working Group

A smart grid working group set up by the Ministry of Employment and the Economy examined the possibilities of smart grids and presented in its final report in 2018 concrete measures that would promote the security of supply and customers' opportunities for active participation in the electricity market. Working group proposes that the flexibity of the demand should be market driven activities as well as electricity storages and new services, giving the ability to the customers to take

part in the market. Aggregators, that is, provides of flexibility services and energy communities are introduced in the report. These new actors would help the consumers to reduce the consumption peaks and profit from lower price hours. (Pahkala, Uimonen and Väre 2018.)

Working group also presents the minimum requirements for the next-generation smart meters. A load control functionality should be integrated to increase the possibility to demand flexilibily. DSO should create the technical platform, but the actual control conmmands would come from a service provider. Control commands should be possible to update several times a day. Next-generation meters should also report the consumption several times a day and enable selling the produced elecricity to the grid if the consumer has production. (Ibid.)

A roadmap proposal is attached to the working group´s report. The roadmap is expecting an increase in the electric cars estimatig their number being 250 000 by the year 2024. (Ibid.) According to Finnish Transport and Communications Agency (later Traficom) the number of electric cars at the end of the year 2020 is 9697 (Finnish Transport and Communication Agency 2021).

The transition to a smart electricity system together with digitalization will bring threats alongside opportunities. The cyber security of the smart electricity system must be balanced to ensure that the development includes adequate measures to protect data and real-time communications. A decentralised energy system will include a lot of remotely controlled intelligent devices which are all taking part in keeping the power balance and the market systems. The controllable devices are presenting a threat to the smart energy system if cyber security in not considered appropriately. Since the devices might be internet facing, a risk is important if the data security is not ensured. The whole society could suffer from a cyber-attack. Each actor should have clear responsibilities and practices to handle exceptional situations. The working group states that international cooperation should be increased, and the authorities should actively take part in creating the EU wide cyber security regulations (Pahkala, Uimonen & Väre 2018, 33).

5.1.2 Digital Self-Sufficiency

Since the electricity network is becoming increasingly intelligent, more technology is required. Finland is not independent from what comes to the supply of technology and devices. Anttila (2019) questions the need for digital self-sufficiency. With digitalization we have been pushed to enter a world where the actors are global. The computing ability is moving from local datacentres into the cloud, and we are increasingly dependent on suppliers. The proposed alternatives are few. The traditional solution yet is still to buy computing ability from a supplier's datacentre.

Until now computing ability and buying the hardware has been accessible to everyone at the same time. Cloud computing is already altering this self-evidence. The suppliers are specializing in answering the hyperscale cloud provider's needs and volumes rather than continuing to produce hardware for the standard market. A decline in the turnover of the two biggest server hardware suppliers has already been seen in 2019. At the same time, the turnover of hyperscale server providers has nearly doubled. (Ibid.)

The specialisation of the server providers could lead to a situation where the national security of supply in endangered since we are unable to buy capacity and services otherwise than from global cloud suppliers. For such suppliers Finland's security of supply is not a priority. Using capacity from clouds is a relatively new domain and there are no studies made concerning their longevity. The whole existence of these services should be questioned since the geopolitical situation is continuously fluctuating. Have we been prepared for submarine data communication cable's major availability problems? (Ibid.)

5.2 Smart Grid Risks

Prent (2019) categorizes the smart grid risks in four distinct categories. The mix of technology with internet connected devices all over the network added with a limited possibility to apply security patches. Cascading effects are the second category since the energy sector interconnects with the entire society as shown in Figure 8. The smart grid requires different security concepts than the IT security. The OT supplier immaturity comes to complete these risk categories.

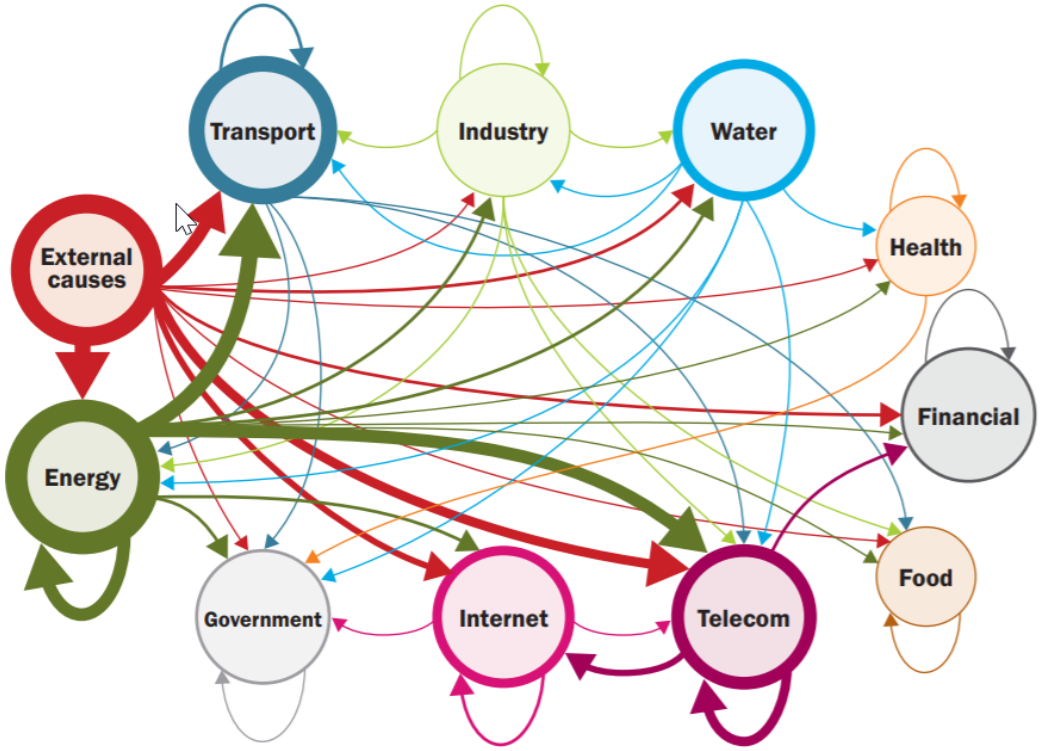


Figure 8. European dependencies and effects of critical infrastructure disruptions 2005-2009 (Luiijf, van Schie, van Ruijven and Huistra 2016, 26.)

The security of supply and the security of operations of the society´s vital functions are shaped by the interdependencies. These dependencies should be identified to minimize the impact of disturbances. Finance, telecommunications, software development, energy and manufacturing production are the core of society and disturbances in these sectors quickly affect the whole society. (National Emergency Supply Agency 2020.)

The cyber security present condition in 12 sectors and 100 companies was studied. The most crucial factor in the cyber security development of an organization is the management´s commitment. When the management has set the responsibilities and follows up the targets, the perfect foundations for systematic and risk based cyber security management are in place. This approach assures that the cyber security level of the organization is not dependent of single cyber security specialist´s knowledge or enthusiasm. (Ibid.)

The regulations have a positive impact on the advancements of cyber security. Also, the continuously changing threat landscape sets challenges to the regulation to cope with the pace of change. (Ibid.)

The study concludes that the national critical infrastructure, all sectors included, have common development needs. These common development needs are a common situational picture, secure software development and cyber security aware and competent personnel. In addition to these common development targets, the energy sector has development needs in the cyber security architecture as shown in Figure 9. (Ibid.)

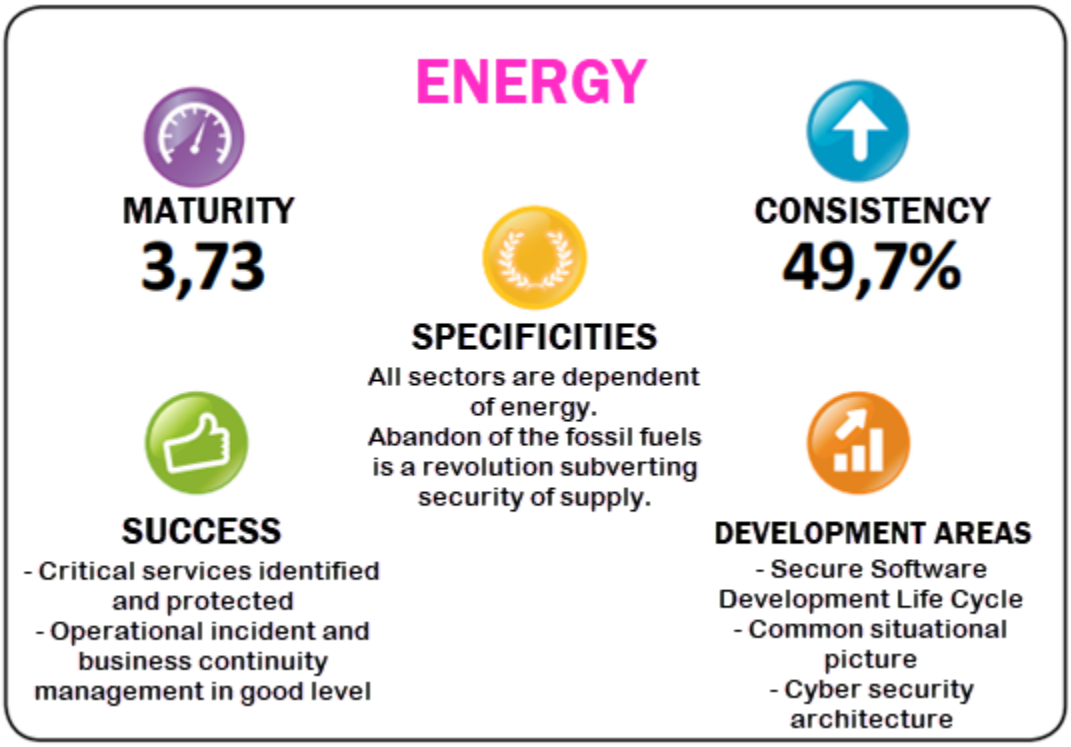


Figure 9. Energy Sector Cyber Security Management Maturity translated by author (National Emergency Supply Agency 2020.)

Figure 9 depicts the energy sector results of the study. The results summarize the maturity of the cyber security processes and methods supporting the management of cyber security. Maturity scoring in this survey was from 0 to 5. The energy sector score is above average but below the finance, telecommunications, and ICT/software sectors. The results of this study give assurance of the national cyber security level

since these four sectors are heavily interconnected and dependent on each other. (Ibid.)

Strategic situational picture is a tool for management to direct future development. Important development has already occurred in the national situational picture for example the Finnish National Cyber Security Centre (later NCSC-FI) has been set up. NCSC- FI publishes different situational picture reports at the national level including sector specific reports. A network of sector specific cooperation has been set up and NCSC-FI is coordinating these Information Sharing and Analysis Centre (later ISAC) groups. (Ibid.)

Secure software development is particularly important in the energy sector because of the long software lifecycle. The secure practises should include the whole lifecycle since cyber security risks are materialised via the software. The secure development practises lower the occurrence of threats, guide the personnel in secure ways of working and lower the impact of mistakes. Secure software development practices should be included in both buying software but also in the company's own software development weather in cloud or in on-premises environments. Since the software lifecycles are long, the supplier’s business continuity risks should be considered to avoid situations where maintenance and support would no longer be available for the software. Knowledge of cyber risks is needed on both sides; the software developers need to have the qualifications and the possibility to apply secure practises and the purchasers of the software need to be aware of the cyber risks. Benefits of widespread secure software development would be nationwide if the baseline of the software security requirements were set up. (Ibid.)

Awareness and cyber security competence of the personnel can be approached from various aspects. Cyber security awareness should start with recruitment including background checks and mandatory training. In addition to the first basic training, complementary education should be based on each person´s work specifications. The basics are the same for everyone, but specific roles and responsibilities require more detailed and sector specific deepening. The lifecycle of each person´s career should also be considered. This way the susceptibility to be a victim of social engineering and other threats is lowered. (Ibid.)

According to a study, cyber security architecture is company specific. The study reveals that only a few companies have included cyber security architecture in their enterprise architecture. The maturity and the implementation level also vary. The management of security should be considered a daily routine, not over-glued protection. (Ibid.)

Concerning the cyber security architecture, Prent (2019) recommends adopting zone model and implementing secure communications and access control. Zone model architecture´s benefit is to protect the interfaces between IT and OT. Zone model should be implemented based on risk level management. Standards could also give valuable guidance, for example IEC 62443.

World Economic Forum has published a playbook for the boards and cybersecurity officers of electricity in 2020. The guide was published during the covid-19 crisis and includes the top ten worrisome risks related to COVID-19. Figure 10 describes the cyber security risks related to the changed working conditions as being the third biggest risks. (World Economic Forum 2020a.)

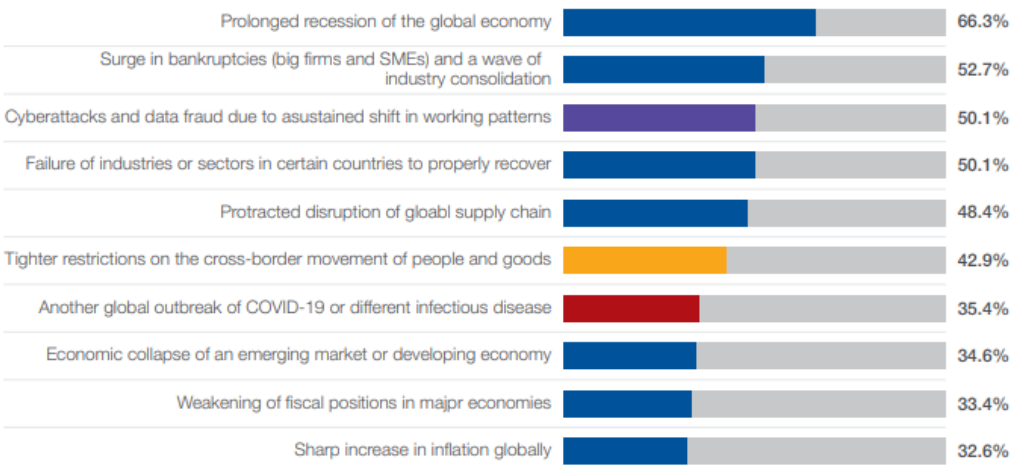


Figure 10. Top Ten Worrisome Risks Related to COVID-19 (World Economic Forum 2020a, 5.)

The energy sector should deal with cyber security from a business point of view and consider the operational risks. Business is increasingly dependent on digitalization and the internet. The governance should adopt a resilient mindset and be prepared to recover from possible cyberattacks. (Ibid.)

Figure 11 presents the areas in which the boards of the energy industry should concentrate their actions. Seven categories have been identified. These are cyber risk and resilience management, governance, organized cyber resilience including resilience planning, performance reviews for board and organization performance and collaboration among the energy entities. (Ibid.)

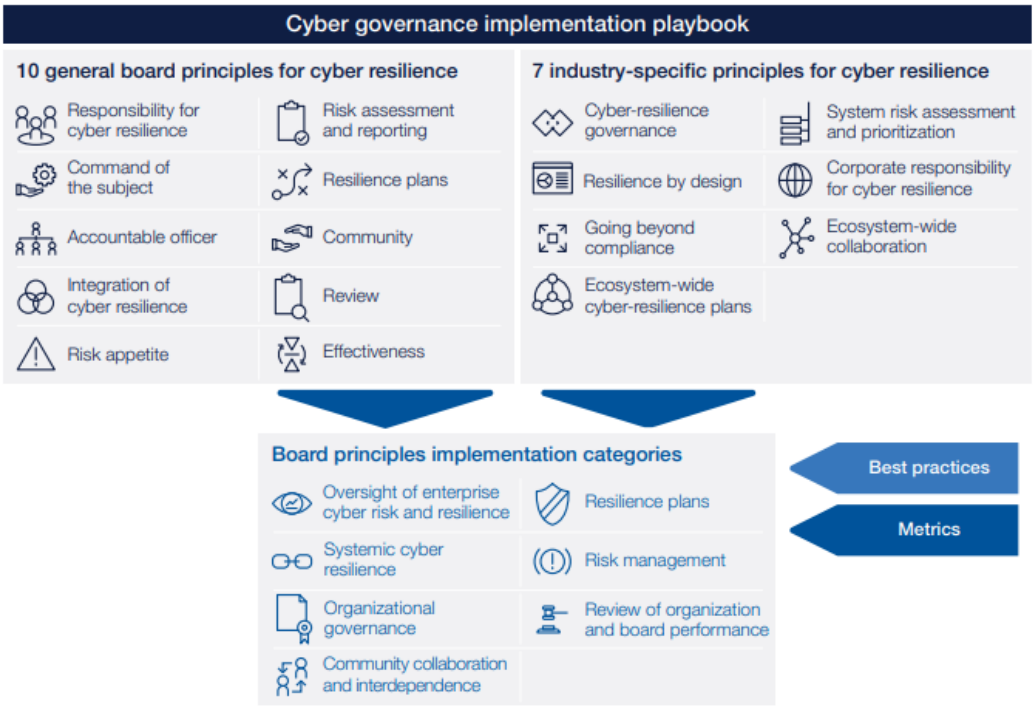


Figure 11. Implementation Categories of Board Principles (World Economic Forum 2020a, 6.)

6 Cyber Security Risks, Threats and Trends

The World Economic Forum has published a global risk report 15 times. The cyber risk impact and likelihood have constantly increased over the years. In 2006, 2007 and 2008 the cyber risks were recognised as threats to the critical infrastructure, starting from 2012, cyber risks entered the reported risk set. Figure 12 presents the 2020 situation. Cyberattacks are number 7 risks when considering the likelihood and number 6 risks when considering the impact of all risks. Climate action failures, extreme weather, biodiversity loss and natural disaster are considered as the most significant risks globally. (World Economic Forum 2020b.)

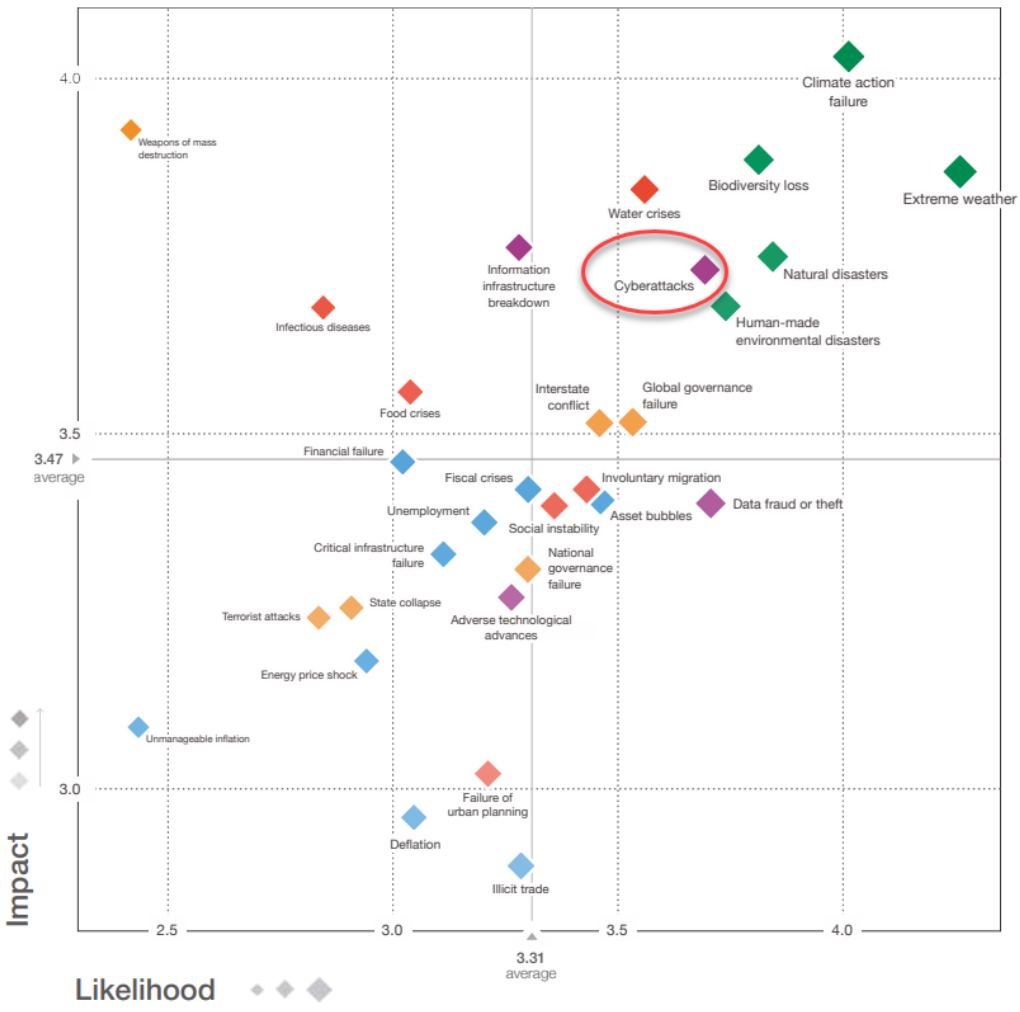


Figure 12. Cyber Attack Impact and Likelihood in Global Risk Report 2020 (World Economic Forum 2020b.)

In the 2012 report the dark side of the connectivity is raised in the executive summary. Cybercrimes, terrorism, and virtual world wars do not equal the ones in the physical world yet but could well do so in the future. The power is moving from the physical world to the virtual world. Everything is connected, five billion mobile phones were connected continuously to the internet and different applications. People are dependent on this technology and daily life is vulnerable to the incidents and crimes of the cyber world. The challenge is global and yet the risk management initiatives are not in line with the importance of the risk. The private sector is enquired to take a more significant part in securing the stability of the virtual world. The world economy requires healthy cyber space. (World Economic Forum 2012, 11.)

In the 2014 report cyberspace defence and offence were discussed. Already in 1988 it was identified and written that espionage in cyber space would offer benefits and is cost-effective. Cybercrime and espionage are occurring daily, yet the society nor information systems hasn´t been broken or suffered from persistent or widespread failures, only information has been stolen. This resilience is due to the standards, investments and private sector actors like service operators and incident response teams. The advantage is on the offensive side. Cyber-attacks have been and will remain easier to realize than encounter. This has a historical background since the internet was built based on trust. A perpetrator needs to find only one security flaw and the defender must ensure the defence of each vulnerable spot. Penetration testing, so called red teaming, has been used by companies since 1979 to find out these vulnerable spots. The red teams usually reach their goals, the prevailing security controls rarely prevent the attackers from accessing the target information. This fact is still true today. (World Economic Forum 2014, 38.)

Cryptographic technologies are the core of digital trust, authentication, and online identities. Online services like banking, commerce and email rely on secrets. Confidential business information and sensitive personal data confidentiality is preserver with cryptography. If these technologies were to collapse, a profound disruption would occur in our society. Quantum computing could put historical data and every encrypted data in danger. With quantum advances it would be possible in the future to decrypt any data previously stolen. Since there is a massive number of resources allocated to quantum research today, new cryptographic algorithms are

already being considered and even a return to offline data management is a conceivable alternative. (World Economic Forum 2019, 7.) Cybercriminals are also taking advantage of cryptography by using encrypted network traffic which makes it difficult for the defender to notice. Organization´s should consider options how the get visibility inside the encrypted traffic. Quantum safe algorithms should already be used.

Finland has also started to invest in quantum technology with the VTT Technical Research Centre of Finland. VTT has started building the Finland´s first quantum computer aiming to be at the top of the quantum technology development. (Ministry of Economic Affairs and Employment of Finland 2020.)

Another important already ongoing development which will affect our future along with quantum computing is AI. AI has remarkably developed and can recognise and predict human emotions and respond to them. Such a capacity could result in new threats since ethical law enforcement nor standards are in place to prevent these risks. These risks could occur because of accidental or intentional misuse of emotional intelligence, for example in healthcare where AI has started to be used in psychological care. Affective computing can recognise emotionally responsive people and supply them with desirable information and finally alter their behaviour. Feeding people with fake news, encouraging violent behaviour and radicalisation, or gaining nationwide oppressive control over people are examples of risks which an emotional control could result in. (World Economic Forum 2019, 13.)

According to Barnhart-Magen and Caltum (2018) when we talk about AI, we mean machine learning. Machine learning software is trained to do something, and the training is done using the occurrences of the past. Due to this fact, machine learning can´t recognise the events of the future.

Since machine learning requires training, the data used, and the responsibility of the developer are important to understand to avoid bias. To enable ethical, non-maleficent, fair, and non-discriminative use of AI, common global rules and standards should be created.

F-Secure (n.d.) recognises the interconnectivity of the energy sector as being unusual considering the threat landscape composed of mobile and physical assets. Cyber security incidents in this sector would affect both the public and private sectors.

The operational technology's lack of cyber security controls is a recognised deficiency. Several components of operational technology (later OT) are missing security controls, for example authentication, even though remote management is enabled. This is because when these systems were installed internet connectivity was not common. Even with the lack of security controls the OT systems have been opened to the internet to face many attacks. Considering the always on nature of these systems, the security patch and security control implementation has only a short or no time at all. The lifecycle of these systems is significant due to an elevated investment cost. These facts enable cyber-attacks on critical infrastructure systems. (F-Secure n.d., 4.)

As the global risk report depicted, cyber risks started to be considered significant and realistic in 2012. Different parties have different interests in penetrating the critical infrastructure systems. Nation-state´s aim is to compromise the systems by gaining a foothold position for political or economic purposes. The goal of the criminals is the people since the people are the weakest link. Companies' personnel in key roles are recognised and targeted by malware delivered by email or SMS to gain access to the company's internal network and important data. Attackers take their time and preparing for an attack can take months. An effective way to detect and restrain incidents is to employ the right competence at the right time with the right information. (Ibid.)

Today the energy sector consists of cloud service providers, supply chains, different organizations and IT and OT infrastructures with ICS hardware. The ICS components are built by a few specific companies and are often missing cyber security controls after installation. The lack of control is due to the companies limited awareness, inadequate segmentation, or incorrect configurations. (F-Secure n.d.)

According to Finnish Security and Intelligence Service (later SUPO) cyber espionage can be encountered with risk management. To shield a company against cyber threats is rigorous and continuous work completed with adequate information

security architecture. Cyber espionage requires resources which are not free of charge for spying nation-states. The adequate information security architecture includes comprehensive log management. Cyberespionage can be put into light by a skilful specialist with the help of logs. (Finnish Security and Intelligence Service 2020, 22.)

The risks related to the hardware bought from countries which are actively spying on Finland should be handled in the planning of the purchase. Such nation-state actors do not need a backdoor on the hardware, they have management connections and firmware updates available. A conflict of interest must consider whether the hardware producer is more bound to the state apparatus of the country of origin or into the customer´s requirements or laws of European Union or Finland. (Ibid.)

The supply chains are targeted by the nation states since more companies have outsourced their activities. This assembly creates a blind spot which hardens the detection of the espionage: the ICT service provider does not recognise the customer´s valuable information and the customer doesn´t have access to the service provider´s logs to discern the espionage. (Ibid., 23.)

In the yearly 2020 review of national security, SUPO describes the situation of intelligence activities against Finland. COVID-19 has hindered illegal human intelligence activities because of the travelling restrictions. Nevertheless, there are a considerable number of foreign intelligence service personnel permanently placed in Finland. The actions of foreign intelligence services are systematic and long-lasting. (Finnish Security and Intelligence Service. n.d.)

One of the aims of human intelligence is the Finnish critical infrastructure. Also, the political field including the arctic area and investments in strategic sectors are of interest. One of the means of intelligence organizations is to obtain the help of people who can directly or indirectly influence national opinion or political decision making. Technology and knowledge adherent to technology are also a target. SUPO estimates that the intelligence activities against Finland will continue broadly. The most important intelligence threats come from China and Russia, both are deeply implemented in different sectors of society and are also instigators of systematic cyber espionage. (Ibid.)

During COVID-19 cyber espionage has seen new possibilities since most of the critical infrastructure activities were carried out using remote access when working from home. The availability is often preferred to confidentiality when quick decisions are needed in abnormal conditions. Such decisions could endanger national security. Cyber criminals with economic purposes have taken advantage of the situation. SUPO estimates that cyber intelligence is more active than usual. Meticulous information security management is increasingly important in exceptional situations. (Ibid.)

NCSC-FI publishes a monthly report called cyber weather. In this report a situational picture is given monthly of the cyber security events, breaches, and news. The report includes, based on the monthly events, a top 5 phenomena ranking. All the phenomena of the year 2020 were collected from the monthly reports in a spreadsheet and a graphical illustration was created by the author to see the yearly changes. The graphical results are presented in Figure 13. As Figure 13 describes the most significant phenomena for the first three quarters of 2020 are phishing, faster vulnerability exploitation and ransomware attacks. In the beginning of the year the top position was held by the faster vulnerability exploitation, during the summer, phishing was at the pole position. On the third quarter the extensive ransomware attacks is the primary phenomena and in the last quarter a raise of different attack methods as a tool for extortion are the primary phenomena. (Finnish National Cyber Security Centre 2021.)

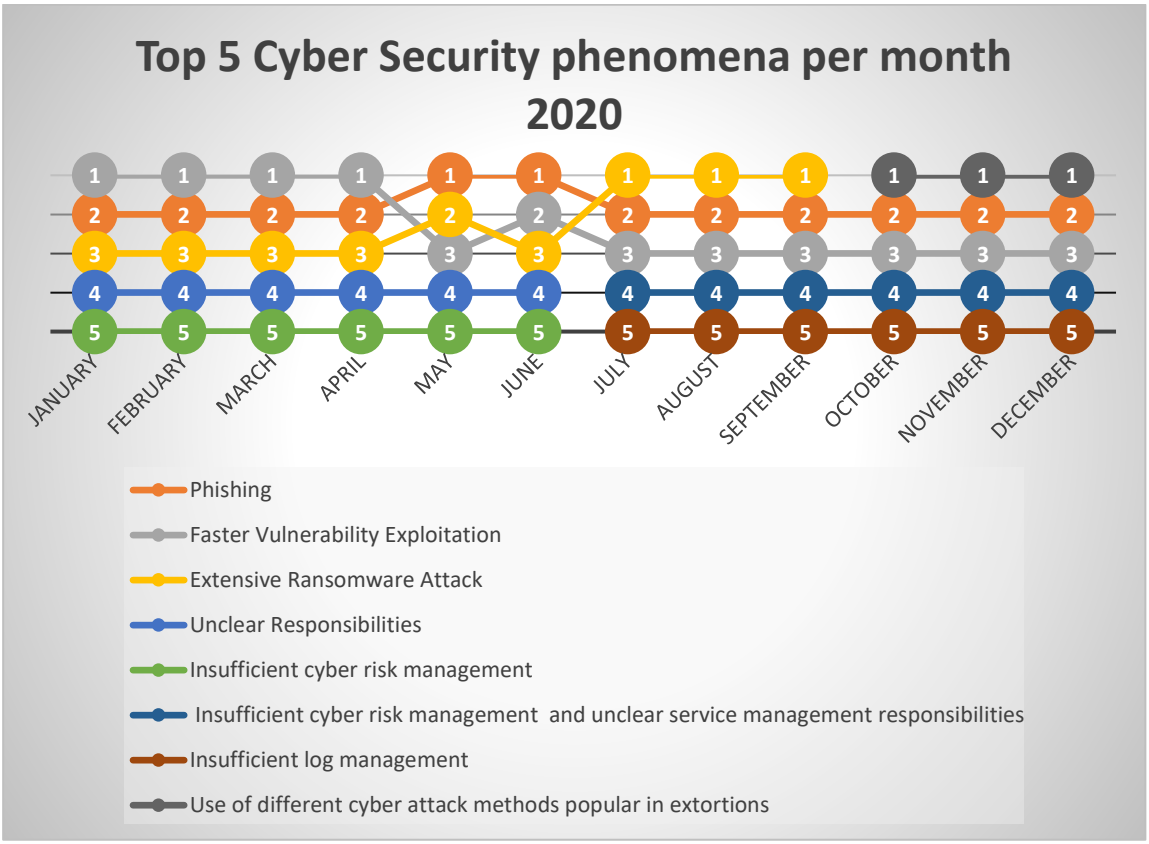


Figure 13. Cyber Security Phenomena per Month Year 2020 after NCSC-FI

ENISA (2020) recognises that the cyber risks will be increasingly difficult to specify. An effective cyber risk management would need knowledge of all variables which is increasingly difficult due to the continuously increasing threat landscape complexity and wider attack surface. Organizations have a wide variety of technology in use, and the attacker´s TTPs alongside with sophisticated tools in use are adapted based on the victim's environment. An effective cyber risk governance would require a novel approach to the organizations to move away from business unit-based thinking towards a hybrid threat approach. Disinformation and fake news are a typical characteristic of the new physical and virtual world interconnectivity threats.

As a cybersecurity challenge, ENISA (2020) mentions the risk complexity. The interconnectivity of the systems and networks enables a fast propagation of incidents. The AI is a key for future cyber defence with its capabilities to detect threats and attacks alongside security orchestration and automation. The complexity of the information system environment continues to enable cyber-attacks since many unintentional errors occur. Public cloud migrations continue to expand and

errors in configuration could expose a company to data breach. Cloud infrastructure providers are also an attractive target. Third party related threats and supply chains are an important part of the complex threat landscape and should be considered as an attack possibility. To fight the well-known alert fatigue of the false positives the cybersecurity industry is expected to bring solutions. COVID-19 has already introduced changes to the business requirements. The remote work has increased, and the business has digitalised, zero trust is seen as the future solution for securing the company assets. (Ibid.)

6.1 Megatrends and Metatrends

Finnish Innovation Fund (later Sitra) publishes megatrends to give a situational picture of important societal changes from the Finnish society point of view. The 2020 megatrends haven´t substantially changed since the 2017 published ones but the understanding and the extent of these phenomena are more widely understood today. Megatrends are typically long-lasting, widely recognized and slowly changing phenomena. They are not sudden; they are already occurring. Megatrends can have different accentuations in different countries. The 2020 megatrends are the following:

- ecological reconstruction as an urgent need,
- strengthening the relational power,
- ageing and diversification of the population,
- redefinition of the economy, and
- technology is embedded in everything.

For ecological sustainability, the discourse has changed from the sustainability aspects to a crisis debate; how to confront climate change, the diminishing biodiversity, and the increasing problem of waste. Will ecological reconstruction be made unequally or fairly for the population or is the environment only seen as an economical resource? Will technology be helpful for ecology, or will it be a disadvantage? The worries about the state of democracy have increased since social media is widely affecting the general opinion and the power is no longer held only by nations but also by global multinational companies, organisations, and regions. (Finnish Innovation Fund Sitra 2019.)

The use of technology is no longer a hype but an integrated part of everyday life. Technology offers solutions, including the energy sector, but on the other hand electricity consumption increases, and production must follow. A new phenomenon also requires new vocabulary. For example, data or circular economy are newly employed terms. (Ibid.)

The future cannot be known since it doesn´t exist and yet, a lot of can already be seen when observing the present situation and the presumed consequences of today´s actions. The possible futures can be seen. (Ibid., 6.)

The capacity and the need to anticipate the future has increased during the last ten years. The anticipation is concentrating on the ability to take advantage of and interpret the knowledge about the visions of the future. The future visions are not necessarily occurring exactly as they were expected. There are also tensions between trends which may affect the trend in a negative or a positive way. (Ibid.)

Understanding megatrends is a valuable resource when looking for possible futures. Megatrends can be described as a general tendency for the future. These trends are usually global and continuous. In addition to the megatrends, it is recommended also to look at the weak signals, more precise trends, and the tensions between the trends. To better understand the big picture, it is necessary to know the interaction and interconnections of the trends. (Ibid.)

In addition to the megatrends there are metatrends which are cutting through the megatrends and may affect the evolution of the trends. Metatrends present a big picture of the megatrends and the changes at hand. One of the metatrends is the arrival of post-normal time which includes accentuated contradictions, surprises, and discontinuity. The second is emotional influence. Loneliness and being separated from others are increasing and it can be said that people are alone but together. The future is not predictable, but it can be controlled with our choices and actions today. (Ibid.)

6.2 Security of Supply Scenarios 2030

In the security of supply scenarios 2030 NESA (2018) is aiming to provide insights, evoke thoughts and contribute to the critical infrastructure´s ‘continuity

management planning. Five scenarios are presented with measures going with, and each includes sector specific cases. The scenarios are global interdependency, armed power politics, blogification and hybrid influence, technological world order and the dominance of the east.

The energy sector specific description for global interdependency describes the creation of policies steering the whole sector towards emission free and renewable energy increasing the need for load-following power. New actors will enter the European energy market, cross-border electricity transmission will increase affecting the energy distribution costs. The EU will need better data security favouring at the same time open interfaces and data. The use of personal data will be more regulated, which will restrict the operations of large corporations located outside the EU. A new global information system will appear while foreign ownership of networks and datacentres will increase. Blockchain use will increase direct democracy European wide when utilised also in political decision making and public sector. Global information exchange will strengthen freedom of speech, which will be Finland's strength. (Ibid., 15, 17.)

In the armed power politics scenario, the risk of strikes against the energy sector has increased. The power politics uses the energy as a lever which creates a risk for Finland´s energy importation. Effective maritime fuel transportation in the Baltic Sea is increasingly important and challenging. European level energy sector steering will be replaced by national taxation and regulation focusing on securing the import of energy, increasing self-sufficiency, and decreasing the Russian dependency. Energy poverty will increase. Emerging cyber risks have diminished cross-border information sharing and cooperation. Research and development lacks resources. Data and information are increasingly isolated while the implementation of innovative technologies and digitalization has slowed down. Authoritarian values will replace liberal society and freedom of speech. (Ibid., 23, 25.)

In the blogification and hybrid influence scenario the uncertainty of energy availability is increased due to resource protectionism. Expansion and harmonisation of regional energy markets has set Finland increasingly dependent of Norway´s and Sweden´s dominant production positions. Imported energy is less dependent on the United States. The functioning of information networks and data security is

increasingly important to energy systems. National restricted information systems, networks and internets appear with escalated cyber risks and strengthening measures. Land acquisitions close to the important data storages or communication nodes are attempted to influence Finland. Information warfare is raised with easier fake news spreading due to people´s diminished trust in authorities and the raise of different reference groups and extremist thinking. Critical ICT systems and the use of media are regulated. (Ibid., 31, 33.)

The fourth scenario, technological world order, depicts advances in energy storage and technologies. There is an increase in electricity conversion into gas and heat. Smart buildings have appeared enabling efficient production and consumption regulations. Microgrids and small-scale electricity production are increasingly common. Dependency of oil decreases, new actors have entered the energy sector and the market has become more international with foreign ownership. Global giants own data and technology, but digital platforms enable the growth of decentralised operating models. Artificial intelligence (later AI) is making decisions, publications and has surpassed human reasoning. Digitalization, robotics, and automatization are everywhere. People´s media literacy differences is pronounced but at the same time technology has bridged linguistic and cultural differences. (Ibid., 39, 41.)

The last scenario, the dominance of the east, emphasizes China´s significant role. To increase the need of raw materials, technologies of storage and Chinese production in general, China has the role of climate and energy policy leader. Mines and oil fields are in Chinese possession and China has become an important energy market player globally. Russia is exporting oil and natural gas mainly to China. The power of the EU has weakened, and decision making is increasingly national. China is making energy investments, especially in bioeconomy, in Finland. Digital surveillance model has spread globally justified by order and security. A dramatical increase in the need for media literacy and education has occurred. It has become difficult to recognize the companies serving national information purposes. Power is at the hands of fewer actors replacing the western democracy model. Chinese are in possession of several European telecommunications and ICT companies. IoT, sensors, facial recognition, video surveillance and fingerprint identification are in place to enable continuous monitoring and automatic optimization. (Ibid., 47, 49.)

The technological world order and the dominance of the east scenarios are describing a less desirable future from a DSO point of view. If locally produced energy significantly increases, the ownership of companies is at foreign hands and the people are fed with information controlled by global giants, the operating conditions, handling of the electricity network asset and the market share of DSO´s would be affected and a significant threat landscape increase would occur. Materials and intelligent devices especially are in the control of big global companies. Global cyber security law enforcement including artificial intelligence and machine learning ethics would be needed to regulate cyber space. Regulation must be flexibly adapted to the global operating environment.

In all scenarios the common vision is the change of the energy sector from a national actor towards an EU wide or global business environment. Competition would increase which could also increase hybrid threats and worsen the prevailing cyber security threat landscape.

Globalization and interconnectivity of the energy networks could escalate a single breach to a large disruption affecting all the actors in the network. To prevent such a significant impact, the actors would be obliged to implement a common cyber risk management program, including threat modelling to understand the impact of one breach. The cyber security should be a constant topic on the boards´ table to secure to continuity of the business operations.

The World Economic Forum´s and NESA´s recommendations to pay attention to risk management and resilience planning today are also valid if one or several of the scenarios of supply were to present. A global operating environment would also increase the need of each employee to be continuously aware of social engineering in various forms. A person working in critical infrastructure would need sector specific cyber security risk management and resilience skills in addition to basic education. The actors operating in the same network should have a common cyber security operation centre whose target is proactively prevent cyber security breaches from occurring by training, monitoring, and constantly hacking all the actors in the network.

In an international environment a common language is needed. Umberto Eco´s observation from 1993 “The language of Europe is translation” is timely, since the English language is questioned as official European Union language after the Brexit. If the Asian dominance scenario were to realise, the artificial intelligence not being at place yet to make instantaneous translations, people in energy and cyber security sector might need to attend Chinese, French, Spanish, or German language courses.

7 Cyber Security Regulatory Requirements and Guidelines

In this chapter the cyber strategy of Finland is presented together with its implementation program followed by European Union guidelines and regulatory requirements of the DSOs. The second research question of this thesis *What is a reasonable level of cyber security for a DSO?* is answered from a regulatory point of view. Statutory requirements of the DSO´s will be identified and detailed at the end of this chapter.

According to NESA study (2020) regulation has a positive impact on cyber security. With effective regulations, the cyber security of the interdependent network could be secured. Noticeable is that the sectors, which are highly regulated, have high rankings when evaluating cyber security maturity. What must be emphasized with the regulation is that it is a slow means to increase security. Also, setting the requirements is challenging in a constantly changing cyber space. A well-balanced regulation in a sector where the organizations are of varied sizes is also challenging. The regulation is at its best for setting the minimum requirements.
(National Emergency Supply Agency 2020.)

7.1 Finland´s Cyber Security Strategy

The first cyber security strategy was published as a decision in principle in 2013 as a part of the national security strategy implementation. The aim of the strategy is to strengthen comprehensive security and initiate nationwide contingency and continuity management planning. (The Security Committee 2013.)

Society is increasingly dependent on electricity. This dependency sets new requirements for the energy sector to secure the availability of energy in normal situations, in abnormal conditions and in extraordinary circumstances. (Ibid.)

To put the strategy into practice a first implementation program was prepared. After the first program, a second implementation program has been published and the strategy has been updated as described in Figure 14.

Figure 14. Finnish Cyber Security Strategy Timeline (Olin & Rousku 2018, 10.)

7.1.1 Strategic Alignments for the Distribution System Operators

The strategy contains ten alignments. Six of these alignments set requirements to the national critical infrastructure including the energy sector. These alignments are the following.

1. An efficient cooperation model will be set up between the authorities and the different actors to promote cyber threat prevention.
2. The overall cyber security situational understanding and awareness of the vital functions of society will be increased.
3. Maintain and develop the ability to detect and combat cyber threats and incidents of the vital functions of society as a part of economic continuity management.
7. Improve the cyber security understanding and competence of all actors in society.
8. National law enforcement will ensure effective cybersecurity.

9. Authorities and business operators will be assigned service models, common fundaments, and responsibilities to manage cyber security. (The Security Committee 2013.)

7.1.2 The Strategy Implementation Program

The second implementation program was published in 2017. This program sets two aims for the critical infrastructure. Both aims are based on the strategic alignment number 3 presented in the previous chapter. These aims are the following.

16. The security of supply is adequate, and the supply is guaranteed for the vital functions of society.

Responsibility: The Ministry of Economic Affairs and Employment of Finland shall secure at the national level the adequate level of the security of supply based on the energy and climate strategy. A common criterion for energy consumers shall be set up taking particularly into account the increased criticality of the ICT-systems.

17. Improve the Cyber Security of the Companies Critical to the Security of Supply

Responsibility: National Emergency Supply Agency shall direct and provide the necessary resources for a program called KYBER 2020 aiming to improve the cyber security of the companies. The program should give rise to permanent structures engaging cyber security expert organizations to take part in long-term cyber security development. (The Security Committee 2017.)

KYBER2020 program included an energy sector specific program called Kyber-ENE. This program was initiated to create business-driven and concrete guidance to energy sector cyber security. Several energy sector companies took part in this voluntary program and a public summary including concrete guidelines is available. (Ahonen 2019.)

7.1.3 Updated Finland's Cyber Security Strategy

The updated strategy is based on the principles of the 2013 published strategy. The aim of Finland continues to be having the best ability and to be among the top cyber secure countries. The changes in the operating environment and distinguished

development needs required an update of the strategy. Several studies have been conducted concerning the state of cyber security in Finland. The results of these studies were considered when updating the strategy. The publication of the updated strategy initiated preparations for a cyber development program directed by a national cyber security director. (The Security Committee 2013.) The position of cyber security director is a fixed term mandate continuing until the end of 2021 (Ministry of Transport and Communications 2020).

7.2 National Emergency Supply Agency

Finnish energy supply is based on diverse sources of energy, decentralized production, and reliable distribution network. NESA´s purpose is to assure an uninterrupted availability of energy, advance the security of supply viewpoints in decision making, develop new sustainable means to assure the security of supply and preparedness planning and survey the effects of the energy market changes on security of supply. The goals are uninterrupted energy supply, ecological sustainability, and competitive pricing. (National Emergency Supply Agency n.d.a.)

Security of supply is planned to handle exceptional situations in normal operating conditions and in prolonged unusual situations including state of defense. The energy sector is central in assuring the security of supply. The companies are participating in the operations of NESA in sector specific pools. These pools coordinate, steer and monitor the preparedness of the sector. (National Emergency Supply Agency n.d.b.)

Electricity distribution is in the same pool with energy production and transmission system operators. The sector specific pool is assuring the preparedness of the sector and is actively developing sector´s preparedness. Regulation is setting requirements for the preparedness planning of DSO including Emergency Powers Act and Electricity Market Act (National Emergency Supply Agency n.d.c.).

7.3 European Commission Recommandations on Cyber Security on Energy Sector

The transformation of the power grid into a smart grid brings new risks. Energy systems are exposed to cyber-attacks and incidents which may endanger the security

of supply. Clean energy package includes legislative proposals to ensure secure development of the digital transformation. Risk preparedness regulation will include measures on cybersecurity which the member states should include in the risk assessment plans at the national level. Technical sector-specific rules for cyber security in form of network code are provided will set common minimum requirements for planning, monitoring, reporting and management of crisis. Steps have already been taken towards resiliency. Since the adoption of the European Cyber Security strategy in 2013, NIS Directive has been adopted in July 2016. (European Commission 2019.)

7.4 The Directive on Security of Network and Information systems (NIS Directive)

NIS directive is setting requirements on suppliers of essential services in different sectors, including the energy sector. Directive require the DSO to ensure the risk management of their networks and information systems. All cyber security incidents must be reported to the supervisory authority without undue delay if the incident is threatening the customer's security of supply. Directive is implemented as part of the national legislation. In Finland, each sector has different supervisory authority. The energy sector's authority is energy authority. (Energy Authority 2018.)

7.5 Network Codes of Electricity

European electricity networks are interconnected and therefore EU-wide rules are needed to manage the energy flows. These rules are called network codes. They are legally binding and govern all system operations and cross-border transactions of electricity exchange. (European Commission 2021.)

Network Code on Emergency and Restoration

European Commission Regulation (EU) 2017/2196 for network code on emergency and restoration entered into force in December 2017. The aim of this code is to set common rules to manage situations of emergency, blackout, and restoration. (Ibid.) This code obliges the transmission system operators to create preparedness and restoration plans for emergency and blackout situations. DSOs are among the

essential service providers who are obliged to implement the frequency protection requirements and assure a 24-hour operational capability of essential services. These abilities must be implemented latest mid-December 2022. (Siltala 2020.)

Network Code Cyber Security

An expert group called smart grid task force was assembled in 2017 after the communication of the commission of Clean Energy for All Europeans (COM/2016/0860 final) aiming to prepare an initial proposal for the cyber security network code. The final report of the group was published in 2019, and a formal consultation process is ongoing. (Smart Grid Task Force Expert Group 2 2019.) After entering into force, the network code will be implemented in national regulation. The recommended structure for the network code is presented in Figure 15.

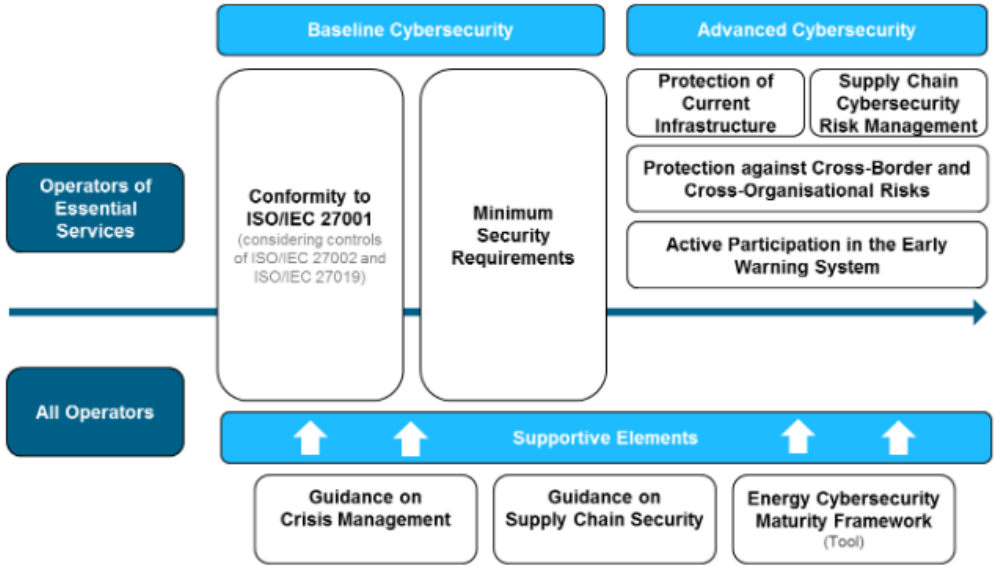


Figure 15. Smart Grid Task Force Recommendation for the Cybersecurity Network Code. (Smart Grid Task Force Expert Group 2 2019, 15.)

The recommendations can be separated into two categories, baseline cybersecurity and advanced cybersecurity. Baseline cybersecurity includes two main pillars, which are conformity to ISO/IEC 27001 and minimum security requirements.

1. Conformity to ISO/IEC 27001: Each operator of essential services should comply with the ISO/IEC 27001 standard requirements supplemented by the controls of ISO/IEC 27002 and ISO/IEC 27019.

2. Minimum cybersecurity requirements: A European wide common security baseline should be achieved. To achieve this target, internationally recognized standards must be used. In addition to the ISO/IEC 27001, the security-by-design thinking requires the implementation of additional electricity sector specific standards presented in Figure 16. ISO/IEC 27019 targets the cybersecurity management of the energy sector, IEC 62443 targets the industrial automation systems and IEC 62351 targets the security of energy sector communications. (Ibid., 19, 27.)

Advanced cybersecurity includes four areas. The areas are protection of current infrastructure, supply chain cybersecurity risk management, protection against cross-border and cross-organisational risks and active participation in an early warning system.

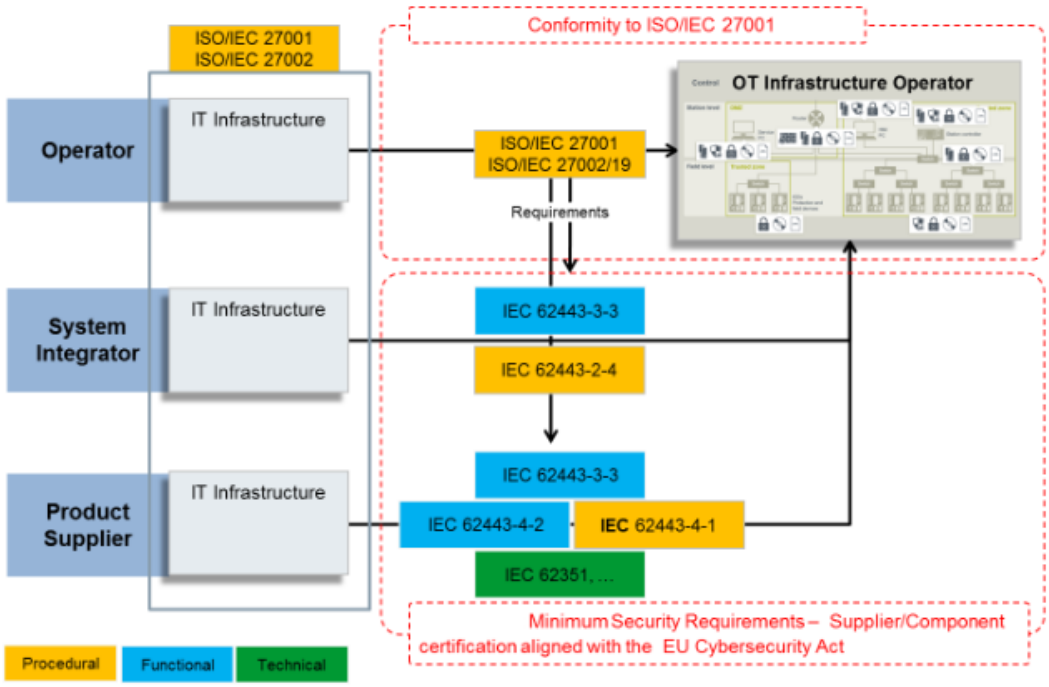


Figure 16. Smart Grid Task Force Proposal for Minimum Security Requirements (Smart Grid Task Force Expert Group 2 2019 19.)

7.6 Electricity Market Act

Electricity market act (588/2013) 28 § sets requirements to the DSOs to prepare for different abnormal situations and take part in the preparedness planning. Preparedness plan must be updated every three years. The plan must be provided to

the Energy Authority which can require changes if the requirements of the electricity market act are not fulfilled. (Energy Authority n.d.b.)

A change was made in 2018 in the law to implement the requirements of directive on security of network and information systems (NIS directive). The section 29 a § oblige the DSOs to handle the risks of network and information systems, the methodology must be expressed in written form and described in the preparedness plan. (ibid.)

7.7 Statutory Requirements

The conciousness of the importance of the cyber security is widespread. For the critical infrastructure, the NIS directive published in 2018 is the main directive setting requirements. The regulation of the DSOs' has been altered at the European level to include the requirements to handle the information security risks. Also an obligation to report in case of an information security incident has been instaured. The regulation has been implemented in the national law and mandatory requirements are set in the DSO's preparedness planning. The regulatory requirements are summarised in Table 1. The content of the table has been translated from the Finnish law by the author. The Finnish version can be found in Finlex service, law 2013/588.

Table 1. The Regulation of the DSO´s Concerning Cyber Security (L 9.8.2013/588, 19 §, 28 §, 29 a § ,75 b §)

Law/Section/Clause	Description	Details/Supervisory Authority
Electricity Market Act (2013/588) **19 § 2 - 3 Network development obligation**	Distribution network must be planned and maintained so that 2) the functioning of distribution network and distribution network services are assured when normal expectable climate based, mechanical origin failure or other external disturbance occurs. 3) the functioning of distribution network and distribution network services are ensured in the disturbances of the normal operating conditions and in unusual conditions stated in the Emergency Powers Act (2011/1552).	

Electricity Market Act (2013/588) **28 § Network holder's preparedness planning**	Network holder must be prepared with adequate planning to the disturbances of the normal operating conditions, to the regulation of energy in case of electric system failures and to the unusual conditions stated in the Emergency Powers Act. Network holder must draft a preparedness plan and take part in contingency planning. The preparedness plan must be updated at least every three years and if the conditions change considerably. More detailed requirements concerning the preparedness plan may be given by a governmental degree.	Additional requirements are given by the energy authority as follows. The preparedness plans must be delivered to the Energy Authority. Energy Authority may, within six months of the reception of the plan, require supplementing, if the plan does not comply with the requirements. In addition to the plan a questionnaire called Sähkökotka is obligatory to answer and provide the answers together with the preparedness plan to the Energy Authority. The answers of the questionnaire form a development plan for the organization. (Energy Authority n.d.b.)
Electricity Market Act (2013/588) **29 a § Obligation of network holder to manage the risks of the network and information systems and report information security related incidents**	Network holder must manage the risks concerning the networks and information systems in use. Network holder must notify without undue delay the Energy Authority of an incident in the networks or information systems which may endanger the security of supply to a significant extent. If the disclosure of the incident is of public interest, Energy Authority may disclose or oblige the service provider to disclose the information after having heard the service provider. The energy authority must evaluate if the incident would affect the other European Union countries and if necessary, notify the other member states. Energy authority may give more detailed orders of when the incident is important, and concerning the content, form and delivered.	The network holders are requested to report each occurred or potential incident which have or may have affected the security of supply to Energy Authority regardless of the statement of the law of significant incident. (Energy Authority 2018).
Electricity Market Act (2013/588) **75 b § Data management related to the electricity market processes**	Energy sector organization must maintain and develop their activities and services related to the market processes, to the imbalance settlement and to the imbalance settlement related processes so that the services are efficient, the	

	information security is adequate, and the usability is easy. These are the conditions to guarantee an adequate and efficient energy market.	

Statutory cyber security requirements today are derived from NIS directive and are implemented in the Electricity Market Act. These are the preparedness planning, information security risk management and obligation to report if an incident occurs which would or have threatened the security of supply.

The preparedness planning requires completion of a questionnaire which provides the organization with a development plan. Two network codes will be setting requirements in the future, especially the cyber security network code. Reasonable level for the cyber security for a DSO today is depending on the organization's own ambition of responsibility, exigency of quality and resiliency since the requirements of the information security and risk management methodology are in general level and not expressed in detail in the lawful requirements. The actual state enables variations of the cyber security maturity among the DSOs.

8 Research

The research is divided in three phases starting from **PESTLE analysis** in which the theoretical background is analysed followed by **interviewing key specialists**, analysing the specialist´s answers to create scenarios for Delphi panel, **creating and conducting a Delphi panel** and finally analysing the Delphi panel results to create the cyber security roadmap proposal. Each phase is presented in detail in the following subchapters and the results in chapter 9.

8.1 Synthesis of Theoretical Background and Topics for the Interview

The future cyber security prospects for a DSO can be either desirable or unwanted. fiveThe desirable future can be reached if the prevailing situational picture is known, including the past events combined with the trends and known unknowns.

In the previous chapters the threats, trends and possible scenarios has been gathered from recent sources to get a situational picture of the DSO´s cyber environment dynamics. The approach is mainly national and European except for the global risks. The actual and forthcoming regulation was presented in chapter 8. In this chapter a synthesis of distinct factors gathered from previous chapters is presented using PESTLE analysis.

PESTLE assessment has been chosen as a tool to understand the key factors of the changing business environment of the commissioner. An analysis of the landscape is done through each PESTLE factor. The outcome of this analysis are the topics which will be compared to the topics raising from the interviews. Theoretical background content of each PESTLE factor is visualised in figures included in each sub-chapter and in Appendix 1. The summary of the selected topics is presented in chapter 8.1.7.

8.1.1 Political

The political factors collected from the theoretical background are presented in Figure 17. The fluctuating geopolitical situation is the first important political factor. Geopolitics affect the nation states' cyber activity, the availability of the goods and the functioning of the logistic chains. The legislation differs in each country and the requirement of a nation bypasses the requirements of the customers. The country of origin and the risks related to it should be considered in the purchases. The same goes for the logistics chains.

The smart grid task force recommendations should be considered as potential future requirements. DSO´s future role will be to offer the platform for the market actors to enable more flexibility to the customers in their energy consumption. A smart and interconnected near real-time communication-based energy system will emerge requiring adequate data security measures to protect intelligent devices. Increase in energy communities and local electricity production could lead to lower consumption of energy and require investments to achieve the required future role. On the other hand, an increase in electric cars would increase consumption.

In October 2020, a large data breach occurred in Finland, in which sensitive personal data including health records of tens of thousands of customers was leaked and a

ransom was requested from each victim (The Guardian 2020). Until this breach, no major data breaches have occurred in Finland and the data security hasn´t been publicly under much attention. This case has increased the awareness of information security and several actions have been started at the national level to increase data and information security in the critical sectors. The outcome of these national level initiatives can result in increased requirements and auditing.

The profitability and the acceptable limits of DSO´s turnover is under constant discussions. There are pressures to regulate the DSO´s profitability which could have a negative impact on the incomes. On the other hand, the security of supply requires investments in the power grid. These factors are also economic and presented in the economical factor's summary in the next sub-chapter and in Figure 18.

From political factors four different topics are raised for the interviews. The topics are geopolitical changes, security of supply, DSO´s future role and data security requirements. Political factors have a vital role in DSOs business since the sector is very regulated.

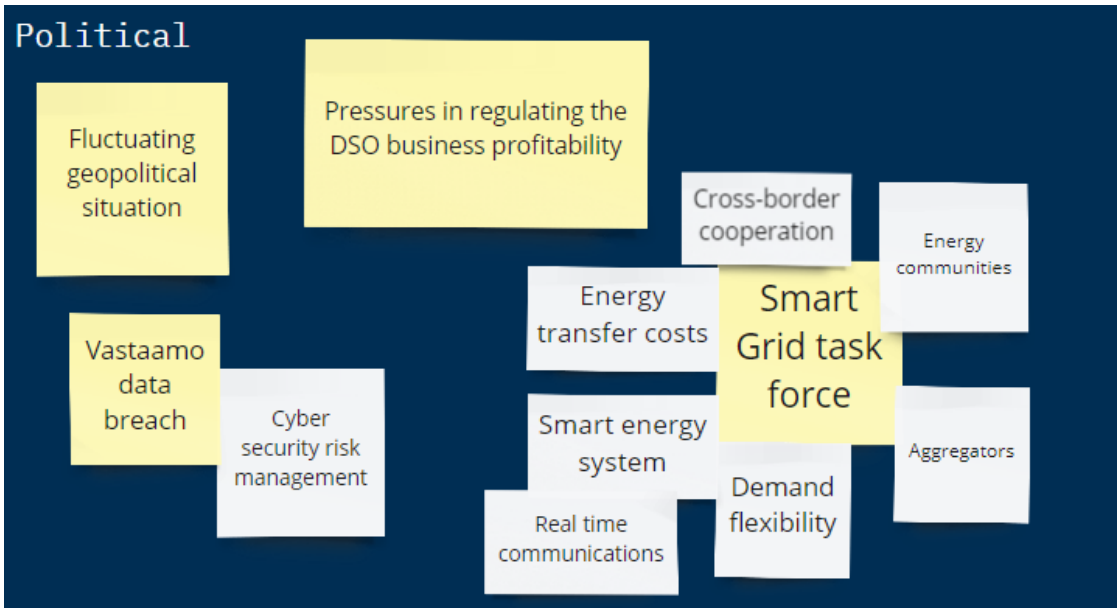


Figure 17. Political Factors from the Theoretical Background

8.1.2 Economic

The economic factors collected from the theoretical background are presented in Figure 18. Consumers are not only consuming but also producing energy. Energy communities could be even larger independent producers not buying energy, but DSO could have the obligation to offer the platform to transfer the produced energy to the grid, measure the production and enable the flexible services for the communities. Prosumerism could lead to lower consumption of energy meaning lower income for the DSO in the actual business context alongside with needs to make investments to achieve the future requirements of the platform for services. In the design of such an interconnected platform, cyber security must be carefully considered. The interconnectivity of the energy sector with the whole critical infrastructure is already important. In such a platform operator context cyber security will be increasingly important.

Due to the increasing demand and the fluctuating production with the use of greener energy sources, the cost of energy could increase for the customers. On the other hand, as mentioned in the political factors, DSO´s profitability could be reduced alongside with more investments required. Our lifestyle is changing including increasingly electrifying traffic, which will require more electricity. At the same time electric cars could present a large power bank which could be used to balance the fluctuating energy production.

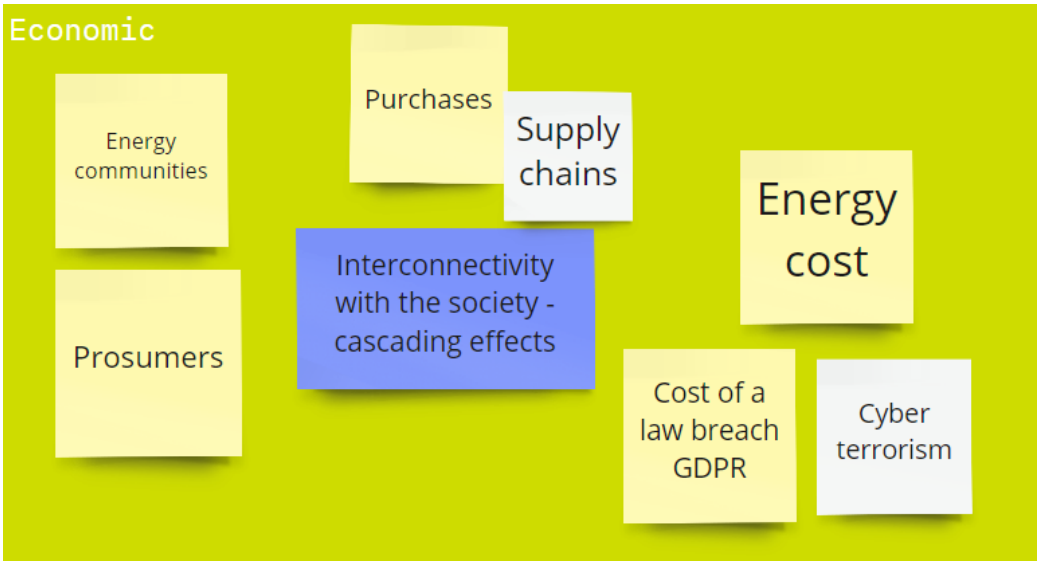


Figure 18. Economic Factors from the Theoretical Background

Global multinationals, public and private clouds and hyperscale computing are increasing their market share of the IT infrastructure. As digitalization advances more computing capacity will be needed for business services. When buying IT infrastructure, the global demand and availability of resources will affect prices. According to the International Data Corporation (IDC) COVID-19 has increased cloud adoption since the cloud-based business and consumer services increased during the lockdown. IDC estimates that the cloud services, both public and private, will continue to grow whereas non-cloud infrastructure investments will be less significant. (International Data Corporation 2020.)

The cost of law breaches and cybercrimes are factors which should be considered adequately when planning the future. Today an administrative fine for a data protection violation could be 20 million Euros or 4% of the company's turnover (Office of Data Protection Ombudsman 2020). According to Wilczek (2020) after IBM the average cost of a data breach is nearly 4 million US dollars. The loss of business and non-returning customers, information system downtimes, legal fines and reputational losses are the major factors when calculating the cost. More than half of the breaches during the year 2020 were perpetrated by malicious attackers. Human errors, information system problems and misconfigured cloud environments are the other principal factors leading to data breach. Half of the malicious attacks can be attributed to extortionists while 13% of the attacks were caused by hacktivists and nation states.

From the economic factors the topics for the interviews are the economic impacts of the prosumerism, future energy consumption needs, and cloud adoption for business services. These factors are connected to political factors as well.

8.1.3 Socio-cultural

The socio-cultural topics selected are the influence of social media and always on society, the dependency of technology and smaller households. The other factors presented in Figure 19 were already discussed in the political or economic analysis.

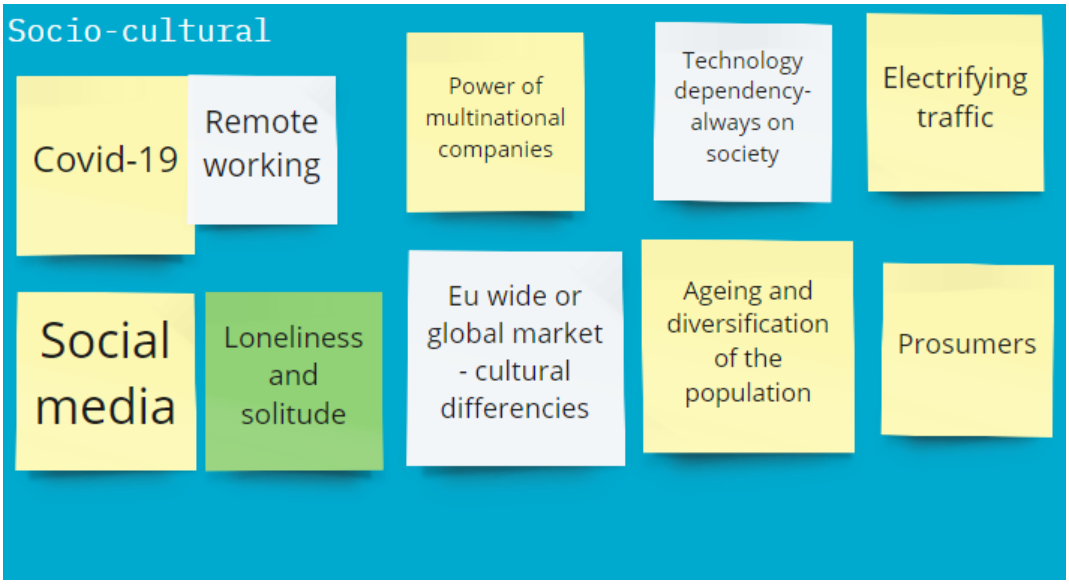


Figure 19. Socio-cultural Factors from the Theoretical Background

The population is ageing, diversifying and being increasingly alone but connected with others with online services and social media. These services are global, and the AI is increasingly used to adapt to the content of the services based on people's behaviours and predilections.

COVID-19 has imposed remote working as a new normal and each consumer should be aware and responsible for their personal home devices security. For most of the employees it is via the home connectivity infrastructure that the business networks are connected to. Assuring the cyber security in these exceptional conditions is challenging since the number of phishing and scamming was estimated to increase significantly already during 2020 as seen in Figure 20. The lockdown has highlighted the dependency of technology and the high availability needs for online services. To enable this always on society, an uninterrupted energy system is an absolute need.

The connectivity removes the barriers of the ancient world where the market was local or national. New actors can enter the Finnish markets since the online world is not limited by nation´s physical frontiers.

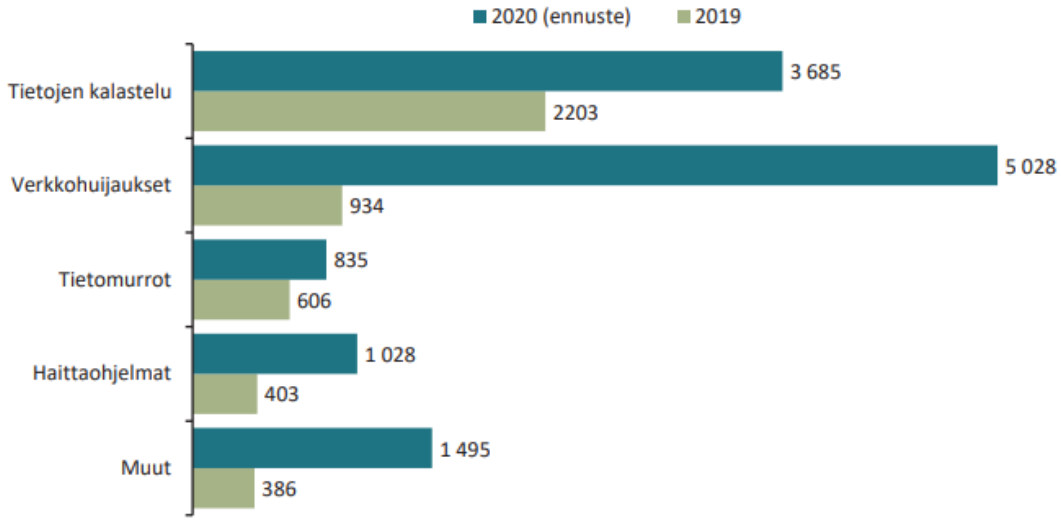


Figure 20. Number of Cyber Security occurrences reported to NCSC-FI years 2019 and estimation for year 2020 (Mattila, Ali-Yrkkö and Seppälä, 4 after NCSC-FI)

8.1.4 Technological

As described in the cyber environment of Elenia, the energy sector supplier and partner networks are vast. So is the number of devices deployed into the infrastructure. The implementation of the security controls of these devices could be inadequate. In addition to the hardware and software threats, the human factor is important. The lifecycle of the software in critical infrastructure is long which requires persistent attention to the new vulnerabilities and threats. Appropriate knowledge is needed to understand the underlying mechanisms, interconnectivity and impacts of the threats to deduce the right and adequate risk level.

Recent technologies like artificial intelligence and quantum computing offer possibilities to enhance business operations but at the same, if not used for good purposes, would endanger business continuity. The criminals are also taking advantage of these technologies. The future interconnected smart grid requires reliable cyber security controls for each device and for the always on connections to

ensure the security of supply and the possibility to consume the right energy products at the right time for the customers.

Hyperscale computing and cloud service providers are increasing their market share. These actors are global and are not driving the interests of the Finnish national security of supply. The digital self-sufficiency could be endangered with such global cloud computing trends.

The technological factors raised for the theoretical background are presented in Figure 21. The selected topics for the interviews are cyber environment partnerships, smart grid, energy system lifecycle, new technologies like AI and quantum computing and digital self-sufficiency. Technological possibilities and threats are one of the key areas in the future.

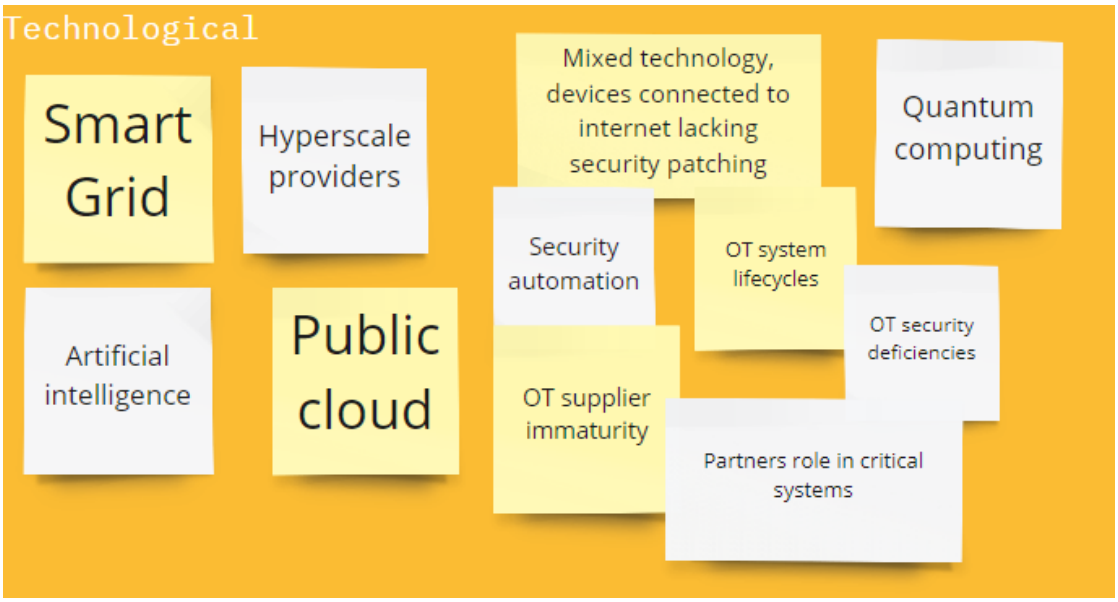


Figure 21. Technological Factors from the Theoretical Background

8.1.5 Legal

As described in Figure 22 statutory cyber security requirements today are derived from NIS directive and are implemented in the Electricity Market Act. Two network codes will be setting requirements in the future, these are Network Code for

Emergency and restoration and Network code on cyber security. The selected factor is the changes in the regulation.

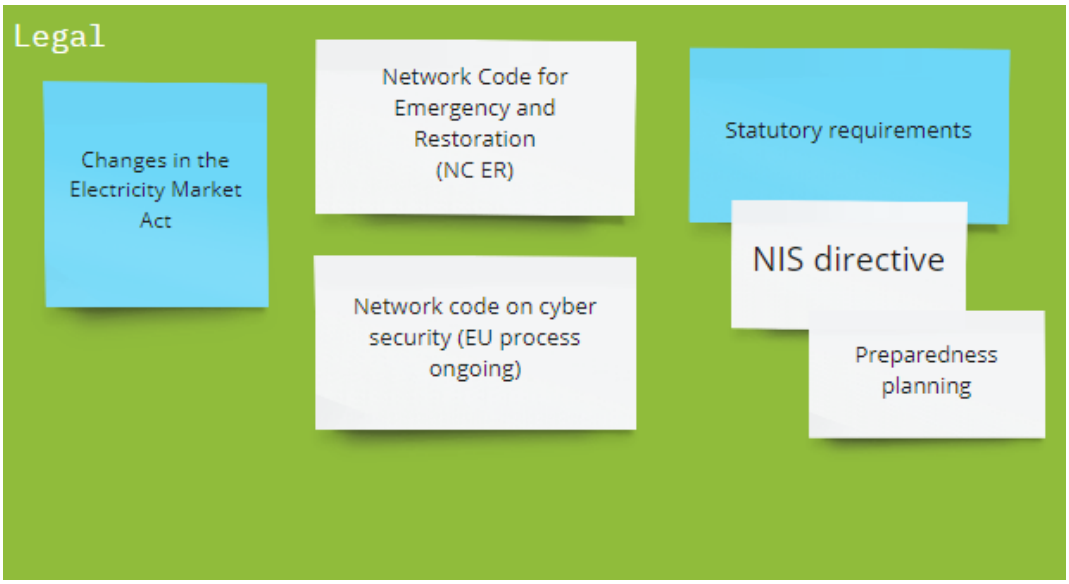


Figure 22. Legal Factors from the Theoretical Background

8.1.6 Environmental

The climate change and risks related to the degrading conditions of our planet´s biodiversity is considered as the most important risks globally. Cyber risks come right after the climate risks. Green and ecological energy production require power balancing technologies like batteries to guarantee the security of supply. The batteries are new services and require new partnerships for the DSOs. At the same time the overhead power lines are replaced by the underground cables and the power grid is less vulnerable to the meteorological phenomena meaning less outage management work for the partners. From the factors presented in Figure 23 the chosen environmental factors as topics are ecological reconstruction, social responsibility, and green/removable energy.

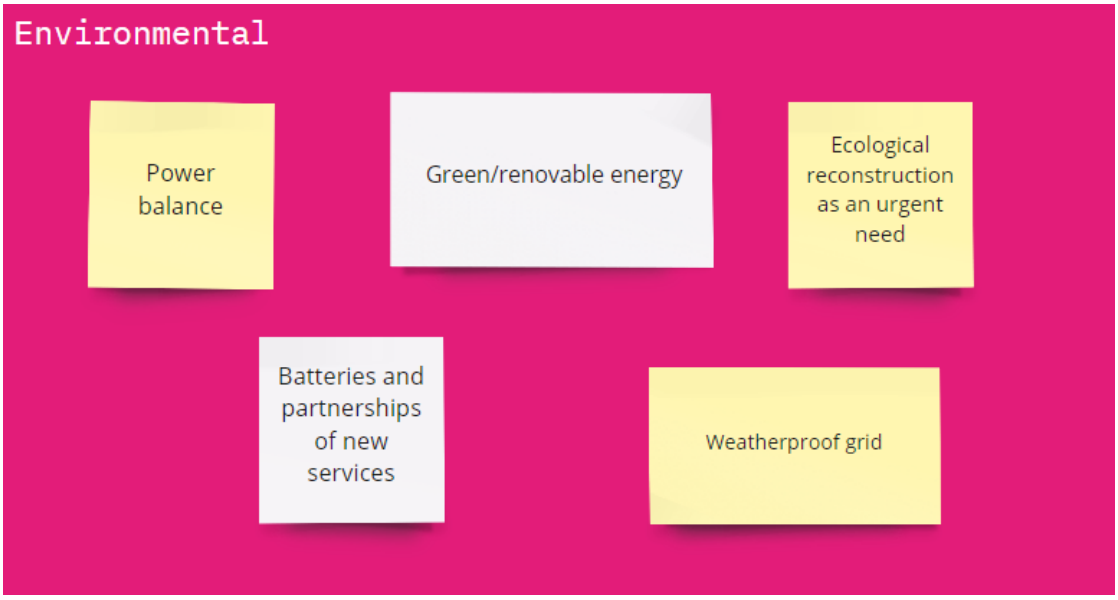


Figure 23. Environmental Factors from the Theoretical Background

COVID-19 has captured people's attention and the climate change worry may not have been of the first concern during the last year. According to, CRED people´s capacity to worry is limited. This capacity can be referred to as a finite pool of worry. People are more worried about the threats presented than near future risks. Also, if one worry grows in importance, the other risks are not perceived as important and are getting less attention. (Center for Research on Environmental Decisions 2009.) This is important to understand when considering the risks during the pandemic situation.

According to Dufva, Hellström, Hietaniemi, Hämäläinen, Ikäheimo, Lähdemäki-Pekkinen, Poussa, Solovjew-Wartiovaara, Vataja & Wäyrynen (2020) the COVID-19 crisis is giving hope to the ecological state of our planet if we direct the post-pandemic reconstruction efforts to ecologically sustainable choices. The values of the people have changed, and many have rediscovered nature as an important source of wellbeing during the crisis.

New week signals have appeared during the pandemic. These are cottage fever in Finland. People have bought 20% more cottages in 2020 than the year before. New York City is building streets for pedestrians and bicycles. Environmental migration is no longer attributed to the disadvantaged; the forest fires and the increasingly hotter climate of the western coast of the United States has started migration. In Uganda

houses are built with ecological tiles made of recycled plastic bottles filled with sand and soil. Bottles are not treated or crushed before use which makes this building material emission free. (Ibid.)

8.1.7 Summary of Selected Factors

The selected factors from the different PESTLE analysis topics from chapters 8.1.1 to 8.1.6 are assembled in Table 2. These factors are presented as the possible change driving forces in the interviews and evaluated against the interviewee's opinions when defining the Delphi panel scenarios.

Table 2. Topics for the Interviews

Topic	Factor
Political	Geopolitical Changes
Political	The Security of Supply
Political	DSO´s role in the Future
Political	Data and Information Security Requirements
Economic	Prosumerism
Economic	Future Energy Consumption Needs
Economic	Cloud Adoption for Business Services
Socio-cultural	Influence of social media and Always on Society
Socio-cultural	The Dependency of Technology
Socio-cultural	Smaller Households
Technological	Cyber Environment Partnerships
Technological	Smart Grid
Technological	Energy System Lifecycles
Technological	New technologies like AI and Quantum Computing
Technological	Digital Self-sufficiency
Legal	Changes in Regulation
Environmental	Ecological Reconstruction
Environmental	Social Responsibility
Environmental	Green/removable energy

8.2 Interviews

The interviewees were selected from the energy sector. The criteria for the choice were several years' experience and knowledge of both energy distribution and cyber security. The interviewees were contacted by phone. The interviewees were provided with the questions before the interviews by email, including the change driving forces presented in Table 2 of the previous chapter and threats collected form the theoretical background. The questionnaire used and the threats supplied beforehand are visible in Appendix 2.

Two persons (N=2) were selected from author´s business acquaintances based on their knowledge, extensive experience, and role in strategic development including the cyber security aspects. The first interviewee was a Chief Information Security Officer of a DSO and the second a System Developer of a DSO working with strategic business projects.

The interviewees will be referenced by the designations CISO and System Developer. The questions were provided to the interviewees before the actual interview by email several days ahead.

The interviews were held using online meeting facilities due to the pandemic restrictions. The interviews were recorded and transcribed, a summary of each interview is presented in Appendices 3 and 4.

The questions were the same in both interviews:

1. What are the changes occurring in the energy sector which will clearly influence the future of electricity distribution?
2. Which weak signals visible today will significantly affect electricity distribution in the future?
3. Which of the changes you selected will influence the energy sector's cyber security 3 to 5 years from now?
    1. Do you think that the influence of these changes will be visible only later and if so, when?
4. Which factors are emphasized in cyber security?
5. Which cyber security threats are the most significant in the electricity distribution business?
    1. Choose the most significant threats and explain the reason for your answer.
    2. Set the threats in order and give a reason for your answer

Both interviewees mentioned the increased interconnectivity of the systems as a change influencing the future. According to CISO, one actor with missing security controls may endanger the business operations of the others including the Finland´s electricity transmission system. System Developer puts emphasis on the change where the actual old segregated systems will be connected to the cloud, and the data would be widely used jointly with decisions made by AI. The decisions made by the AI could be fed back to the system and could control the entire process in the future. The development pace of technology and electronics is fast, and their lifecycle is at most 20 years. Threats can be handled in newly implemented systems whereas assuring the security, correct use of AI and the right business operations of this interconnected system, is the most important question to solve concerning the cyber security after System Developer. This new complex system could control the whole electricity network system in the future.

The energy communities, electric cars, and increase at some points of small-scale production are also recognised as future changes by both interviewees. According to System Developer the future and the extent of the implementation of energy communities and small-scale production are dependent on the regulatory changes and the energy prices whereas CISO thinks that energy communities may endanger the DSOs monopoly status. Concerning the regulatory changes, CISO thinks that the regulation will increase, and the smaller DSOs may not be able to cope with the new requirements. Concerning the electric cars CISO appointed a possibility to use them as a reserve battery since the energy storage technologies and the possible use of the hydrogen is yet to come. CISO also stresses the importance of cyber security of the market actors offering services and infrastructure for electric cars. If security is not implemented to the new arising services, many vulnerable devices connected to the cloud may emerge. Vulnerabilities of the interconnections, for example unprotected clouds, could enable the controlling of the household’s systems at a distance. This could affect the system largely and cause important system failures. The responsibility questions are important. According to System Developer the venue of the electric cars is more certain than the increase of small-scale production and energy communities. Both recognise these as possible weak signals and yet System Developer stresses the importance of starting to prepare for this likely future

since the electricity networks' lifecycles are long and the future-proof network requires planning.

Another weak signal according to CISO is COVID-19, which has increased people's interest in rural areas. The summer cottages or houses could be equipped with remotely controllable solutions like geothermal heating. If this trend continues, the System Developer's thoughts about the peak loads caused by the households in rural areas when charging the electric car upon arrival at home, are the future.

The extensive use of data collected from the electricity grid, use of different sensors and components will increase according to System Developer. New technologies would enable business development, but data security or copyright problems could emerge, limiting the business possibilities. The use of artificial intelligence is increasing but the limits and rules to use its capabilities are not yet defined. This cyberphysicality is also mentioned by CISO. CISO emphasizes the interconnectivity of the cyber and physical world where automation is controlling the physical world's devices. Therefore, cyber security is not only a technical question including network and information system security, but physical security is equally important.

Both interviewees recognise the significant role of partners and suppliers. System Developer emphasizes lifecycles. If the system is not bought as an overall service, it is challenging to handle the separate lifecycles of the different vendors if the organization doesn´t want a vendor lock-in situation. How to guarantee the security of the entire system if one part is not under support contract anymore. CISO stresses that cyber security should be considered starting from the contract requirements with a new partner. The instructions and the awareness of security should be considered carefully in the field operations since the partners are working every day in the field and are continuously in contact with the cyberphysicality. The components affecting the cyber security of the distribution networks are geographically scattered around the distribution network and the contractors are working closer than the DSO personnel with these components. Due to this physical geographical dispersion of the electricity network, a possible malicious actor has plenty of time to work before being noticed.

Both mentions also that the lifecycles of the investments are playing a role in this complex interconnected system. CISO emphasizes the possibility to divest the obsolete systems more often than the actual regulation permits. There are vulnerable systems in the field where no security is implemented, especially devices on layers 0 and 1 after Purdue Enterprise Reference Architecture. The security of these devices should be assured with other controls, for example physical controls.

The separation of IT and OT systems is questioned by both. CISO thinks that OT systems are not so segregated as they are thought to be. The business requirements are directing the OT systems towards the cloud since the systems fulfilling the business development requirements can no longer be implemented in the on-premises data centres. The clouds are proposing the needed machine learning capabilities. The questions are, how and under what conditions the cloud can be used for the OT systems. Even if in the private clouds the tenants are separated, there might be vulnerabilities allowing access from one tenant to another. System Developer thinks that if the OT has been so far a system controlling the operations of the transmission network, tomorrow with the AI combined, it may be expanded to a maintenance system. The process could be developed further, and the system could also create work orders and decide about the necessary investments. How to separate, what is IT and OT in this probable future scenario.

AMR meters are mentioned by both as already being an important cyber security threat. The meters are controlled using interfaces at a distance and can make decisions unattended. To handle the large quantity of information, clouds are used.

CISO also mentioned data and telecommunications security, the younger generation and management's commitment as threats. DSOs rely on data and telecommunications operated by telecommunication operators and not controlled by the companies themselves. Are the communications end-to-end encrypted or are there possibilities to interfere or eavesdrop on these connections? This is a black box today. Concerning the young generation, the basics of the TCP/IP are not known, and they are willing to use mobile phones for everything. The segregated systems are disappearing together with the older generation who understood the risks and reasons related to the accessible anywhere and interconnected systems.

8.2.1 Synthesis and Analysis of the Interviews

To collect the contributory factors of the cyber security of DSOs, the interviewees answers were transposed in a spreadsheet, analysed, condensed, and categorised in sub and main categories. As a result of the analysis, 37 different condensed meanings were recognised. The subcategory is the PESTLE factor, and the main categories were defined inductively by the author during the analysis process. The condensed meanings with their subcategories and main category are presented in Table 3. One condensed meaning could be included in several PESTLE subcategories.

Table 3. Contributory Factors of the Cyber Security of DSOs after Interviews

Condensed Meaning	Subcategories (PESTLE)	Main Category
Increased system interconnectivity	Primary: Technological: Smart Grid Socio-cultural: The Dependency of Technology Political: Security of Supply	Interconnectivity
IT and OT converge	Technological: Smart Grid	Interconnectivity
Data and telecommunications security	Socio-cultural: The Dependency of Technology	Interconnectivity
Assuring the security of interconnected system	Primary: Political: Security of Supply Political: Data and Information Security Requirements	Interconnectivity
Interconnectivity of the cyber and physical world, automation controlling the physical world's devices. Create work orders or decide the investments.	Technological: Smart Grid	Interconnectivity (Cyber physicality)
Future-proof grid	Primary: Technological: Smart Grid Environmental: Ecological Reconstruction Environmental: Social Responsibility Environmental: Green/removable Energy	New services and products
Lifecycle of the grid	Technological: Energy System Lifecycles	New services and products
Weak signal: increase in habitants in rural areas	Socio-cultural: Smaller Households	New services and products
Younger generation	Socio-cultural: Influence of social media and Always on Society	New services and products
Responsibility questions	DSOs future role	Regulation/policies/principles

Weak signal: Energy communities	Primary: Economic: Prosumers Political: DSO´s Role in the Future Economic: Future Energy Consumption Needs	New services and products
Weak signal: Small-scale production	Primary: Economic: Prosumers Political: DSO´s Role in the Future Economic: Future Energy Consumption Needs	New services and products
Electric cars	Primary: Economic: Future Energy Consumption Needs Economic: Prosumerism Environmental: Ecological Reconstruction Environmental: Green/removable Energy	New services and products
Reserve battery from electric cars	Primary: Economic: Future Energy Consumption Needs Environmental: Ecological Reconstruction Environmental: Green/removable Energy	New services and products
Hydrogen	Primary: Economic: Future Energy Consumption Needs Environmental: Ecological Reconstruction Environmental: Green/removable Energy	New services and products
Data used jointly with AI	Primary: Technological: New technologies like AI and Quantum Computing Political: Data and Information Security Requirements	New services and products (AI)
AI making decisions and controlling the electricity network system	Primary: Technological: New technologies like AI and Quantum Computing Political: Data and Information Security Requirements	New services and products (AI)
AMR meters, use of clouds	Economic: Cloud Adoption for Business Services	New services and products (AMR meters)
Old segregated systems connected to the cloud	Economic: Cloud Adoption for Business Services	New services and products (Cloud)
New vulnerable services connected to the cloud	Economic: Cloud Adoption for Business Services	New services and products (Cloud)

Requirements for the use of cloud for the OT systems	Economic: Cloud Adoption for Business Services	New services and products (Cloud)
Significant role of partners and suppliers	Technological: Cyber Environment Partnerships	Partners/supplier
Contract requirements with a new partner	Technological: Cyber Environment Partnerships	Partners/supplier
Security awareness in the field operations	Technological: Cyber Environment Partnerships	Partners/supplier
Contractors working closely with field components	Technological: Cyber Environment Partnerships	Partners/supplier
Rules using AI	Primary: Political: Data and Information Security Requirements Technological: New technologies like AI and Quantum Computing	Regulation/policies/principles
Security during the entire lifecycle, when one part is not under support contract anymore	Technological: Energy System Lifecycles	Regulation/policies/principles
Lifecycles of the investments	Primary: Technological: Energy System Lifecycles Legal: Changes in Regulation	Regulation/policies/principles
Cyber security includes technical and physical security	Technological: Cyber Environment Partnerships	Regulation/policies/principles
Vulnerable systems scattered geographically in the field with no security implemented	Political: Security of Supply	Regulation/policies/principles
Increasing regulation	Primary: Political: Data and Information Security Requirements Political: Geopolitical Changes Political: DSO´s Role in the Future Legal: Changes in Regulation Environmental: Social Responsibility	Regulation/policies/principles
Smaller DSOs difficulties to cope with regulation	Political: DSOs future role	Regulation/policies/principles
Missing security controls endangering the entire system	Political: Security of Supply	Regulation/policies/principles
Data security or copyright problems	Primary: Political: Data and Information Security Requirements Technological: Digital Self-sufficiency	Regulation/policies/principles
Management's commitment	Political: Data and Information Security Requirements	Regulation/policies/principles
Regulatory changes affecting energy prices	Primary: Legal: Changes in Regulation Political: DSO´s Role in the Future Environmental: Social Responsibility	Regulation/policies/principles

As described in Figure 24 all PESTLE factors are covered in the answers. The political and technological aspects are emphasized alongside future energy consumption needs, the raise of green and renewable energy and cloud adoption for business services.

Figure 24. Number of Condensed Meanings in different Subcategories by PESTLE Category

Four main categories were recognised in the analysis. First is the **interconnectivity of the systems** including OT and IT and the convergence of cyber and physical worlds. Second category are the **new services and products** including future proof grid, use of AI and cloud, smart AMR meters and new rising customer needs. The third category is **partners and suppliers** whose vital role in the daily DSO activities was emphasized. The fourth category is **regulation, security policies and principles** including the areas where an energy sector national level regulation or DSO internal policy might or should be implemented or is already under preparation. The distribution of the condensed meanings by main category is depicted in Figure 25.

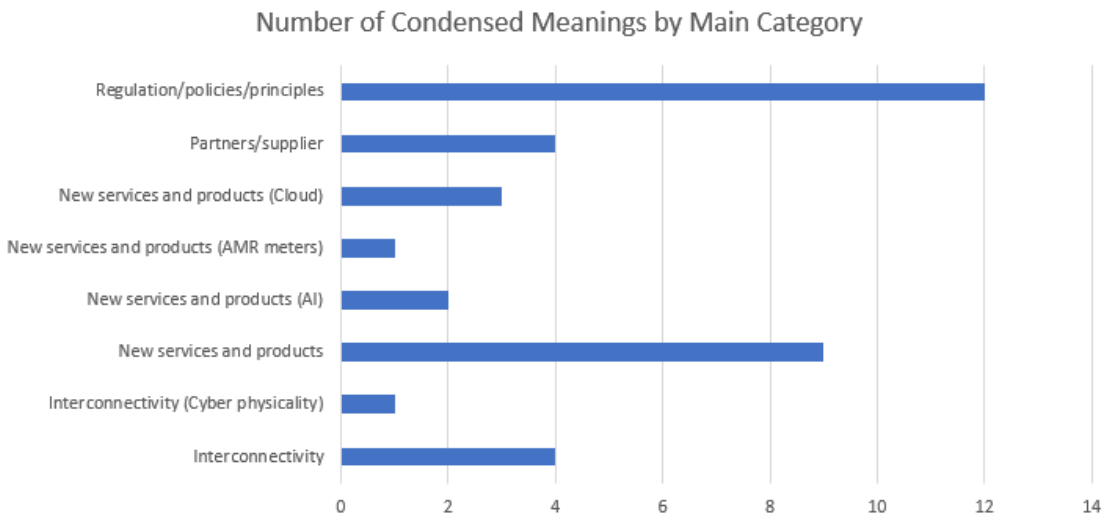


Figure 25. Number of Condensed Meanings by Main Category

8.3 Delphi Panel Construction and Panellists

The scenarios for a single round Delphi panel were defined based on the analysis of the interviews. The panelists were selected from the energy organizations, energy authorities and from the research & development field. Cyber security experts were also invited to take part in the panel. The author contacted the panelists by email or by phone to enquire about the willingness to take part in foreseeing the future of the cyber security of the energy supply. eDelphi online program was used to conduct the panel. The questions of the panel are presented in Appendix 5. Each participant received a personal invitation email to the panel including a personal link to the program. The author was in the role of the panel manager and did not answer the questions by herself. After the first week of the panel, a summary of the answers was sent to the panelists to emphasize the consensus and dissensus points at that time and to invite the panelists to re-evaluate their positions and elaborate their comments after taking a closer look on the opinions of the other panelists. The communications sent to panelists are presented in the appendices. Appendix 6 is the invitation to the panel and Appendix 7 is the email sent at mid-point of the panel.

The Delphi panel conduction started with the construction of the questions based on the main and subcategories from the interviews and the realization of the questions

in the eDelphi tool. The panel was named *Electrifying Life - The future of cyber security in energy distribution.* It took time to get familiar with the eDelphi tool and choose the right question types from various possibilities. Creating the content of the questions required a lot of reflection since the number of questions must be limited and at the same time the questions must be pertinent to collect as meaningful arguments from the panellists as possible. The aim of the panel is not to reach consensus. The questions were created iteratively: energy distribution and market specialists from Elenia were consulted in the creation process as well as the Delphi studies' tutors and Elenia's management team. Initially four questions were constructed, and one question was added at the mid-point of the panel.

Based on the results of the interviews four probable future scenarios including a future thesis were created. When creating the questions, it was important to keep in mind that the main categories raised from the interviews are presenting a possible state of the energy sector in the future. Both successful, desirable, and undesirable futures were presented in the questions. Detailed content of each question is presented in Appendix 5.

In addition to the questions, notices were added on the welcome page of the panel in eDelphi. The notices included the time schedule of the panel, a welcome message and information about organizations taking part in the panel.

At the same time with the scenario construction process the panellists were chosen and contacted individually. The panellists represented both the interest and expertise groups. As presented in Figure 26 the panellists' interest groups were authorities, energy sector, research & development, and corporations. The expertise categories were energy sector and cyber security. For anonymity reasons the names or organizations of the panellist will not be shown. 22 persons were sent the invitation, three of the invited panellists didn´t take part (**N=19)**.

	Energy Sector	Cyber Security
authorities	☑	☑
energy sector	☑	☑
research & development	☑	☑
corporations	☑	☑

Figure 26. The Interest and Expertise Categories of the Panellists

The panellists were sent two communications when the panel opened: an invitation email from the author and a personal link to the panel from the eDelphi tool. The content of these communications is visible in Appendix 6. In the invitation email the iterative process of Delphi was emphasized. The aim is to return regularly to the panel to read the arguments of the others, write new arguments and reflect own answer, should it be changed. The panel was open for 14 days and panellist had the possibility to argument and change their opinions during that time. The participation was anonymous. At the mid-point of the panel a brief status was sent to the panellists encouraging to review the arguments of others and revise own answer. The email sent is visible in Appendix 7. At mid-point, a new question was also added where a new scenario concerning creation of a digital twin was introduced. Also, a new question was added in the comments of question number 1: How important is it to ensure the cyber security on the energy sector?

eDelphi tool includes reporting capabilities. Live2D question type includes real time observation of the results. As depicted in Figure 27 the comments are directly positioned in a four square in descending order by the first criteria of the question, in this panel probability. The reports can be filtered by expertise and downloaded to a file in PDF, csv or png formats.

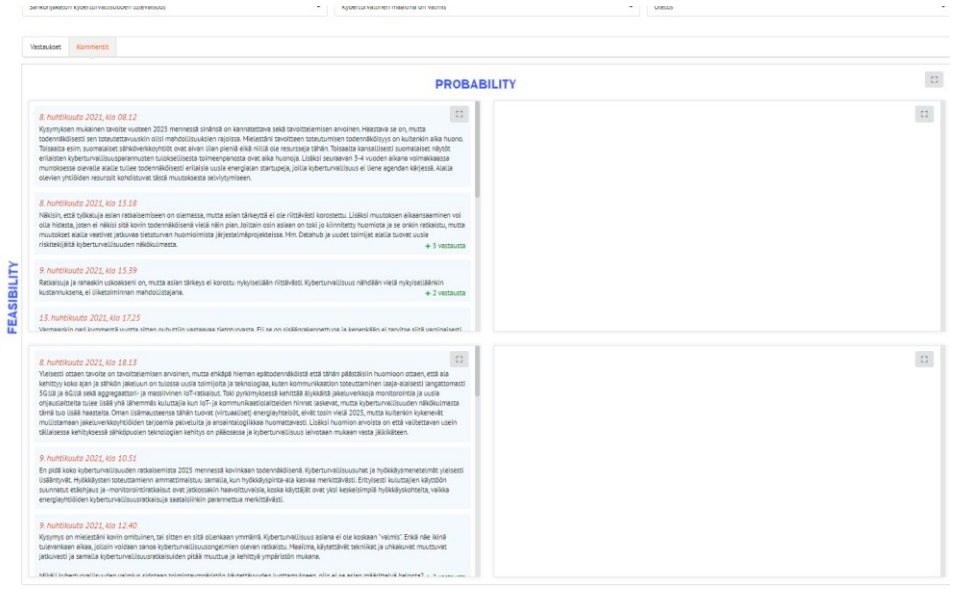


Figure 27. eDelphi Live2D Question Comment Reporting View

9 Results

Results of this thesis consist of analysis of the Delphi panel results and the regulatory environment of DSO. The research questions are answered based on these two analyses and a proposal for cyber security development areas is given to the commissioner.

9.1 Delphi Panel Results

The results of the panel represent the opinions of the panelists concerning the most important characteristics, threats, requirements, and options to solve cyber security in the energy sector. Results are analyzed based on the eDelphi visual diagrams and analysis of the opinions. The analysis produced condensed meanings and inclusive categorization of main category and a solution category. Each question is analyzed individually in this chapter and finally a roadmap proposal is made.

Three different question types were used with different Likert scales. In questions 1 and 2 the dimensions to be evaluated were probability and feasibility on a seven-step percentage scale from < 10% to > 90%. This question type in eDelphi is Live2D.

As Figure 28 represents probable is representing possibility and improbable impossibility. Feasibility represents realism.

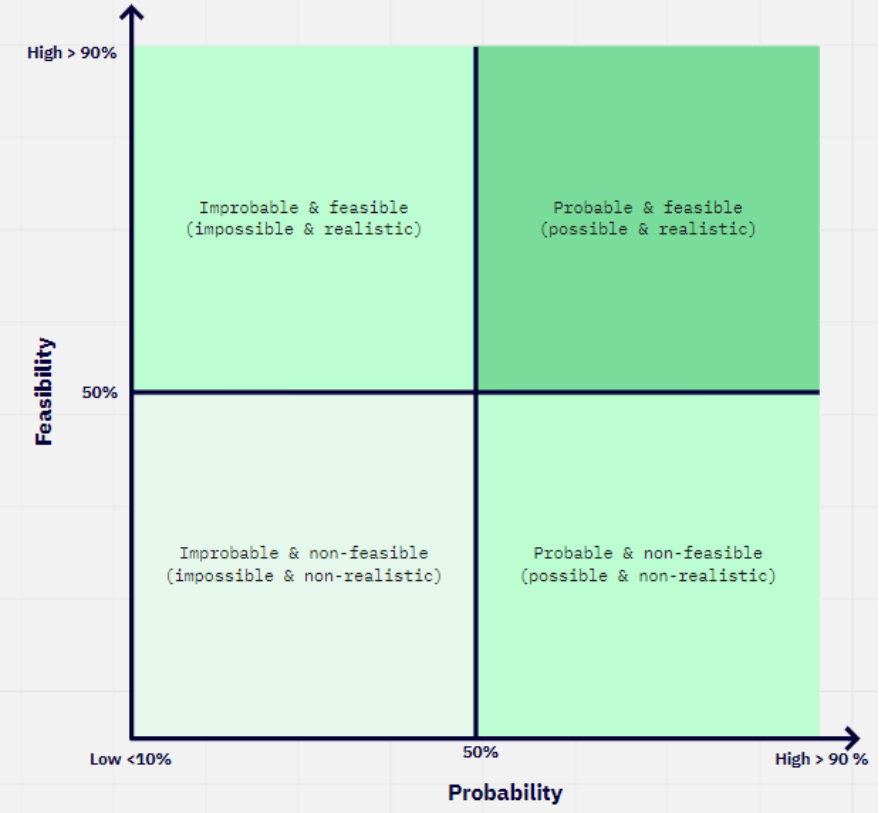


Figure 28. Evaluation Scale of Questions One and Two

9.1.1 Question 1

The first scenario was a desirable future named *Cyber Secure world is ready*. In this future the cyber security of the energy sector is solved by 2025 likewise safety is today.

Thesis: In 2025 cyber security is built-in in the operations of the energy sector likewise safety.

Question: How likely and possible is it to solve cyber security by 2025? Remember to comment on your arguments!

16 panellists answered this question. As presented in Figure 29 the panel agrees on the impossibility to solve cyber security by 2025 whereas the question if cyber security can be solved or not divides the panellists slightly.

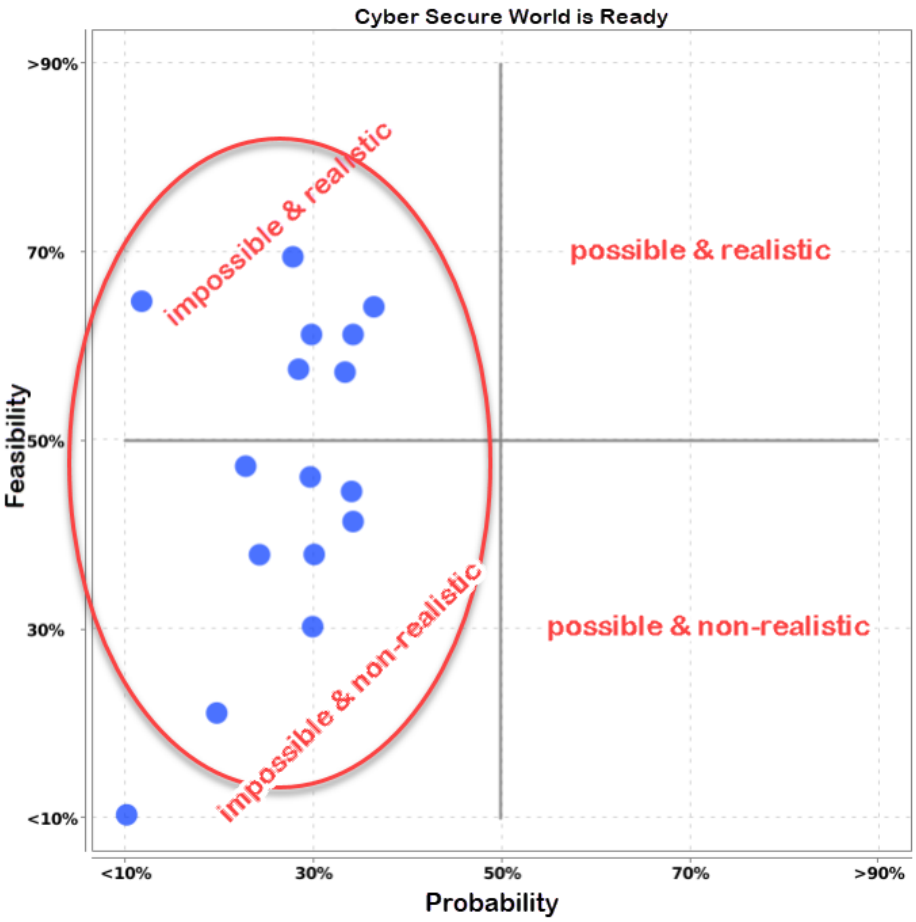


Figure 29. First Delphi Panel Question Results

The panellists emphasize the changes which are occurring in the energy sector: new regulation, new production methods, new companies and new technologies are appearing. These changes are constantly raising new threats. The organizations in the energy sector must keep up with the changes of the sector, for example today datahub, and cyber security may not be the primary focus.

> *"The cyber security is never ready and never will be since the world is changing, the technologies and threats are evolving, and cyber security must evolve alongside the changing environment."*

According to the panel, the attitude towards cyber security questions requires revision, more interaction and knowledge are required of the management and the whole organization. Cyber security is not seen as a business enabler but as a cost. GDPR has brought the privacy questions to the board's table, a similar regulation including legal fines should be degreed concerning cyber security, the implementation of information security standards is not seen as a solution.

> *"Even in bigger companies in Europe cyber security is the business of a handful of people. Cyber security knowledge is concentrated in one team and is not dispersed in the business units and there is no interaction with the management."*

The opinions of the panellists reveal that the suppliers of the sector are slightly outdated and the new start-ups entering the sector are not cyber security aware either. The old legacy systems are difficult or impossible to containerize or virtualize. Cyber security should be implemented in information system development. In the actual situation security and privacy by design are not applied efficiently.

> *"Coming from another sector I was amazed about the low cyber security maturity of the energy sector suppliers. Many of them hear the word information security for the first time when negotiating with them."*

The panel also raises the fact that proof of cost-effectiveness and a common aim are missing. Regulation is insufficient and the responsibilities are unclear. A national level aim should be emphasized including the European and Nordic collaboration. Smaller DSOs have limited resources, bigger companies are leading the dialog with authorities for a creation of an effective regulation which is seen as a primary solution to the question. Sharing knowledge among the specialists should be increased.

> *"The extent of the energy sector and the different maturity levels of DSOs are not enabling extensive roll-out in a short term."*

According to the panel DSOs should be prepared for the constant changes in the threat landscape and anticipate the new emerging threats. The extortions and

attacks which may destroy the infrastructure are conducted in a professional manner.

> *"Looking into the future and anticipating the cyber-attacks of 2030 is important."*
>
> *"It is a wrong approach to stay waiting for the new emerging technology threats. The threats are known if one wants to think about them and perform a systematic threat modelling."*

The experts of the panel acknowledge that cyber security is expected to be inbuilt and is not visible until a breach occurs, the customers may not be willing to pay for the security and yet the importance of cyber security is increasing. The security of the consumer solutions is also important.

> *"Cyber security is mainly invisible and an abstract matter which makes the development challenging compared to safety, which is more present daily, and people have personal experience for example with a sprained ankle."*

9.1.2 Question 2

Second scenario named *Freezing Hell vol. 2* is an undesirable future where an incident occurs with the smart meters including new services, partnerships, and interconnected smart grid as an attack vector.

Thesis: A scenario describing a cyber-attack on the smart meter infrastructure causing interruption of electricity distribution for many inhabitants of Finland was presented in this question. For cyber security reasons the content of the scenario is not opened in detail in this report.

Question: How likely and possible is the depicted scenario? Remember to comment on your arguments!

16 panellists answered this question. As presented in Figure 30 the panel agrees on realism of the scenario. The intensions to carry out a disruptive attack targeting citizens are emphasized by the panellists, a disruptive attack would not occur without a nation state willingness to attack, and the prevailing political situation does not give ground to a disruptive attack targeting citizens. Possibilities of extortion,

manipulating the consumers' opinions or manipulating the electricity markets are also questioned. Each attack requires a business case which is not necessarily present in this scenario.

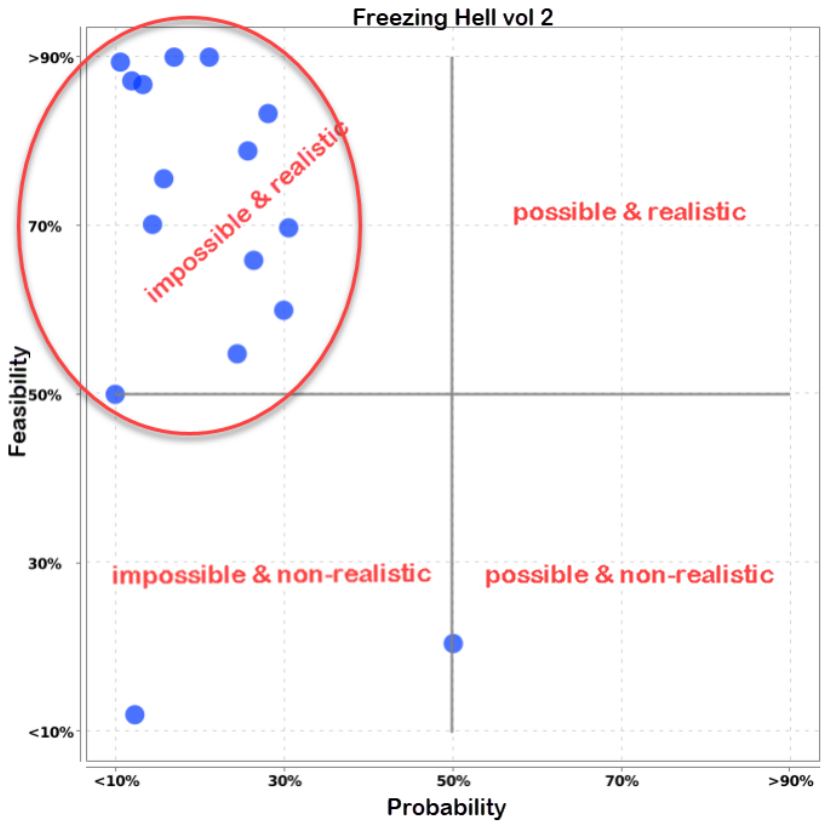


Figure 30. Second Delphi Panel Question Results

The panellists recognise the importance of the suppliers and logistic chain. The responsibility of the suppliers should be emphasized, the regulation and standardization should be mandatory for the suppliers of the national critical information systems and the authorities should control these suppliers regularly.

> *"Should there be a list of critical system suppliers, wider perspective than energy sector, based on which requirements could be set to the suppliers? If a new supplier becomes critical in one sector, it would be noticed, this supplier would be added on the list and the requirements concerning certifications and audits would be applied."*

> *"Should the regulatory requirements prevent dominant market positions in critical infrastructure -- so that one supplier can't endanger the security of supply of 200 000 electricity user."*

According to the panel the role of employees is controversy, at the same time the employees are the weakest and the strongest link of cyber security. The systems are built by humans and humans can destroy them.

> *"When the question is approached from the point of view of defending the interconnected systems, the employees are the strongest link and can scent the danger."*

According to the panel, protecting the smart meters from attacks should be done on the software level and resilience should be inbuilt in the smart meters. All the systems are vulnerable to attacks and become more vulnerable if cyber security is not considered during the whole lifecycle of the information systems and devices. Especially if the lifecycle of the device is exceptionally long. Would it be possible to access the consumer devices via the smart meters is also questioned as well as the future energy communities' effects on the security of supply?

9.1.3 Question 3

In the third scenario a desirable future named *Windy Energy Markets* is presented where the parties of the system should be capable of operating together in a complex environment which requires systems thinking. This scenario includes interconnectivity and partners and suppliers proposing new services. The capability of the parties to operate so that system level interruptions can be avoided is set to be evaluated on a 6-point Likert scale were

5 = no capability
6 = marginal capability
7= limited capability
8= partial capability
9= mostly capable
10= full capability

Thesis: In 2025 the critical infrastructure is a network-like system. To manage the complexity of this system, ability and system thinking is required from each actor of the system.

Question: Are the actors of the system capable of operating together so that system level interruptions will not occur? Evaluate the capability on the scale from 5 to 10 where 5 = no capability, 10 = full capability. Remember to comment on your arguments!

15 panellists answered this question. As presented in Figure 31 the panel is thinking that parties have partial or limited capability to operate together to avoid incidents.

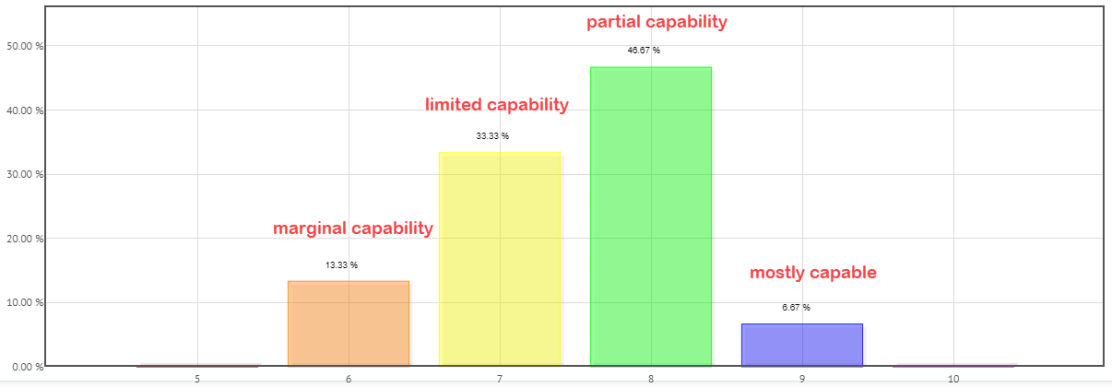


Figure 31. Third Delphi Panel Question Results

The panellists think that a national level consensus, trust and capability exist to guarantee the security of supply, but it is a system level question and dependent on several parties. Interruptions may occur due to coincidences. Active understanding and cooperation among the parties is important. Some parties are driven by profit and this conflict of interests can result in taking more risks reaching business goals since the understanding of the system wide consequences may be insufficient. New actors may not have experience of the sector and the responsibility of the system is not defined. The international dimension is also brought up and the already occurring system wide incidents outlined.

> *"Significant system failures are already occurring in Europe. Because production and consumption must always be in balance, the system is vulnerable to changes. At the European level network code on electricity emergency and restoration is under implementation. Due to the growing*

importance of the energy markets and the volatility of the market prices, a purposeful incident could be caused to gain profit."

"Closer the decision making of commercial or marketing activities more distant is the systems thinking and increased is the tendence to disturbing behaviour."

One of the panellists emphasizes the fact that the Finnish energy system is dependent on the capability of transmission system operator and the other parties are operating according to the common rules. New services and products are appearing, and new rules may take time before being set up. Energy production is based on nuclear and hydropower and imported energy. These parties can operate together with the transmission system operator.

The panellists also acknowledge the new technologies including machine learning requirements and the long lifecycles of the devices. New services are not concerning the whole energy consumption since the industry and public consumption are representing 75% of the total consumption in Finland.

Digital twin is introduced as an imperative solution by one of the panellists to simulate the functioning of the system. All parties of the system should integrate their operations in this digital twin and the license to operate in the system would be granted only after the mandatory simulation of the operations in the digital twin. Other panellists are wondering if the twin could be realised from a national cyber security budget or by the transmission system operator. Digital twin could increase the systems thinking of the parties.

"I would say that the systems thinking is one of the key competence areas in the top management."

9.1.4 Question 4

The fourth scenario named *Money, or your life* derogates about the future of cyber security of the operational technology describing the actual motivation of the attackers to gain profit. The old segregated systems no longer support the business development needs which will lead to convergence of IT and OT and use of cloud

services. How the data can be used in compliance with the regulations. How extortion attacks are avoided in the automation systems.

Thesis and question: Which factors are assuring the OT cyber security in 2025? Choose the five most principal factors! The factors were the following:

- Regulation
- Awareness
- Shorter lifecycle
- Requirements of the suppliers, hardware, and software
- AI, big data, and automated decision making
- Cloud services
- Competence
- Partnerships
- Information Security Technology
- Collaboration in co-operation networks
- Cyber resiliency
- Other?

15 panellists answered this question. As presented in Figure 32 the panel thinks that the five most crucial factors to assure cyber security in automation are regulation, competence, requirements of the suppliers, hardware, software, and awareness. In the *other* category a proposal for a digital twin was raised.

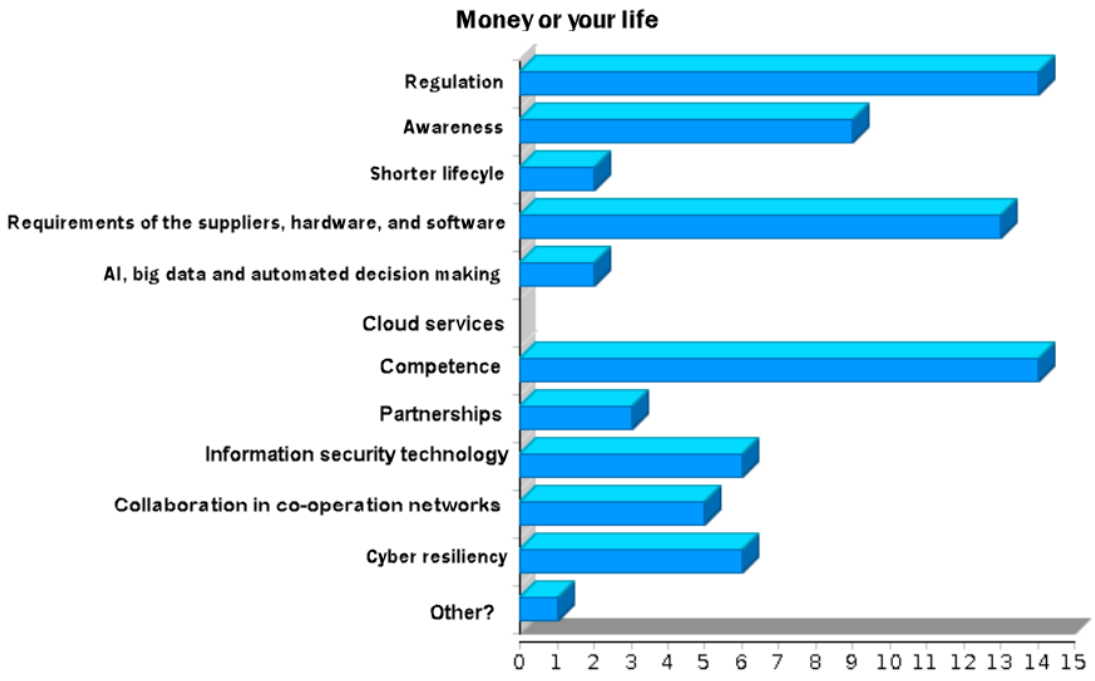


Figure 32. Fourth Delphi Panel Question Results

According to the panel the question of European level regulation is important. The interpretation of the requirements is broad and distorted by commercial aspects. The regulation should set the required level since Finn's require binding regulation and motivation. A missing regulation shows the political will and the unimportance of the matter. Some of the panellists think that the regulation cannot only be relied on.

> *"Unfortunately, the regulation has the power to make organizations invest in cyber security."*

> *"The energy distribution business is highly regulated. If we can set the power line frequency to 50 Hz, why can't we set as exact and binding cyber security requirements."*

According to the panel the second most crucial factor in assuring cyber security is competence. Competence is an obvious element since humans are required in the functioning of the OT systems and more competence is needed. Without competence it is challenging to react or be prepared for the future. The competence needs can be patched with partnerships. Collaboration in cooperation networks is a solution for remediating the missing competence.

> *"Cooperation networks enable efficient distribution of competence and awareness. The people working with cyber security are often alone and sharing information with interlocutors of the same field are worth more than gold."*

> *"Cyber security shouldn't only be observed inside the energy sector, a broader cooperation is meaningful."*

In addition to the regulation and competence the requirements of the suppliers are raised as a key element. The services proposed for the critical infrastructure should require a license. To remediate the lack of agile suppliers and needs to customise commercial off-the-shelf products' scalability and reliability, the energy sector could develop its own applications. The IT project management and process development competence may be missing though in the sector.

> *"Finally, competence solves everything but to get the competence solve the cyber security challenges, investments in regulation are needed."*

Technology is seen as an obvious key area to keep solutions up to date. The technology would enable us to reach compliance. Another panellist thinks that technology is not a problem, it is a tool, and technology is not an invention in automation.

Cyber resilience is important in maintaining and developing the security of supply. Resilience is the result of awareness and competence.

> *"Starting point is the awareness, without it the regulation and contracts can't be established, because the risks and solutions are not known, or the necessary competence is not acquired. After the awareness, the competence is needed to draft the regulatory and contract requirements to build a cyberresilient network."*

The panellists think that lifecycle management should be segmented since the lifecycles of some of the components might be long. The systems should be developed so that one part could be updated without changing the entire system. This is a commercial question to avoid vendor locks.

9.1.5 Question 5

The iterativity of the Delphi method was applied with the fifth question. The scenario *Towards the highway of the future* was added after the first week since it was raised by one of the panellists as a solution in the previous question. In this scenario a digital twin exists to simulate the functioning of the interconnected energy system and would be a mandatory evaluation tool before accepting new parties to be integrated in the system. This question type is Live2D, but the evaluation differs from questions 1 and 2. Instead of feasibility the desirability is evaluated together with possibility.

Thesis: Digital twin to assure cyber security in 2025.

Question: How likely and possible is the depicted scenario? Remember to confirm your arguments!

9 panellists answered this question. As presented in Figure 33 the panel agrees on the impossibility to implement the digital twin by 2025 but thinks it is desirable.

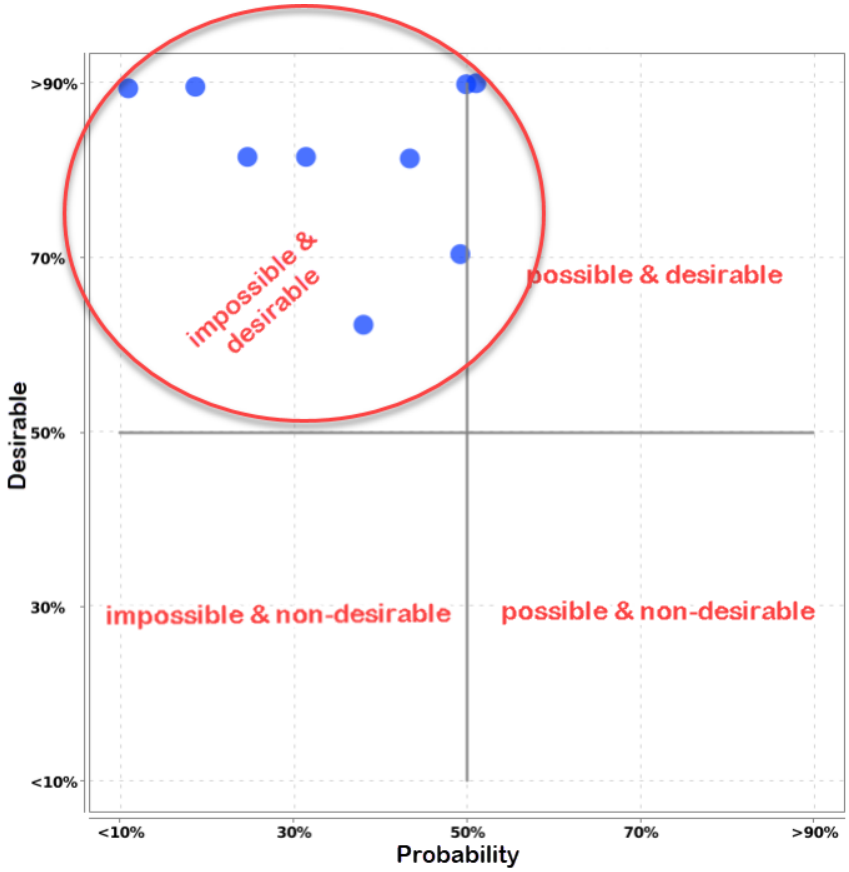


Figure 33. Fifth Delphi Panel Question Results

According to the panel, the year 2030 would be more realistic to implement a digital twin due to the novelty of the idea. By 2025 the first proof-of-concepts might be possible to realise. One of the panellists raised the worry of protecting the twin itself. A competing idea of simulated worlds alongside the production system instead of a whole duplicate of the electricity network was raised by another panellist.

9.1.6 Question 6

Question was added at mid-point of the panel in the comments of question number 1. Question was added since panellists were discussing the importance of cyber security in the comments of the first question.

Question: How important is it to ensure the cyber security of the energy sector?

According to the panellists it is vital for society to handle cyber security. People may die and economic consequences would be massive if the electricity distribution network came to collapse. The batteries, distributed energy production and

microgrids could guarantee the security of supply in rural areas, but not the functioning of the infrastructure in cities and as a whole.

The panellists wonder if microgrids could bring resilience since households would be less dependent on electricity grids. On the other hand, the microgrids would be less secure but the impact of a failure is lower. Some risks may emerge since microgrids would be connected to super grids. In Europe, the microgrids are already appearing, in Finland they may be less likely during this decade except for cooperative housing. Smart grids and small-scale production could also bring new threats if the smart grids are still in use by 2025. Are the customers aware of how to securely connect an electric car to the network, charging pole, solar panels, wind turbine, air heating pump or heating systems which are controlled at a distance from a cloud service?

The panellists see that the super grids are already appearing in Europe and the whole electricity system could be synchronised European wide. Such an interconnected network could cause problems in each country and requires adequate regulation.

9.2 Cyber Security Roadmap Proposal

To solve the cyber security the regulation is seen as the primary solution to the question. Each company should spread cyber security awareness inside the company and apply security and privacy by design principles. When awareness and competence are widespread the resources dedicated to cyber security can be adjusted cost-efficiently. New services and products are appearing, and European wide interconnectivity is at hand. In super grid world one DSO is dependent and must rely on the common regulation, taking part in drafting European wide regulation and the national implementation would be important.

The responsibility of the suppliers is emphasized alongside the vulnerability management. A common aim for the sector should be decided to standardize the requirements set to the suppliers of the sector.

The responsibility of the consumers and their understanding of the threats connected to the use of new technologies should also be addressed by the requirements set to the devices and suppliers. DSO should consider a more

responsible role concerning the guidance given to the customers when using intelligent home devices.

Management must understand that cyber risks are business risks. Since the threat landscape is changing, companies should be prepared for future threats and be able to recover from an attack, preparedness and resiliency are important.

Simulating the functioning of the interconnected system would be beneficial for each organization. Maintaining a duplicate of the electricity network would require resources and the sole purpose of assuring cyber security may not be enough for a business case. Such a simulating environment could be also used in operational activities of DSO like network planning and testing purposes.

Today Finnish DSOs requirements are set in the electricity market act. Preparedness planning requires completion of a questionnaire which provides the organization with a development plan. Two network codes will be setting requirements in the future, especially the cyber security network code. Reasonable level for the cyber security for a DSO today is depending on the organization's own risk management competence, ambition of responsibility, quality, and resiliency requirements since the requirements of the information security and risk management methodology are in general level and not expressed in detail in the lawful requirements. The actual state enables variations in the cyber security maturity among the DSOs.

The cyber security network code proposal recommends the inclusion of several procedural, functional, and technical standards. The development of the network codes should be followed and influenced closely.

The opinions of the Delphi panellists were transposed in a spreadsheet, analysed, condensed, and categorised in main and solution categories. The solution categories are derived from the question four answers. The condensed meanings with main and solution categories from the Delphi panel opinions are presented in Table 4. The roadmap proposal was created based on these results.

Table 4. Contributory Factors of the Cyber Security of DSOs after Delphi panel

Condensed Meaning	Main Category	Solution Category
Changing and developing energy sector: old systems must be updated, new regulation (e.g., datahub), new technology and new actors, cyber security is not in-built.	New services and products	1. Regulation, security, and privacy by design principles
Lack of cyber security awareness among the suppliers: old fashioned large companies or new start-ups.	Partners and suppliers	1. Regulation, common requirements for the suppliers of the sector
Emphasize on cyber security missing. Case Vastaamo or similar needed, certifications not solving the problem.	Regulation, security policies and principles	1. Regulation, common requirements for the energy sector
Regulation, control, and ownership required	Regulation, security policies and principles	1. Regulation, Common requirements for the energy sector
DSOs limited resources and capabilities focused on energy sector development requirements, not on cyber security.	Resources, cost-effectiveness	1. Organization wide knowledge 2. 2. Collaboration of specialists to share knowledge among the sectors
Proof of cost-effectiveness missing, cyber security seen as a cost, not a business enabler.	Resources, cost-effectiveness	1. Regulation, Common requirements for the energy sector
Cyber-attacks capable of destruction. Extortion or data breaches resulting in public data exposure. New emerging threats with new technologies, professional crime, case Ukraine.	Risk management, business enabler	1. Reciliency
Legacy systems cannot be virtualized or containerised	Regulation, security policies and principles	1. Reciliency
Customer's willingness to pay for cyber security doubted, expected to be inbuilt.	Resources, cost-effectiveness	1. Regulation, Common requirements for the energy sector
Ability, awareness, and interaction missing with management, employees, and information system developers.	Resources, cost-effectiveness	1. Organization wide knowledge

Common national, Nordic, and European level aim and regulation.	Regulation, security policies and principles	1. Regulation, Common requirements for the energy sector and suppliers
Consumer awareness, vulnerable consumer devices	New services and products	1. Regulation, common requirements for the services and devices 2. Awareness of the customers
Cyber security is never ready. Vulnerability and threat management. Cyber security risks are business risks.	Risk management, business enabler	1. Management's commitment 2. Organization wide knowledge
The extent of the energy sector and the different maturity levels of DSOs.	Resources, cost-effectiveness	1. Management's commitment 2. Organization wide knowledge
Actions of employees	Resources, cost-effectiveness	1. Awareness of employees
Requirements on critical infrastructure system suppliers. Gaining profit at the cost of energy system security.	Resources, cost-effectiveness	1. Regulation, Common requirements for the suppliers of the sector
TSO's significant role in setting common rules	Regulation, security policies and principles	1. Regulation, Common requirements for the energy sector
European wide energy system	Regulation, security policies and principles	1. Regulation, Common requirements for the suppliers of the sector
Systems thinking in decision making	Risk management, business enabler	1. Management's commitment 2. Organization wide knowledge

The roadmap proposal is divided into short and long-term actions. The goal is to reach the aims set in Elenia's cyber strategy. Four equally important tracks are presented in the roadmap proposal as shown in Figure 34.

Knowledge and competence management should be handled so that the risk management and threat modelling become part of the company's culture. Eventually the knowledge management target should be set to cover the partnerships as well.

Regulatory requirements are presented in two different tracks, first the regulatory requirements where a GAP analysis conduction is proposed against the network code cyber security requirements followed by the implementation of the desired level. Active shaping of the future includes active participation in European and national level legislative reforms and opinion leadership. These two tracks emphasize Elenia's

strategic aim to be the most responsible reformer of energy services and markets. Risk and resilience management is the third track which consists of the short-term action to conduct a comprehensive cyber risk evaluation followed by long term action proposal to plan a digital twin or similar environment. This long-term goal should be synchronised at the national level with the whole energy sector. Finally, the active shaping of the future should continue, and a new Delphi or similar study should be conducted to foresee the future beyond 2025.

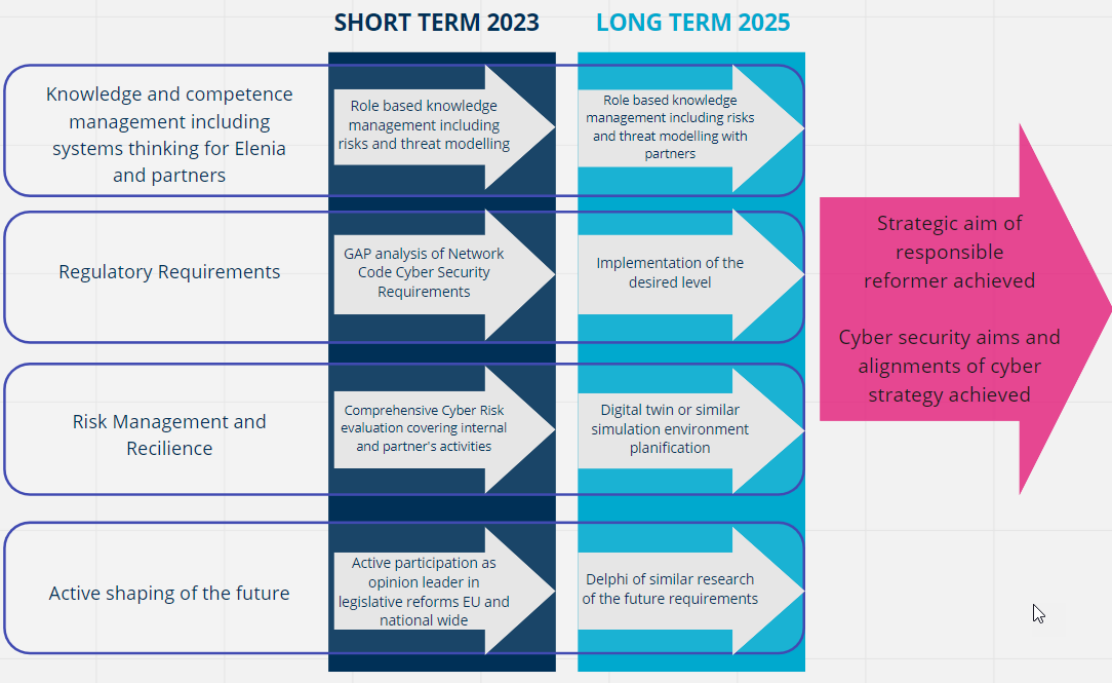


Figure 34. Cyber Security Roadmap Proposal for Elenia

10 Conclusions

The lack of previous studies concerning cyber security strategy development in critical infrastructure companies prove the need to study this area more. In general, evidence of measurable and fit for purpose cyber security performance management is missing, cyber security is approached from the risk management perspective and is seen as a cost. Both research questions were answered in this research.

The results of the research confirm that regulation is the principal factor in cyber security. The regulation must cover all the actors of the system, especially the

suppliers and devices, not only DSOs. The energy sector is already highly regulated and a new regulation concerning cyber security is under preparation.

Systems thinking must be applied at all levels in companies. This research confirms the previous study of future energy sector competence needs: skills for managing larger entities are needed. Other new roles are also needed, If the regulation comes to increase, more legal competency is needed.

Exceptional situations should be considered though and managed, resilience must be assured. The resilience and risk management should cover the cyber security aspects concerning global suppliers.

The first research question was **What is the meaning of cyber security in the electricity distribution business in the future?** The importance of cyber security was emphasized in the interviews and in the Delphi panel. Cyber security is vital for a DSO in the future where the electricity network will be an interconnected system consisting of parties with different cyber security maturity levels. Digitalization has dramatically increased during COVID-19. Society is totally dependent on electricity distribution and the security of supply.

Second research question was **What is the reasonable level of cyber security for a DSO?** Reasonable level for the cyber security for a DSO today is depending on the organization's own ambition of responsibility, exigency of quality and resiliency since the regulatory requirements of the information security and risk management are in general level and not expressed in detail in lawful requirements. Statutory cyber security requirements today are derived from NIS directive and are implemented in the Electricity Market Act. These are the preparedness planning, information security risk management and obligation to report if an incident occurs. The actual state enables variations of the cyber security maturity among the DSOs.

To achieve reasonable and cost-effective regulation for DSOs, an active role in the drafting and implementation processes of regulatory requirements should be taken to raise the understanding of the system wide importance of the suppliers of the sector. If the implementation of the regulation is not actively managed, a less desirable future may appear where the regulation is only applied to DSOs. Active

shaping of the future is important to avoid the undesirable scenarios depicted in the security of supply scenarios.

The meaning of cyber security in the electricity distribution business in the future is being a business enabler. When the reasonable level of cyber security is applied with awareness, competence, risk and resilience management and adequate regulation, the future business development can be planned with confidence since the company is prepared for the future. Active shaping of the future continuously comes to complement the futureproofing.

Knowledge management as a solution was presented in previous studies and the findings of this thesis confirm the importance of awareness and competence management. Concrete actions are given to Elenia to achieve a cost-effective and reasonable level of cyber security by investing in knowledge management inside the organization and in partnerships. Awareness and competence management result in cyber secure culture where the risks are managed also in the systems with long lifecycles.

Elenia has already taken steps towards an effective cyber security by implementing externally audited and continuously developed ISMS with the ISO/IEC 27001:2013 certification and proven the willingness to assure the quality of security of supply of the customers. The implementation of a certified ISMS may be a requirement for each distribution system operator in the future.

This research has supplied understanding to Elenia concerning the future of cyber security in the electricity distribution business. The research applies to each Finnish DSO although the research was started by the needs of a single DSO. The applicability of the recommended roadmap actions is the whole energy sector and can be extended to any sector. The results of this thesis confirm the findings of the reports in theoretical background, but this research goes further and gives concrete action points for DSOs.

The results of this thesis, the cyber security roadmap, are supporting Elenia's business strategic goals. These results provide Elenia with information about where cyber security investments and stakes should be directed. The results of this research also provide solutions to the aims set in the Finnish cyber security strategy.

Use of Delphi method in the energy sector was novel and this thesis is the first research applying Delphi method in cyber security studies in Jyväskylä University of Applied Sciences. The Delphi panellists represented widely the best cyber security knowledge in Finland, visionary experts also outside the energy sector took part in the panel. COVID-19 may have encouraged people to foresee the future in business activities since when enquiring about the willingness to take part in the panel, the people were positive, interested and asked for the possibility to get the results. The results were also discussed in the energy sector information sharing and cooperation group, several members of which took part in the panel.

The conducted Delphi panel had double advantages. First being to answer the research questions and form the cyber security roadmap proposal. The second to spread thinking and awareness among a larger audience with the questions, answers, and opinions of the panellists.

For the author, the Delphi method was a new acquaintance, and this was the first Delphi panel realization. Delphi panel could have had several rounds so that there would have been several months between the rounds to see if the opinions and arguments of the panellists would change. The iterativity, which is a characteristic of Delphi method, was realised in this research with the interviews and questions added at mid-point of the Delphi panel.

11 Discussions

Cyber security and hybrid threats are a manifestation of a world where the digital and physical worlds are tied together. Managing information security risks inside one and unique network is no longer enough. These new ways of working have increased the need for security competence but have cyber security and risk management skills been on the table when planning for the new profiles and creating human resource strategies. Has society done what is necessary to educate the people to media literacy and to derogate each action and actor adequately? What is the responsibility of society and of a single company when we think about the critical infrastructure and the societal impact of its´ disturbances? You can recognize a thief on the street but what about cyber space, how do you recognise if someone has illegal attention?

One of the risk treatment choices in Elenia's ISO/IEC27001:2013 compliant ISMS is to stop an action if the risks related to it are estimated to be intolerable. Can we stop being part of cyber space?

Handling cyber security risks is not only a company specific issue but a national and global societal field of work. DSOs must do their share by giving required resources to educate the employees to understand the risks and be resilient.

Cyber security responsibles' key role in the future is to guide and enable active systems thinking to increase the understanding of cyber security related issues. This role is far from the technical IT security expert not speaking business´ language.

The thesis journey has been rewarding and interesting in many ways. The theoretical background brough into light an exhausting picture of threats and risks in the cyber domain. The always on and interconnected world is at hand, and we are still searching for the best practise of this new digital world. If the nations power would come to diminish and the control would be given to global multinational organisations, the national interests would have no meaning in this world. This has already started. The development of AI and machine learning will change the course of humanity if the limits of their use are not set clearly and globally. It is time to enter a global discussion and mutually agree on the use of such powerful technologies capable of affecting and altering human behaviour.

The risks are increasing with the prospects of the future complex interconnected energy system. To avoid undesirable scenarios, DSO's must anticipate the future. To deepen the understanding of the consequences and impacts of cyber security risks in the complex energy system two proposals for future research are suggested.

1. The impact of a cyber security incident on integrated energy systems
2. Applying game theory in cyber security research and development

According to Siilasmaa (2020) the purpose of leadership and management is to take an active part in shaping the future towards the desired scenarios. Trust in the future is created by influencing the likelihood of positive scenarios. The anticipation of the risks and creation of the roadmap are strategic choices of management. The future can be shaped when the understanding and the willingness of the management are

present. DSO's must flexibly adapt to the new conditions which may be foreseeable or unexpected as COVID-19 has proven. Even the megatrends have been affected by COVID-19. Therefore, the roadmap proposal includes the active shaping of the future continuously.

The learning aim of this thesis was to familiarise the author with the Delphi method to be able to use if efficiently also in the future. Alongside learning the method, the personal thinking and understanding of cyber security matured and diversified. Even if a strategy itself is looking further, the implementation steps could require adjustments more often. Now the possible futures were studied for the next five-year period, but in the future, there might be a need for shorter or longer-term plans. The Delphi method is versatile and can be used in both needs. In addition to the Delphi method a deep dive in the qualitative and quantitative research methods, energy sector revolution and regulation which is under development at the European level became familiar and the knowledge gained from this thesis can be transposed directly in the everyday work of the author as Chief Information Security Officer of the commissioner, Elenia. The learning goals were fully achieved.

11.1 Ethics and Quality

To guarantee the ethics and quality of this research the research process was described in detail and several research methods were used in addition to the main research method, the Delphi method. The quality of the content analysis of theoretical background was verified with the interviews. With both interviewees a telephone discussion was held where the details of the interview were explained and the willingness to take part was enquired. The questions of the interview were supplied beforehand and the names or the companies of the interviewees are not published, only the titles were referred to in the analysis. The recordings of the interviews were removed after the litteration was ready.

The results in form of a roadmap proposal were done based on subjective opinions of the Delphi panel panellists. The quality and truthfulness of the questions of the panel was assured with the consultation of the commissioner's energy sector experts. The questions of the panel were formed neutrally, and the quality of the questions from

research point of view was assured with the Delhi study tutors and Elenia's management. The choice of the panellists was made carefully based on their proven knowledge concerning cyber security, cyber security of the energy sector and the energy sector. Bigger and smaller DSOs took part in the panel. Both groups were represented, the experts and the generalists. The participants included experts from different organizations and from authorities. The participation in the panel was voluntary and anonymous. The names or the companies of the panellists are not published. The privacy policy of eDelphi tool is compliant with the GDPR regulation.

Background information such as gender or age was not collected from the participants of this research since the main purpose of the research was to collect information for commissioner's internal needs at not for a generalization purpose. The participation was voluntary in each phase.

Since the analysis process was conducted by the author alone, human mistakes caused by erroneous interpretation are possible. Manifest content analysis was used to remain as close to the data as possible. The limited number of interviewees and Delphi panellists must be considered when evaluating the quality of the research.

11.2 Solving Cyber Security

The regulation concerning the critical infrastructure has been under discussions, centred on the requirements to be set for the organizations. Instead, the emphasis should be put on assuring the cyber security of the entire system including the suppliers and the logistic chains. The suppliers of the critical infrastructure are in a key role. The suppliers should be imposed clear requirements and the authorities should control the suppliers continuously. Critical infrastructure should not be at the hands of only a few suppliers. It is rather a question of responsibility of the authorities than of a single company in critical infrastructure.

In the physical world national security is the responsibility of the authorities and defence forces. The citizens and the companies must implement the sector specific regulatory requirements. Where is the authority in the digital world, who oversees national security? The digital delinquency must be taken in charge by the authorities and clarify the roles, where is the digital police office. Finnish National Cyber Security

Centre could be in this role, and the Finnish competence should be centred in such a digital police office. The responsibility to counter cyber delinquency must be the responsibility of the nation. In addition to the digital police forces, clear and detailed regulations and requirements should be set to the critical infrastructure with detailed instructions on how to implement the required level. When the requirements are expressed clearly, the gap of the skill shortage in the cyber security capabilities is measurable and solvable. Each critical infrastructure company would know how to protect themselves cost-efficiently and what kind of skills are needed. Finnish educational system could better concentrate on the exact skills needed and emphasize of the educational system can be put on innovative technologies, like AI and machine learning. With these concrete actions, cyber security would be solved, and society can be centred on increasing wellbeing of the people. The actual situation where the companies must implement police like capabilities by themselves is not profitable for the national economy nor guaranteeing the security of supply.

11.3 Acknowledgements

I want to express my deepest gratitude to my husband who has supported me during the studies and tirelessly took care of our children while my thoughts were in the cyber world. Special thanks are also expressed to my thesis tutor of Jyväskylä University of Applied Sciences, Jari Hautamäki, for the valuable guidance during the whole thesis process. I would also like to thank my tutor in Elenia, Heikki Paananen, for the insightful and inspiring guidance every time I needed support. Finally, I want to thank all the experts who took part in realising this research with their continuous support as well as the cyber security domain colleagues who are passionately working to guarantee the security of supply of Finland every day.

References

Ahonen, P. 2019. *KYBER-ENE - Energia-alan kyberturvaaminen 1-2* [KYBER - ENE – Assuring the cyber security of Energy sector 1-2]. A publication of National Emergency Supply Agency. Accessed on 13 March 2019. Retrieved from https://www.huoltovarmuuskeskus.fi/files/b365153bf8b369253950c816e4c222ae523bb1d4/vtt-kyberene.pdf

Ang, C. K. G., & Utomo, N., P. 2017. Cyber Security in the Energy World. Accessed on 16 October 2020. Retrieved from https://janet.finna.fi, IEEE Xplore Digital Library. doi: 10.1109/ACEPT.2017.8168583

Anttila, T. 2020. *Mikä on kansallinen digitaalisen huoltovarmuuden tilanne? Tulisiko varmuusvarastoista löytyä myös teknologiaa?* [What is state of the national security of supply? Should there be technology in reserve supply?] A blog on Suomidigi website. Accessed on 15 December 2020. Retreived from https://www.suomidigi.fi/blogit/mika-kansallinen-digitaalisen-huoltovarmuuden-tilanne-tulisiko-varmuusvarastoista-loytya-myos-teknologiaa

Barnhart-Magen, G. & Caltum, E. 2018. Jarvis never saw it coming - Hacking machine learning (ML) in speech, text, and face recognition – and frankly, everywhere else. A presentation in T2 Infosec conference in Helsinki Finland 25th– 26th October 2018. Accessed on 2 April 2021. Retrieved from https://youtu.be/BSee7lwnj6w

Bengtsson, M. 2016 How to plan and perform a qualitative study using content analysis. Accessed on 15 April 2021. Retrieved from https://doi.org/10.1016/j.npls.2016.01.001

Center for Research on Environmental Decisions. 2009. Beware the Overuse of Emotional Appeals. Accessed on 5 January 2021. Retrieved from http://guide.cred.columbia.edu/guide/sec4.html

Directive (EU) 2016/1148. 2016. Directive of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. Accessed on 9 March 2020. Retrieved from https://eur-lex.europa.eu Up-to-date legistlation

Dufva, M., Hellström, E., Hietaniemi, T., Hämäläinen, T., Ikäheimo, H-P., Lähdemäki-Pekkinen, J., Poussa, L., Solovjew-Wartiovaara, A., Vataja, K. & Wäyrynen, A. 2020. *Megatrendit koronan valossa* [Megatrens in the light of COVID-19]. Accessed on 5 March 2021. Retrieved from https://media.sitra.fi/2020/10/02085411/megatrendit-koronan-valossa.pdf

Elenia. 2019a. *Elenian kyberstrategia* [Elenia's cyber strategy]. Elenia internal publication. Accessed on 8 March 2020. Retrieved from Elenia intranet

Elenia. 2019b. *Elenia ISO/IEC 27001:2013 Tietoturvan hallintajärjestelmän sovellusalue* [Elenia ISO/IEC 27001:2013 ISMS scope statement 2019]. Elenia internal publication. Accessed on 7 March 2020. Retrieved from Elenia intranet

Elenia. 2020. *Elenia and sustainability 2019 - Report.* A publication on Sustainable Elenia website. Accessed on 29 October 2020. Retrieved from https://www.elenia.fi/en/sustainability/sustainable-elenia

Elenia. N.d.a. About us. A page on Elenia's website. Accessed on 7 March 2020. Retrieved from https://www.elenia.fi/en/elenia/company/about-us

Elenia. N.d.b. Brändimme ja maineemme [Our Brand and Reputation]. Elenia internal publication. Accessed on 7 March 2020. Retrieved from Elenia intranet

Energy Authority. 2018. *Energiaviraston ohje tietoturvallisuuteen liittyvän häiriön ilmoittamisesta* [Energy Authority instruction on reporting information security incident]. A publication of Energy Authority *1914/402/2018.* Accessed on 15 November 2019. Retrieved from https://energiavirasto.fi/documents/11120570/12857531/Energiaviraston-ohje-NIS-ilmoituksista.pdf/b5dcd909-ca59-fda1-f2b4-f941eab59c4c

Energy Authority. N.d.a. *Verkkotoiminnan luvanvaraisuus* [Electricity network business is subject to license]. A page on Energy Authority website. Accessed on 15 June 2019. Retrieved from https://energiavirasto.fi/verkkotoiminnan-luvanvaraisuus

Energy Authority. N.d.b. *Verkonhaltijoiden varautuminen ja tietoturva* [Network holder's preparedness and information security]. A page on Energy Authority website Accessed on 16 March 2020. Retrieved from https://energiavirasto.fi/varautuminen-ja-tietoturva

ENISA. 2020. *ENISA Threat Landscape - Emerging trends.* ENISA homepage publications. Accessed on 8 March 2021. Retrieved from https://www.enisa.europa.eu/publications/emerging-trends

ENISA. N.d. The ISMS Framework. Accessed on 8 January 2020. Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-isms/framework

European Commission. 2019. Commission recommendation on cybersecurity in the energy sector. A European Commission publication of 3th April 2019. Accessed on 15 March 2021. Retrieved from https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf

European Commission. 2021. Electricity network codes and guidelines. A European Commission webpage updated 5th Feburary 2021. Accessed on 15 March 2021. Retrieved from https://ec.europa.eu/energy/topics/markets-and-consumers/wholesale-energy-market/electricity-network-codes_en?redir=1

Financial Times. 2020. Prospering in the pandemics: the top 100 companies. Page on Financial Times website. Accessed on 13 October 2020. Retrieved from https://www.ft.com/content/844ed28c-8074-4856-bde0-20f3bf4cd8f0

Finnish Innovation Fund Sitra. 2019. *Megatrendit 2020* [Megatrends 2020]. Accessed on 18 December 2020. Retrieved from https://www.sitra.fi/julkaisut/megatrendit-2020/

Finnish National Cyber Security Centre. 2020. *Kybermittari* [Cyber meter]. Accessed on 31 March 2021 Retrieved from https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen/kybermittari

Finnish National Cyber Security Centre. 2021. *Cyber weather*. Finnish Cyber Security Centre's monthly update on key information security incidents and phenomena. Accessed on 12 February 2021. Retrieved from https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/kybersaa

Finnish Security and Intelligence Service. 2020. *Supo Year Book 2019*. Accessed on 14 December 2020. Retrieved from https://supo.fi/documents/38197657/40760242/2019_EN_Supo_yearbook.pdf/9be682cf-bfb6-50d6-d7b7-cc903d8e5802/2019_EN_Supo_yearbook.pdf?t=1602666410607

Finnish Security and Intelligence Service. N.d. *Kansallisen turvallisuuden katsaus 2020* [Overview of National Security 2020]. Accessed on 15 December 2020. Retrieved from https://supo.fi/documents/38197657/39761269/FI+Kansallisen+turvallisuuden+katsaus_2020.pdf/dd60c411-2ee5-d5c9-83a0-2e91b08ccd36/FI+Kansallisen+turvallisuuden+katsaus_2020.pdf?t=1603899390368

Finnish Transport and Communication Agency. 2021. *Passenger cars in traffic on 31 March 2021 by area 2021.* Statistics database on Finnish Transport and Communication Agency website. Accessed on 15 April 2021. Retrieved from https://trafi2.stat.fi/PXWeb/pxweb/en/TraFi/TraFi__Liikennekaytossa_olevat_ajoneuvot/010_kanta_tau_101.px/

Flyktman, J. 2016. Implementing Information Security Management System as a part of business processes: Where to gain competitive advantage for ISMS? Master's thesis. JAMK University of Applied Sciences, School of Technology, Degree Programme in Information Technology. Accessed on 8 January 2021. Retrieved from http://urn.fi/URN:NBN:fi:amk-2016060311816

F-Secure. N.d. The State of the Station. A report on attackers in the energy industry. Accessed on 12 December 2020. Retrieved from https://www.f-secure.com/content/dam/press/en/media-library/reports/F-Secure%20Report%20-%20Energy%20(English).pdf

Haapala, M. 2020. *Energiamurros ja huoltovarmuus* [Energy sector changes and the security of supply]. An article on National Emergency Supply Agency website. Accessed on 28 October 2020. Retrieved from https://www.varmuudenvuoksi.fi/aihe/energiahuolto/497/energiamurros_ja_huoltovarmuus

Hiltunen, E. 2012. *Matkaopas Tulevaisuuteen* [A guide towards the future]. Talentum

International Data Corporation (IDC). 2020. Cloud IT Infrastructure Spending Continued to Grow in Q1 2020 While Spending on Non-Cloud Environments Saw Double-Digit Declines, According to IDC. A press release on IDC' s website published

25 June 2020. Accessed on 17 March 2021. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS46639820

ISO27k toolkit. N.d. Accessed on 5 March 2021. Retrieved from https://iso27001security.com/html/toolkit.html

Juujärvi, O. 2021. *Sähkölämmittäjä: tee palvelus kukkarollesi ja ilmastolle sähkökuorman ohjauksen avulla!* [User of electrical heating: Do a favor to your wallet and climate with electric load control!]. A news on Caruna website. Accessed on 16 March 2021. Retrieved from https://www.caruna.fi/ajankohtaista/sahkolammittaja-tee-palvelus-kukkarollesi-ja-ilmastolle-sahkokuorman-ohjauksen-avulla

Kunnaskari, M. & Peltonen, K. 2018. *72 tuntia innostaa urbaaniin varautumiseen* [72 hours inspire urban preparedness]. National Emergency Supply Agency publication *Huoltovarmuuden skenaariot 2030* [Security of supply scenarios 2030]. Accessed on 15 November 2020. Retrieved from https://cdn.huoltovarmuuskeskus.fi/app/uploads/2018/10/23143222/Skenaariot-2030_2p.pdf

Kuusi, O. N.d. *Delfoi-metodi* [The Delphi method]. Accessed on 6 November 2020. Retrieved from https://metodix.fi/2014/05/19/kuusi-delfoi-metodi/

Kyber VPK. N.d. Community Cyber Response Force website. Accessed on 15 November 2020. Retrieved from https://kybervpk.fi/en/

Law 9.8.2013/588. *Sähkömarkkinalaki* [Electricity market act]. Accessed on 9 March 2021. Retrieved from https://www.finlex.fi Up-to-date legistlation

Limnéll, J., Majewski, K., Salminen, M., & Samani, R. 2015. Cyber security for decision makers. Jyväskylä: Docendo.

Linturi, H. 2020. *Delfoi-menetelmän tunnusmerkit* [Delphi method characteristics]. An article on Metodix website published on 12.6.2020. Accessed on 20 April 2021. Retrieved from https://metodix.fi/2020/06/11/delfoi-menetelman-tunnusmerkit

Linturi, H. N.d. *7. Delfoi-analyysi* [7. Delphi analysis]. A webpage on Metodix website. Accessed on 20 April 2021. Retrieved from https://metodix.fi/2020/12/11/delfoi-analyysi/

Luiijf, E., van Schie, T., van Ruijven, T. & Huistra, A. 2016. Critical Information Infrastructure Protection Good Practice Guide. A publication of Global Forum on Cyber Expertise. Accessed on 11 January 2021. Retrieved from https://thegfce.org/release-critical-information-infrastructure-protection-good-practice-guide/

Lähdeaho, T. 2020. Fortum and Elenia's battery pack stores electricity for power outages and for maintaining electricity network balance. A news on Elenia website. Accessed on 15 March 2021. Retrieved from https://www.elenia.fi/en/news/fortum-and-elenias-battery-pack-stores-electricity-for-power-outages-and-for-maintaining-electricity-network-balance

Martin, A., Rashid, A., Chivers, H., Danezis, G., Schneider, S. & Lupu, E. 2019. Introduction to CyBOK – Issue 1.0. The Cyber Security Body of Knowledge program

publication led by the University of Bristol. Accessed on 3 January 2021. Retrieved from https://www.cybok.org/media/downloads/Introduction_to_CyBOK.pdf

Mattila, J., Ali-Yrkkö, J. & Seppälä, T. 2020. *Kyberuhat yleistyvät – Miten Suomen yritykset pärjäävät?* [Cyber threats are common – how does the Finnish companies manage?] Brief number 93 published on ETLA website 14.12.2020. Accessed on 7 January 2021. Retrieved from https://www.etla.fi/wp-content/uploads/ETLA-Muistio-Brief-93.pdf

Ministry of Economic Affairs and Employment of Finland. 2018. *Selvitys älyverkkojen mahdollisuuksista sähkömarkkinoilla* [Report on smart grids´ potential for the electricity market]. Accessed on 15 December 2018. Retrieved from https://tem.fi/alyverkot

Ministry of Economic Affairs and Employment of Finland. 2020. *Building of Finland's first quantum computer begins – VTT partners with quantum startup IQM*. A press release on Ministry of Economic Affairs and Employment website. Accessed on 5 January 2021. Retrieved from https://tem.fi/en/-/building-of-finland-s-first-quantum-computer-begins-vtt-partners-with-quantum-startup-iqm

Ministry of Economic Affairs and Employment of Finland. 2021. *Lakiesitys hillitsee sähkön siirtohintoja ja leikkaa jakeluyhtiöiden tuottoja* [Legislative proposal to cut electricity distribution prices and profits of distribution companies]. A notice on Ministry of Economic Affairs and Employment website. Accessed on 15 March 2021. Retrieved from https://tem.fi/-/lakiesitys-hillitsee-sahkon-siirtohintoja-ja-leikkaa-jakeluyhtioiden-tuottoja

Ministry of Transport and Communications. 2020. *Valtion kyberturvallisuusjohtaja on nimitetty* [National cyber security Director is appointed]. An announcement of Ministry of Transport and Communication website on 27.02.2020. Accessed on 13 March 2020. Retrieved from https://www.lvm.fi/-/valtion-kyberturvallisuusjohtaja-on-nimitetty-1033603

Mäkinen, J. 2016. Cyber threats against critical infrastructure-Is there a need for national programme? Bachelor´s thesis. Laurea University of Applied Sciences, Degree Programme in Security Management. Accessed on 2 March 2021. Retrieved from http://urn.fi/URN:NBN:fi:amk-2016052910640

National Emergency Supply Agency. 2018. *Security of Supply Scenarios 2030*. Accessed on 25 October 2020. Retrieved from https://cdn.huoltovarmuuskeskus.fi/app/uploads/2018/09/06091431/Eng-Scenarios-2030.pdf

National Emergency Supply Agency. 2020. *Kyberturvallisuuden nykytila eri toimialoilla – Kartoituksen keskeiset havainnot* [Present condition of cyber security in different sectors – Key observations of the study]. Results of a study conducted by Digipool of National Emergency Supply Agency. Accessed on 22 October 2020. Retrieved from https://www.huoltovarmuuskeskus.fi/a/johdon-ohjaus-on-ratkaisevaa-yrityksen-kyberkestavyyden-kannalta

National Emergency Supply Agency. N.d.a. *Huoltovarmuuskeskuksen rooli* [The role of National Emergency Supply Agency]. A webpage on National Emergency Supply Agency's website. Accessed on 19 April 2021. Retrieved from

https://www.huoltovarmuuskeskus.fi/toimialat/energiahuolto/huoltovarmuuskeskuksen_rooli

National Emergency Supply Agency. N.d.b. *Sektori ja poolit* [Sectors and poles]. A webpage on National Emergency Supply Agency's website. Accessed on 19 April 2021. Retrieved from https://www.huoltovarmuuskeskus.fi/toimialat/energiahuolto/sektori-ja-poolit

National Emergency Supply Agency. N.d.c. *Toimintaa ohjaavat lait* [Enforced legislation]. A webpage on National Emergency Supply Agency's website. Accessed on 19 April 2021. Retrieved from https://www.huoltovarmuuskeskus.fi/toimialat/energiahuolto/toimintaa-ohjaavat-lait

National Institute of Standards and Technology. 2018. NIST Cybersecurity Framework. New to Framework. A page on National Institute of Standards and Technology website. Accessed on 18 April 2021. Retrieved from https://www.nist.gov/cyberframework/new-framework

Office of Data Protection Ombudsman. 2020. Office of the Data Protection Ombudsman's sanctions board imposed three administrative fines for data protection violations. A publication on office of Data Protection Ombudsman's website 22.5.2020. Accessed on 19 February 2021. Retrieved from https://tietosuoja.fi/en/-/tietosuojavaltuutetun-toimiston-seuraamuskollegio-maarasi-kolme-seuraamusmaksua-tietosuojarikkomuksista

Olin, P. & Rousku, K. 2018. *Kyberturvallisuusstrategia ja sen toimeenpano-ohjelma Julkisen hallinnon digiturvallisuuden teemakuukausi.* [Cyber Security strategy implementation program] Accessed on 13 March 2019. Retrieved from https://vm.fi/documents/10623/10333141/10_Kimmo_Rousku_VRK_Kyberturvallisuusstrategia_eteneminen_JHDTTK_0810_2018.pdf/9467b6b2-016e-4a70-9bbc-f4555452249c/10_Kimmo_Rousku_VRK_Kyberturvallisuusstrategia_eteneminen_JHDTTK_0810_2018.pdf.pdf

Pahkala, T., Uimonen, H., & Väre, V. 2018. Flexible and customer-centred electricity system; Final report of the Smart Grid Working Group. Publications of Ministry of Economic Affairs and Employment 39/2018. Accessed on 25 November 2020. Retrieved from http://urn.fi/URN:ISBN:978-952-327-352-8

Partanen, J. 2018. *Sähkönsiirtohinnat ja toimitusvarmuus* [Electricity transmission pricing and security of supply]. Publications of Ministry of Economic Affairs and Employment 43/2018. Accessed on 15 December 2019. Retrieved from http://urn.fi/URN:ISBN:978-952-327-356-6

Prent, B. 2019. Cyber security – Fundamentals of the Smart Grid 2019. Fundamentals of the Smart Grid 2019 conference publication on Smart Grid Forum's website. Accessed on 13 January 2021. Retrieved from https://www.smartgrid-forums.com/past-presentations

Pullinen, M-J. 2012. *Kriittisten tietojärjestelmien suojaaminen kyberuhilta* [Protection of Critical Information Systems against Cyber Attacks] Master's thesis. Laurea University of Applied Sciences, Degree Programme in Information Technology.

Accessed on 3 March 2021 Retrieved from http://urn.fi/URN:NBN:fi:amk-2012060611923

Rubin, A. N.d. *Tulevaisuudentutkimus tiedonalana* [Futurology as dicipline]. Accessed on 16 November 2020. Retrieved from https://tulevaisuus.fi/perusteet/tulevaisuudentutkimus-tiedonalana/

Sallos, M.P., Garcia-Perez, A., Bedford, D. and Orlando, B. 2019. Strategy and organisational cybersecurity: a knowledge-problem perspective. Journal of Intellectual Capital. Accessed on 11 November 2020. Retrieved from https://janet.finna.fi, Emerald Insight. doi: 10.1108/JIC-03-2019-0041

SFS-EN ISO/IEC 27000:2020. *Information technology. Security techniques. Information security management systems. Overview and vocabulary.* Finnish Standards Association SFS. Approved 28 February 2018. 2nd ed. Accessed on 3 January 2021. Retrieved from https://janet.finna.fi, SFS Online

SFS-EN ISO/IEC 27001:2017. Information technology. Security techniques. Information security management systems. Requirements. Finnish Standards Association SFS. Approved 3 March 2017. 1st ed. Accessed on 3 January 2021. Retrieved from https://janet.finna.fi, SFS Online

Siilasmaa, R. 2020. *Paranoidin optimistin päiväkirja, vieraana Risto Siilasmaa* [Diary of a paranoid optimist]. An internet podcast of F-Secure published 20th August 2020. Accessed on 13 November 2020. Retrieved from https://www.f-secure.com/fi/business/podcasts/herrasmieshakkerit

Silfversten, E., Jordan, V., Martin, K., Dascalu, D. & Frinking, E. 2020. Cybersecurity: A state-of-the-art review: phase 2. Accessed on 2 January 2021. Retrieved from http://hdl.handle.net/20.500.12832/3016

Siltala, J. 2020. *Emergency and Restoration verkkosääntö – vaatimukset ja toimeenpano Suomessa* [Emergency and restoration network code – requirements and implementation in Finland]. A publication of Fingrid. Accessed on 7 April 2021. Retrieved from https://www.fingrid.fi/globalassets/dokumentit/fi/sahkomarkkinat/verkkosaannot/nc-er-toimeenpano-perustietopaketti-julkinen.pdf

Smart Grid Task Force Expert Group 2. 2019. Recommendations to the European Commission for the Implementation of Sector-Specific Rules for Cybersecurity Aspects of Cross-Border Electricity Flows, on Common Minimum Requirements, Planning, Monitoring, Reporting and Crisis Management. Accessed on 14 March 2021. Retrieved from https://ec.europa.eu/energy/sites/default/files/sgtf_eg2_report_final_report_2019.pdf

The Guardian. 2020. 'Shocking' hack of psychotherapy records in Finland affects thousands. A news on Guardian's website on 26.20.2020. Accessed on 3 January 2021. Retrieved from https://www.theguardian.com/world/2020/oct/26/tens-of-thousands-psychotherapy-records-hacked-in-finland

The Security Committee. 2013. *Suomen kyberturvallisuusstrategia* [Finland´s Cyber Security Strategy]. Accessed on 13 December 2019. Retrieved from https://turvallisuuskomitea.fi/suomen-kyberturvallisuusstrategia/

The Security Committee. 2017. *Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017 – 2020* [Finnish cyber security strategy implementation program 2017-2020]. A publication of the Security Committee. Accessed on 13 December 2019. Retrieved from https://turvallisuuskomitea.fi/wp-content/uploads/2018/02/Toimeenpano-ohjelma-2017-2020-final.pdf

The Security Committee. 2018. *Kyberturvallisuuden sanasto* [Vocabulary of Cyber Security]. 2018. A publication of The Security Committee. Accessed on 12 June 2020. Retrieved from https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/

Tuomi, J. & Sarajärvi, A. 2018. *Laadullinen tutkimus ja sisällönanalyysi* [Qualitative research and content analysis]. 2nd ed,. Rev. Ed. Helsinki: Tammi

Vacca, J. R. 2017. Computer and information security Handbook. Third edition. Retrieved from https://janet.finna.fi, ProQuest Ebook Central. doi: 1195617

Valli, R. & Aarnos, E. 2018. *Ikkunoita tutkimusmetodeihin: 1, Metodin valinta ja aineistonkeruu: virikkeitä aloittelevalle tutkijalle* [Windows to research methods 1: choice of the method and collection of data: stimulus for an aspiring researcher] 5th ed,. Rev. Ed. Jyväskylä: PS-kustannus.

Vepsäläinen, J. 2017. *Energia-alan osaamistarpeet tulevaisuudessa* [Energy sector future competence needs]. Report of Finnish National Agency for Education study. Accessed on 6 November 2020. Retrieved from https://www.oph.fi/fi/tilastot-ja-julkaisut/julkaisut/energia-alan-osaamistarpeet-tulevaisuudessa

Warner, A. G. 2010. Strategic analysis and choice: A structured approach. Accessed on 13 March 2021. Retrieved from https://janet.finna.fi, ProQuest Ebook Central. doi: 8765

Wilczek, M. 2020. Average Cost of a Data Breach in 2020: $3.86M. A publication on DarkReading website on 24.8.2020. Accessed on 13 March 2021 Retrieved from https://www.darkreading.com/vulnerabilities---threats/advanced-threats/average-cost-of-a-data-breach-in-2020-$386m/a/d-id/1338660

World Economic Forum. 2012. *Global Risks 2012.* A world Economic Forum report. Accessed on 29 September 2020. Retrieved from http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf

World Economic Forum. 2014. *Global Risks 2014.* A world Economic Forum report. Accessed on 29 September 2020. Retrieved from http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

World Economic Forum. 2019. *The Global Risks Report 2019 - Future Shocks.* Accessed on 29 September 2020. Retrieved from https://www.zurich.com/en/knowledge/topics/global-risks/the-global-risks-report-2019-future-shocks

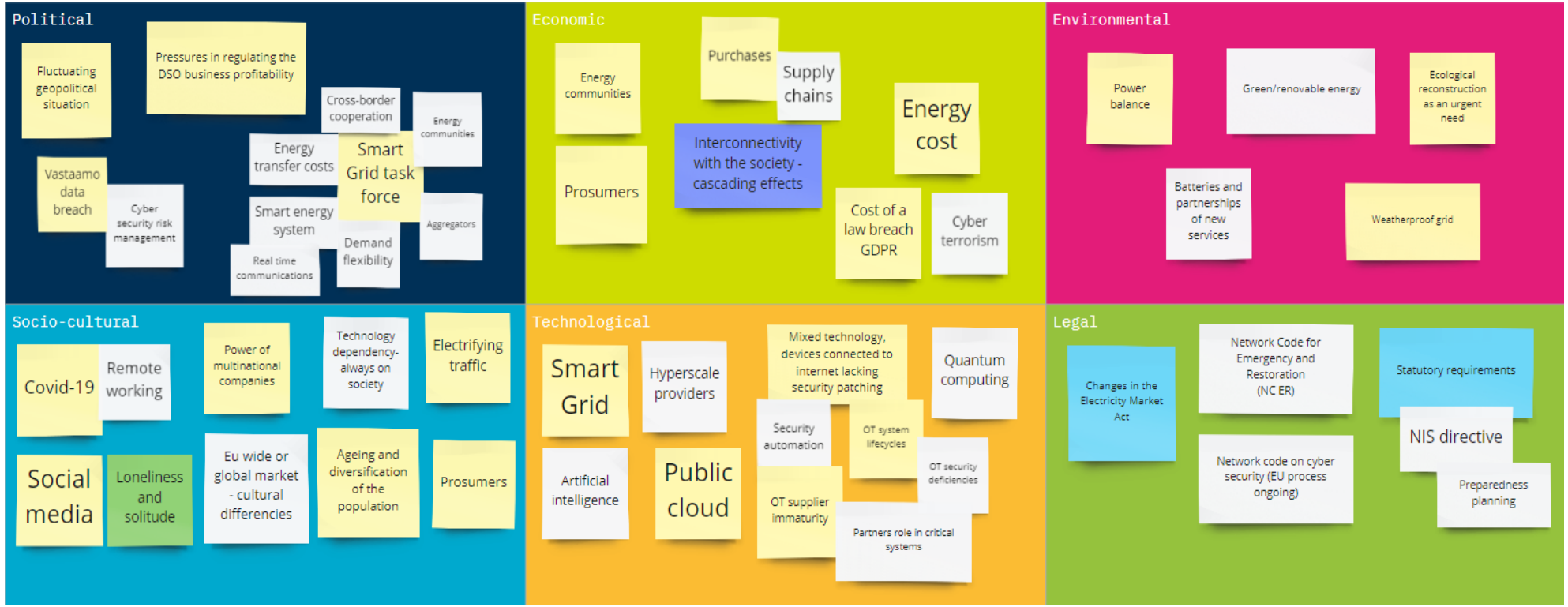
World Economic Forum. 2020a. *Cyber Resilience in the Electricity Ecosystem: Playbook for Boards and Cybersecurity Officers*. A world Economic Forum report.

Accessed on 20 September 2020. Retrieved from https://www.weforum.org/reports/cyber-resilience-in-the-electricity-ecosystem-playbook-for-boards-and-cybersecurity-officer

World Economic Forum. 2020b. *The Global Risk Report 2020.* A world Economic Forum report. Accessed on 29 September 2020. Retrieved from https://www.weforum.org/reports/the-global-risks-report-2020

Appendices

Appendix1. PESTLE Analysis



Appendix 2. Questionnaire of the Interviews

1. What are the changes occurring in the energy sector which will clearly influence the future of electricity distribution? (The below table of the change drivers was included in the material provided)

Topic	Factor
Political	Geopolitical Changes
Political	The Security of Supply
Political	DSO´s Role in the Future
Political	Data and Information Security Requirements
Economic	Prosumerism
Economic	Future Energy Consumption Needs
Economic	Cloud Adoption for Business Services
Socio-cultural	Influence of social media and Always on Society
Socio-cultural	The Dependency of Technology
Socio-cultural	Smaller Households
Technological	Cyber Environment Partnerships
Technological	Smart Grid
Technological	Energy System Lifecycles
Technological	New technologies like AI and Quantum Computing
Technological	Digital Self-sufficiency
Legal	Changes in Regulation
Environmental	Ecological Reconstruction
Environmental	Social Responsibility
Environmental	Green/removable Energy

2. Which weak signals visible today will significantly affect electricity distribution in the future?
3. Which of the changes you selected will influence the energy sector's cyber security 3 to 5 years from now?
    1. Do you think that the influence of these changes will be visible only later and if so, when?
4. Which factors are emphasized in cyber security?
5. Which cyber security threats are the most significant in the electricity distribution business? (The below picture of the threats was included in the provided material)
    a) Choose the most significant threats (8 + two own threats) and explain the reason for your answer.
    b) Set the threats in order and give a reason for your answer


OT system lifecycles, missing security by design
Cyber security culture, knowledge and practises
IT and OT cyber security competence
Cyber and human intelligence
Russia
China
Cyber crime, terrorism and virtual war
Cloud computing
Cyber security architecture
Resilience plans
Management´s commitment
Increasing Regulation
Remotely controlled Intelligent devices including AMR meters
Interconnectivity and interdependent bidirectional smart grid
Number of stakeholders in Elenia´s cyber environment
COVID-19
Automation, IoT
New technologies, AI, Quantum Computing
Microgrids and energy production
Supply chains
Unpredicted changes in the DSO´s environment requiring development
Globalization
Social media influence
Always on society, technology embedded in everything
Ageing of population

Appendix 3. Transcription of the First Interview

Interview with a Chief Information Security Officer of a DSO in Finland

Date: 22 March 2021

Content summary:

1. Changes in the energy sector
   - Increase in EU wide transmission network interconnectivity will influence the future.
   - Increase of solar and wind power production and transmission of these energies.
   - Increase in small scale production. People will be tempted to install solar panels or wind power which will produce electricity towards the grid also.
   - Increase in electric cars will enable a reserve battery, but also cause load peaks at times. This is also a cyber security concern.
   - Regulation will increase and will influence cyber security since electricity distribution is increasingly vital for society. The tightening of the regulation may occur only after a major cyber security incident. Smaller DSOs may not be able to cope with the requirements of the regulation.

2. Weak signals
   - Changes in the electricity production methods, increase in hydrogen maybe in ten years. Hydrogen would offer possibilities to store the produced energy. Hydrogen is a possibility since our capability to produce lithium batteries is limited due to the limited number of natural resources.
   - Energy communities could affect the DSOs monopoly status.
   - COVID-19 may have changed people's willingness to live and work more in rural areas. The houses or cottages previously used only in summertime could be equipped with, for example, geothermal heating which is controlled at a distance at any time.

3. Changes influencing the energy sector's cyber security 3 to 5 years from now
   - The interconnectivity of all electricity networks. An actor with missing security controls could affect the operations of the whole network including the transmission system operator of Finland.
   - The growing role of consumers.
   - The growing number of new services and possible vulnerabilities of the interconnections, for example unprotected cloud which could enable the controlling of the household's systems at a distance. This could affect the system largely and cause important system failures. The responsibility questions are important.
   - New service creating pioneers should be cyber security aware and the security by design principles should be applied to all new services.

3.1 Changes visible only later

- Increase in electric cars when tens of thousands of electric cars are in use. The threat comes from the possibility to influence and control the loads in a harmful way.
- The new business possibilities are enabled by the growth of the electric car market. For example, the vulnerabilities of the infrastructure used to load cars. If the actors of this new market are not taking care of cyber security, there is a potential of an important number of vulnerable devices installed.

4. Emphasized cyber security factors

- Cyberphysicality in two ways. First the automation which is controlling the devices of the physical world and secondly the physical security of, for example the substations. A comprehensive approach should be taken to security. Cyber security is not only a technical question including network and information system security, but physical security is also equally important.
- The operations of the partners and the suppliers are in a significant role. Cyber security should be considered starting from the contract requirements. The instructions and the awareness of security should be considered in the field operations since the partners are working every day in the field and are continuously in contact with the cyberphysicality. The components affecting the cyber security of the distribution networks are scattered around the distribution network and the contractors are working closer than the DSO personnel with these components.
- The lifecycle of the components and systems. The possibility to divest the obsolete systems more often than the actual regulation permits.
- The vulnerable systems in the field where no security is implemented; Purdue Enterprise Reference Architecture layers 0 and 1. The security of these devices should be assured with other controls, for example physical controls.

5. The most significant cyber security threats in the electricity distribution business

- Supply chains
- Internet of things
- OT system lifecycles – missing security by design
- Different conception of the security in OT and IT. The missing dialogue led by the IT department´s cost driving initiatives to consolidate everything. For example, the use of only one remote connection solution for all different business needs. COVID-19 has brought out needs to allow various kinds of remote connections.
- In the OT, a misconception is prevailing: the OT networks are isolated. The seemingly isolated OT networks are not isolated. Information is transmitted in both directions from OT to IT and the other way round.
- Advanced cyber threats. Organised criminals could have a significant possibility to earn money if the extortion would be extended to the operational networks. Now extortions are occurring in the IT networks and systems.

- The increasing use of the cloud services, both the public and private clouds. The systems fulfilling the business development requirements can no longer be implemented in the on-premises data centres. The clouds are proposing the needed machine learning capabilities. The questions are, how and under what conditions the cloud can be used for OT systems. Even if in the private clouds the tenants are separated, there might be vulnerabilities allowing access from one tenant to another. Private clouds are sales talk and doesn´t really exist.
- AMR meters. Hundreds of thousands of meters are on the field operable at a distance. The cyber threats are significant in both directions, towards the customers and the electricity grid.
- Young generation not understanding the basics of the TCP/IP and willing to use mobile phones for everything. The segregated systems are disappearing together with the older generation who understood the risks related to the accessible anywhere and interconnected systems.
- The physical geographical dispersion of the electricity network. A malicious actor has plenty of time to work before being noticed.
- Data and telecommunications. Are the black fibres so secure as we think they are? These are operated by telecommunication operators and are not controlled by the companies themselves. Are the communications end-to-end encrypted or are there possibilities to interfere or eavesdrop on these connections? This is a black box today.
- Management´s commitment is obvious, but so important to mention.

Appendix 4. Transcription of the Second Interview

Interview with a System Developer working with strategic business projects for a DSO in Finland

Date: 23 March 2021

Content summary:

1. Changes in the energy sector

- Segregated information systems will be combined with larger entities. Until now the information systems have usually served one purpose. In the future, with the possibilities of big data, the same information system will be used to serve diverse needs. This is a possibility for the energy sector, but the outcome of this change is yet unclear.
- The changes and challenges of the future are connected to how to handle this merge of the systems into one. Data will be collected in a data lake and machine learning is applied to the data; the outcome will be controlling the business.
- The electricity network must be designed to incorporate production coming from energy communities and small-scale production.
- Electric cars will increase energy consumption. In the cities there will be sort of service stations to charge cars, but the rural areas will also require the possibility of charging at home. The peak loads are expected when the people arrive at home instead of only during saunas. Will it be possible to regulate or stagger the consumption to avoid the load peaks?
- Small-scale production is more easily controllable for the energy sector than electric cars.
- The regulatory changes in energy pricing will influence the development of energy communities and small-scale production. These are alternatives for consumers whereas electric cars are the future, no combustion engine cars will be produced at some point.
- The extensive use of data collected from the electricity grid, different sensors and components will increase. New technologies would enable business development, but data security or copyright problems could emerge, limiting the business possibilities.
- The use of artificial intelligence is increasing but the limits and rules to use its capabilities are not yet defined.

2. Weak signals

- When the decentralised small-scale energy production and the number of electric cars increase, the electricity distribution network can´t be operated with the present state´s segregated systems. These are the drivers for the change and the use and combination of the data for automated decision making is the solution. The electricity network must be designed to guarantee the security of supply and at the same time bottlenecks and cost efficiency

must be handled to avoid the oversizing of the network and unnecessary investments.

3. Changes influencing the energy sector's cyber security 3 to 5 years from now

- The use of data from segregated systems. The data is transferred to a larger entity, processed with AI, and fed back to the process. How to ensure the security of the process, the accuracy and correct use of the AI etc. Such a process would control the entire system in the future. This is the most important question concerning cyber security.

3.1 Changes visible only later

- Not answered separately, included in the content of this appendix.

4. Emphasized cyber security factors

- Not answered separately, included in the content of this appendix.

5. The most significant cyber security threats in the electricity distribution business

- Each of the threats presented in the material received before the interview are manageable.
- The development pace of technology and electronics is fast, and their lifecycle is at most 20 years. The threats can be handled in newly implemented systems.
- Diverse cultures and restrictions apply in various parts of the actual systems. A new architecture will emerge when the data of the actual systems are transferred to the cloud and the AI is used to process the whole data.
- IT and OT are separated today but is that so in the future?
- If the OT has been so far a system controlling the operations of the transmission network, tomorrow with the AI combined, it may expand to a maintenance system.
- The process could be developed further, and the system could also create work orders and decide the necessary investments. How to separate, what is IT and OT in this probable future scenario.
- With AMR meters this is already occurring. The meters are controlled using interfaces at a distance and can make decisions unattended. To handle the large quantity of information, clouds are used.
- Supply chain and partnerships. If the system is not bought as an overall service, it is challenging to handle the separate lifecycles of the different vendors if the organization doesn´t want a vendor lock-in situation. How to guarantee the security of the entire system if one part is not under support contract anymore. The lifecycle of investments is also playing a role in this complex interconnected system.

Appendix 5. eDelphi Panel Questions

1. Cyber Secure World is Ready

Kyberturvallinen maailma on valmis

Vuonna 2025 kyberturvallisuus on sisäänrakennettu energiasektorin toimintaan vastaavasti kuin työturvallisuus.

Kyberturvallisuuden sanaston mukaan kyberturvallisuus on tavoitetila, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan.

Kyberturvallisuuteen kuuluvat toimenpiteet, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia.

Kybertoimintaympäristön toiminnan häiriytyminen aiheutuu usein toteutuneesta tietoturvauhkasta, joten kyberturvallisuuteen pyrittäessä tietoturva on keskeinen tekijä. Tietoturvan lisäksi kyberturvallisuuteen pyritään muun muassa toimenpiteillä, joiden tarkoituksena on turvata häiriytyneestä kybertoimintaympäristöstä riippuvaiset fyysisen maailman toiminnot.

Siinä missä tietoturvalla tarkoitetaan tiedon saatavuutta, eheyttä ja luottamuksellisuutta, kyberturvallisuus tarkoittaa digitaalisen ja verkottuneen yhteiskunnan tai organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin.

2017 Sounil Yu käsitteli RSA-konferenssin esityksessään "Solving Cybersecurity in the Next Five Years" militaaristrategiasta tutun OODA-loopin merkitystä kyberhyökkäyksessä ja kyberturvallisuuden historiaa NISTin kyberturvallisuuden viitekehyksen kautta.

Miten todennäköisenä ja toteutettavana pidät kyberturvallisuuden ratkaisemista energiasektorilla vuoteen 2025 mennessä? Perustele vastauksesi kommenteissa!

Konferenssin tallenne on halutessasi katsottavissa alla.

Thesis: In 2025 cyber security is in-built in the operations of the energy sector likewise safety.

Question: How likely and possible is it to solve the cyber security by 2025? Remember to confirm your arguments!

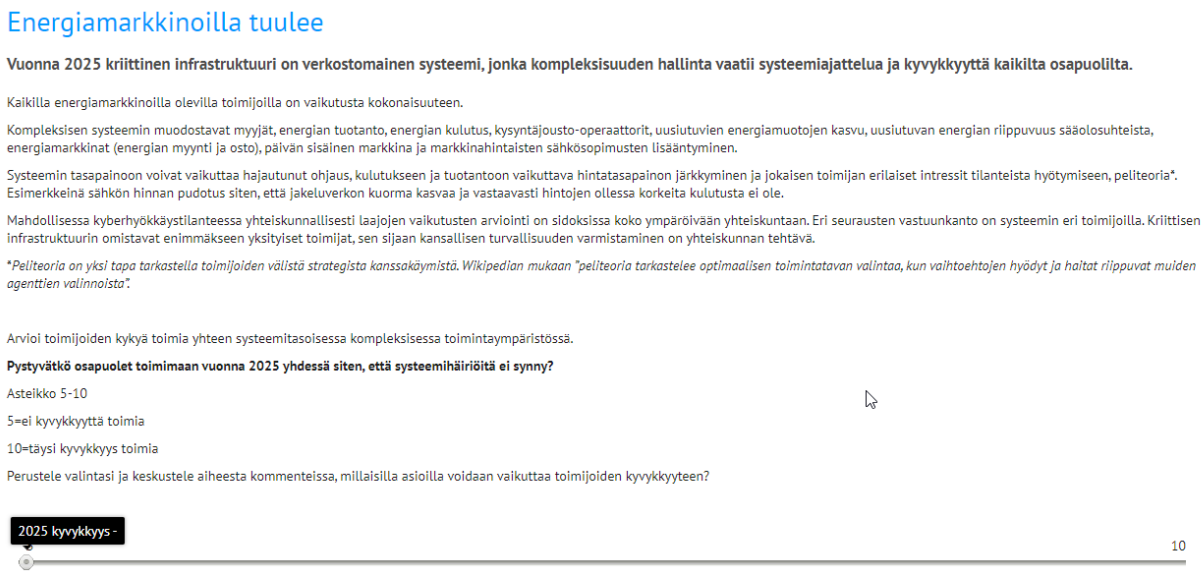
Details: Description of cyber security is presented and a brief introduction to Sounil Yu's RSA conference presentation entitled "Solving Cybersecurity in the Next Five Years."

2. Freezing Hell vol. 2

Thesis: A scenario describing a cyber-attack on the smart meter infrastructure is presented in this question. For security reasons the content of the scenario is not opened in detail in this report.

Question: How likely and possible the depicted scenario is? Remember to confirm your arguments!

3. Windy Energy Markets



Thesis: In 2025 the critical infrastructure is a network-like system. To manage the complexity of this system, ability and systems thinking is required from each actor of the system.

Question: Are the actors of the system capable of operating together so that system level interruptions will not occur? Evaluate the capability on the scale from 5 to 10 where 5 = no ability, 10 = fully able. Remember to confirm your arguments!

Details: Each actor of the energy market has an importance in the functioning of the system. The complex system is formed by the sellers of energy, energy production, energy consumption, flexibility operators, increase of the renewable energy, renewable energy dependence of the weather conditions, energy market (selling and buying), intraday market and market price contracts.

Factors affecting the balance of the system are decentralized controls, disturbances related to the balance of production and consumption and different interests of the actors, see game theory. A disturbance in the balance can result in low energy prices which could increase the consumption or when the energy prices are high the consumption is low.

In case of a cyber-attack the evaluation of the impact is connected to the whole society. The actors of the system have different responsibilities. The critical infrastructure is owned by private companies whereas the security of the nation is the responsibility of the society.

4. Money or your life

Rahat tai henki

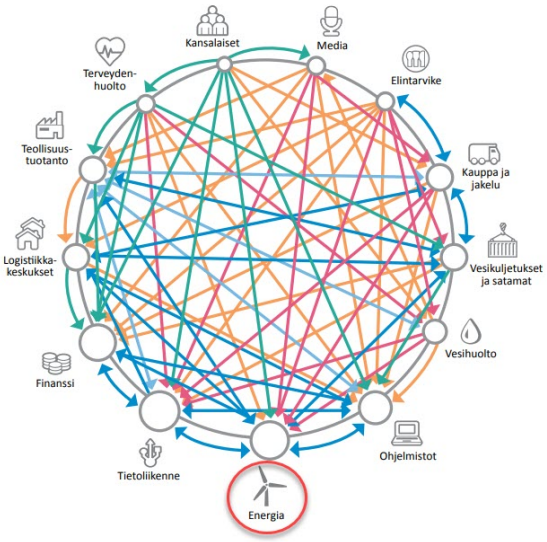
Millä tekijöillä varmistetaan tuotantoteknologian ja sähköverkkojen automaation kyberturvallisuus vuonna 2025? Poimi viisi tärkeintä tekijää!

Kyberhyökkäyksen motiivina on useimmiten taloudellisen hyödyn tavoittelu. Vuonna 2020 puolet hyökkäyksistä olivat kiristyshyökkäyksiä.

Energiamurroksen myötä toiminen nykytilan pitkien elinkaarten siiloutuneissa järjestelmissä tulee haasteelliseksi. Tuotantoteknologiat tulevat yhä lähemmäs IT-teknologioita. Miten tulevaisuuden sähköverkosta laajasti kerättävää tietoa käsitellään mm. tietosuojasäännösten mukaisesti siten, että liiketoiminnan kehitys on mahdollista ja uusien teknologioiden mahdollisuudet saadaan hyötykäyttöön? Miten kiristyshyökkäykset OT-ympäristöissä vältetään?

Huoltovarmuusorganisaation Digipoolin kyberturvallisuuden nykytila eri toimialoilla -kartoituksessa kuvataan toimialariippuvuuksia. Alla olevassa kuvassa energian solmun koko kuvaa energian tärkeyttä riippuvuusverkostossa. Mahdollisen kiristyshyökkäyksen vaikutukset voisivat ulottua koko verkostoon, koska automaatiolla ohjataan fyysisen maailman laitteita.

Toimialariippuvuudet



Millä tekijöillä varmistetaan sähköverkkoihin liittyvän automaation kyberturvallisuus vuonna 2025?

Valitse viisi tärkeintä tekijää, joilla on merkitystä automaation kyberturvallisuuden varmistamisessa.

Jos listalta puuttuu jokin mielestäsi oleellinen tekijä, ehdota sitä kommenteissa!

Perustele valintasi ja keskustele aiheesta kommenteissa.

- [ ] Regulaatio
- [ ] Tietoisuus
- [ ] Elinkaaren lyhentäminen
- [ ] Toimittajien, laitteiden ja sopimusten vaatimukset
- [ ] Tekoäly, big data ja automatisoitu päätöksenteko
- [ ] Pilvipalvelut
- [ ] Osaaminen
- [ ] Kumppanuudet
- [ ] Tietoturvateknologia
- [ ] Yhteistyö verkostoissa
- [ ] Kyberresilienssi
- [ ] Muu, mikä?

Thesis and question: Which factors are assuring the OT cyber security in 2025?

Choose five most principal factor! The factors are

- Regulation
- Awareness
- Shorter life cycle
- Requirements of the suppliers, hardware, and software
- AI, big data, and automated decision making
- Cloud services
- Competence
- Partnerships
- Information Security Technology

- Collaboration in co-operation networks
- Cyber resiliency
- Other?

Details: Motivation of a cyber-attack is usually economical profit. Half of the attacks in 2020 were extortions.

With the energy sector revolution, the operations in the systems with long lifecycles become challenging. OT technologies are coming closer to the IT technologies. How to protect and handle the information collected from the future electric grid so that the regulatory requirements e.g., GDPR, are not violated and the business development is possible enabling the use of new technologies. How to prevent the extortion in operational networks?

5. Towards the highway of the future

Kohti tulevaisuuden valtatietä

Miten todennäköisenä ja toivottavana pidät alla kuvattua skenaariota?

Digitaalinen kaksonen kyberturvallisuuden varmistajana 2025

Energiasektorilla on digitaalinen kaksonen koko siirtoverkosta ja siihen vaikuttavista voimista, mukaan lukien AMR-mittarit. Toteutuksella voidaan simuloida turvallisesti erilaisia systeemin toimintaan vaikuttavia tilanteita ja uutta teknologiaa. Kaksonen auttaa havaitsemaan ongelmia ennalta, suunnittelemaan tarvittavaa regulaatiota ja määrittämään tietojärjestelmille asetettavia vaatimuksia. Kaksosen avulla varmistetaan jokaisen toimijan edellytykset liittyä osaksi kokonaisuutta.

Kuinka todennäköinen ja toivottava kuvattu skenaario on? Perustele näkemyksesi kommenteissa!

Thesis and question: Digital twin is ensuring the cyber security by 2025. How likely and desirable the depicted scenario is? Remember to confirm your arguments!

Details: Energy sector has a digital twin of the entire electricity network covering all the parties, including smart meters. With the twin simulations of different scenarios and new technologies can be tested safely. With the help of the twin problems can be anticipated and planning of required regulation can be done. Each party willing to operate in the Finnish electricity market must comply with the regulation verified with the twin.

Appendix 6. eDelphi Panel Invitation Email and Email from eDelphi

Hei,

Tervetuloa mukaan sähkönjakelun kyberturvallisuutta käsittelevään Delfoi-paneeliin. Paneeli aukeaa tänään ja on avoinna 21.4. asti.

Paneeliin vastaaminen tapahtuu eDelphi-työkalussa. Vastaamaan pääset henkilökohtaisen linkin kautta, joka tulee hetken päästä sähköpostiisi eDelphi-työkalusta otsikolla ”Kutsu eDelphi-paneeliin Elämää sähköistämässä". Voit vastata kaikkiin kysymyksiin yhdellä kertaa tai jatkaa myöhemmin. Paneeliin kannattaa säännöllisesti palata tutustumaan uusiin kommentteihin ja tarkastella omia vastauksia, muuttuvatko ne, kun pohdit kysymyksiä tarkemmin ja tutustut toisten kommentteihin. Vastausta siis saa muuttaa ja omia kommentteja täydentää.

Paneelin osallistujat koostuvat Suomen huippuosaajista energiasektorilta, kyberturvallisuudesta, tutkimuksesta ja kehityksestä sekä viranomaistahoilta. Olet siis hyvässä seurassa keskustelemassa, millaisia askelia erityisesti jakeluverkkoyhtiössä tulisi ottaa kyberturvallisuuden varmistamiseksi tulevien vuosien aikana.

Paneeliin vastaaminen ja kommentointi tapahtuvat täysin anonyymisti. Osallistujien henkilöllisyys ei paljastu missään vaiheessa prosessia.

Delfoi on luonteeltaan iteratiivinen prosessi, joka tyypillisesti koostuu useista kierroksista. Tässä paneelissa on kyse yhden kierroksen reaaliaikaisesta Delfoista eli kaikki vastaukset ovat koko paneelin ajan nähtävillä ja kommentoitavissa.

Toimin paneelin managerina ja paneelin edetessä viestin tilanteesta, miten vastaukset jakautuvat, onko jokin aihe herättänyt erityisesti keskustelua sekä kutsun tutustumaan kommentteihin ja tarkastamaan omaa näkökantaa.

Huomioithan, että paneelin sisältö on luottamuksellinen, ja vastaamalla paneeliin sitoudut paneelissa kuvattuun TLP-luokitukseen. Saat käyttöösi julkisen yhteenvedon paneelin tuloksista paneelin päätyttyä.

eDelfin sivulla on lisätietoa Delfoi-metodista, mikäli haluat perehtyä metodiin tarkemmin.

Jos kirjautumisessa tai eDelphi-ohjelmiston käytössä ilmenee ongelmia, laitathan siitä viestin minulle ja ratkaistaan ongelma pikaisesti.

Kevätauringon siivittämänä toivon ajatuksia herättäviä hetkiä kyselyn parissa, syty kysymyksistä ja toisten ajatuksista, keskustele ja kommentoi aktiivisesti!

Anonyymisiin tapaamisiin paneelissa!

Elina Dauchy

E-mail from eDelphi

Tervetuloa paneeliin [PANEELIN NIMI]!

Paneelissa tarkastellaan energiatoimialan kyberturvallisuuden tulevaisuuden kehitystarpeita sähköverkkojen näkökulmasta.

Kaikki vastaukset ovat täysin anonyymeja, henkilöllisyytesi ei paljastu missään vaiheessa prosessia.

Suuret kiitokset, että annat asiantuntemuksesi paneelin käyttöön!

Henkilökohtainen linkkisi paneeliin: [HYVÄKSYMISLINKKI]

Huomaa, että linkki on henkilökohtainen. ÄLÄ siis JAA sitä muille, ettet menetä tietoturvaasi ja anonymiteettiäsi!

Anonyymisiin tapaamisiin paneelin parissa,

[LÄHETTÄJÄN NIMI]

eDelphi-tietosuojakäytäntö on täysin GDPR (General Data Protection Regulation: EU Regulation 2016/679) -yhteensopiva (ks. https://www.edelphi.org/privacypolicy.page).

Appendix 7. Communication at mid-point of the Panel

Hei,

paneeli on ollut avoinna viime keskiviikosta lähtien ja keskusteluissa on tuotu hyvin perusteltuja näkemyksiä esille. Kiitos kaikille tähän mennessä osallistuneille!

Paneeli on avoinna vielä viikon, joten on hyvin aikaa käydä katsomassa keskustelujen kehittymistä, mielipiteiden jakautumista ja osallistua, jos et ole vielä ehtinyt. Linkki paneeliin on henkilökohtainen ja löytyy sähköpostistasi otsikolla ”Kutsu eDelphi-paneeliin Elämää sähköistämässä".

Muutamia nostoja paneelin tilanteesta ja uusia kysymyksiä:

- Kyberturvallisuuden ratkaisemisessa energiasektorilla painottuvat muutokset, uudet toimijat, teknologinen kehitys ja aiheen merkityksellisyys. Paneelissa on hajontaa arvioitaessa kyberturvallisuuden toteutettavuutta vuoteen 2025 mennessä. Sivulle 2/7 on tuotu lisäkysymys kommentteihin kyberturvallisuuden varmistamisen merkityksellisyydestä, käyttehän kertomassa mielipiteenne tähän näkökulmaan.

- Älykkäiden sähkömittareiden arvioinnissa hyökkäyksen kohteena painottuvat motiivit ja ihmisten toiminnan merkitys.

- Systeemiajattelun tueksi kompleksisuuden hallintaan on ehdotettu digitaalisen kaksosen toteutusta siirtoverkosta. Digitaalisen kaksosen toteuttamisesta on luotu lisäkysymys 6/7, arvioitavana todennäköisyys ja toivottavuus, käyttehän vastaamassa uuteen kysymykseen.

- Tuotannon ja automaation kyberturvallisuus varmistettaisiin tulevaisuudessa erityisesti regulaatiolla, toimittajien, laitteiden ja sopimusten vaatimuksilla sekä osaamisella.

Vielä on hyvin mahdollisuuksia päästä vaikuttamaan ja kertomaan rohkeasti omia mielipiteitä!

Hyvää loppuviikkoa toivottaen,

Elina