Cyber-Security in Digital Metering Value Chain for Mountain Landslide Warning

Mari Aarland, Jaziar Radianti, Terje Gjøsæter

Cyber-security in Digital Metering Value Chain for Mountain Landslide Warning

Mari Aarland[1], Jaziar Radianti[2] and Terje Gjøsæter[2]

[1] NC-Spectrum, Kviteseid, Norway
mari.aarland@nc-spectrum.no
[2] CIEM, University of Agder, Kristiansand, Norway
{jaziarr, terjeg}@uia.no

Abstract. The Norwegian Water Resources and Energy Directorate (NVE) are initiating a digitalization process that involves the use of a digital metering value chain and cloud computing. The main objective of this study is to investigate how NVE can ensure cyber-security in digital meters and the cloubased metering value chain for mountain landslide warning. The study is based on a qualitative approach including methods like document analysis and semistructured interviews used as input to a risk analysis based on the ISO 31000 standard. The risk analysis covered three different scenarios from NVE. Those three scenarios were internal, external Norwegian, and transnational value chains for metering landslide warning. The results of the risk analysis showed that the largest risk was loss of metering data caused by failures in complex digital value chains combined with the risk of human error. We concluded that the risk is significantly higher for the transnational digital value chains, and that the recommended risk mitigation is a combination of organizational and technical countermeasures.

Keywords: Risk assessment, Digital value chain, Critical infrastructure.

1 Introduction

The paradigm shifts of digital transformation that the society is experiencing comes with both opportunities and challenges. Amongst these challenges, cyber-security is very prominent, in particular in critical infrastructure. Critical infrastructures are defined by EU as [1, p. 3]:

> "an asset, system or part thereof located in Member States which is essential functions, health, safety, security, economic or social well-being people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those function."

A report from the Norwegian Institute of International Affairs (NUPI) highlights that the digital transformation in critical infrastructure poses greater vulnerabilities, and that cyber-security becomes an even more important aspect to prevent unwanted attacks on system weaknesses [2]. Digital transformation in critical infrastructure is the process of

implementing new technology in order to better collect, analyze and gather decision-making information [3].

The main contribution of this paper is to present a preliminary study on the risks involved in the digital transformation for The Norwegian Water Resources and Energy Directorate (NVE), specifically in their landslide warning system. NVE is an organization responsible for critical infrastructure, amongst them the critical infrastructure called mountain landslide warning [4].

Digital transformation in this critical infrastructure involves implementing digital sensors and cloud computing in a digital metering value chain to support decisionmaking, which is the most important aspect to mountain landslide warning [3]. A digital value chain is a structure of deliveries between organizations where the delivery either is of a digital service, software or hardware. The digital value chain is characterized by three factors [5]:

1. Error occurs unexpectedly, and the error may spread instantly.
2. A service which is a part of the digital value chain is cross-sectorial, where the service is also subjected beneath different jurisdiction and supervisory regimes.
3. It is difficult to map out the vulnerability for the entire digital value chain.

The mountain Aknes based in Geiranger, is an unstable mountainside that could potentially send 54 million cubic meters of rock down towards the water, which could result in a tsunami wave as high as 85 meters. NVE's task is to conduct 24/7 surveillance of high-risk mountains like Aknes and inform the public about any changes to ensure the safety and security of the Norwegian population [6]. In addition, NVE is also responsible for other activities connected to mountain landslide warning. They are responsible for notifying the community if any circumstances change for the worse, this implies that the preparedness level is changing. They are also in charge of implementing countermeasures to prevent any harm upon life, environment and other valuable assets [7].

However, implementing new technology does not come without risk. Incidents or attacks on such high-risk objects could potentially harm up to 10 municipalities, making the digital metering value chain a critical infrastructure [6]. In order to protect such a critical infrastructure, this paper aims to highlight the challenges by conducting a risk assessment of the digital and cloud-based metering value chain for mountain landslide warning. Digital value chains today are already complex and vulnerable. According to a Norwegian Official Report (NOU) from the Norwegian government, the digital value chain is one of the main contributing factors for not being able to determine an organization's digital risk [8].

The rest of this article is organized as follows. Section 2 present previous studies in context of digital supply chain and background on risk management, Section 3 describes our risk analysis approach, Section 4 outlines the risk analysis process and results, Section 5 contains discussion, and our conclusions are presented in Section 6.

2 Previous Studies and Study Context

2.1 Previous studies

Previous studies have examined the advantages and values of using cloud infrastructures for delivering business services. Mohammed et. al., [9] for example, have reviewed and analyzed the grid and cloud market services, projects, tools and technologies, using value chain theories. The "value chain" term itself was made popular by Porter, who initially intended to introduce a template to analyze the value chain of manufacturers, which has to do with the increasing connectivity between value components and how the value is created and delivered [10]. Later, it has been used as value chain thinking, to analyze many interconnected value components and value creations, and has been adopted into broader applications such as digital value chains, and various contexts in information-communication technology settings such as cloud computing [9], [11].

Stanoevska-Slabeva et al. [11] look at the grid value chain models by including the linkages among the grid stakeholders or the value networks involving the flow of goods and revenues, flow of knowledge and other intangible benefits such as cobranding. It is presented as role-based value chain. The cloud services are not so much in the pictures, although the framework has introduced some Information Technology elements. Mohammed et al., e.g., propose a highly-connected three-layer cloud value chain model consisting of *business-oriented support services* (value added services, brokers and resellers, financial services, market place), *primary services* (hardware services, middleware services, grid middleware services, software services and data-content services), and *cloud-oriented support services* (technology operators, consultancy services, etc). In these two frameworks, the focus is mostly on the economic and business aspects of the supply chain. Giannakis et al., [12] proposed a novel cloud-based supply chain management system framework, by examining different *cloud service models* (i.e., Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS)) and *cloud-based approaches* (e.g., on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service), then link them to the supply chain responsiveness.

The notion of digital supply chain (DSC) is relatively new, it emerges with the development of new innovative technologies such as big data, cloud computing and internet of things, robotics, sensor technologies and trends such as digitalization and digital transformation. The overview of the application of DSC has been discussed in the literature e.g., by Büyüközkan, G., & Göçer, F. [13] and Ageron et al. [14]. The latter defines a digital supply chain as "the development of information systems and the adoption of innovative technologies strengthening the integration and the agility of the supply chain and thus improving customer service and sustainable performance of the organization". Büyüközkan, G., & Göçer, F. [13] add the features of DSC that include speed, flexibility, global connectivity, real-time inventory, intelligent, transparency, scalability, innovative, proactive and eco-friendly. DSC also involve the new emerging technologies mentioned earlier. In other words, DSC is a combination of supply chain management, technology implementation and digitalization.

The notion of cloud-based smart metering is introduced by Pau et al., [15]. The study emphasizes the architecture of the smart meter based on the cloud platform. Cybersecurity comes into the picture, especially in terms of selection of smart metering, which in this study, support secure and trusted communication among different components. However, the main goal is to demonstrate the architecture that can support different services for management and the automation of future distribution grids but is not linked to DSC. The idea of linking DSC with cybersecurity and disaster management is still limited. Indeed, in the literature, studies are available that link the block-chain technology to the supply chain [16], but mostly focus on how technically to apply blockchain distributed ledger technology to promote secure software and hardware in energy sector setting. Risk analysis is also often not a part of the picture of the DSC.

Our study focuses specifically on the cybersecurity in digital metering value chain and the risk management, which can be an initial effort to contribute to the research gaps in these three main areas: DSC, cybersecurity and risk/ disaster management. We take the case from the Norwegian experience in the digital metering value chain.

2.2 Study Context: Risk management in a Digital and Cloud-Based Metering Value Chain

The National Security Authority in Norway (NSM) points out in their report "Risiko 2020" [17] that one of the risk factors for national security in 2020 is the growing dependency of digital infrastructure and digital value chains that stretches across geographical borders. NVE is dependent upon the digital value chain suppliers to distribute their metering data for mountain landslide warning to satisfy their responsibility as surveillance authority for mountain landslide warning. However, a survey conducted by The Norwegian Center for Information Security in 2019 showed that as much as 69% of the Norwegian population lacked training on digital safety culture based on the last two years. This should be alarming news for NVE. When implementing technology into the digital and cloud-based value chain it changes the infrastructure and it affects the entire value chain. If the Norwegian population is not up to date with the evolving technology, they eventually pose a risk towards the value chain by making human errors [18]. Risk management for a digital value chain only works when the entire chain helps contribute with cyber security activities, and the consequences of poor digital safety culture can potentially lead to loss of life for the population living in the area around the unstable mountain. It is critical that the data collected from the unstable mountain is available at all time, continuously processed and consist of the correct metering value data.

NVE uses an operative national surveillance service that utilizes hydro metrological real-time data from the measuring station on each unstable mountain. The protecting and maintenance of the landslide warning is a collaboration between NVE, State Highway Authority, Meteorological Institute, Bane NOR, Geological Survey of Norway and NVE's Section for Landslide [7]. The digital value chain for metering mountain landslide warning can be divided into three different value chains: Internal, Norwegian supplier and Transnational. Transnational value chain means that an external supplier from

another country contributes to the value chain making the value chain cross national borders. These types of value chains can often lead to jurisdictional challenges [5].

The instruments used in the digital and cloud-based value chain is both digital and analogue devices to measure movements in the mountain. Instrument like Global Navigation Satellite System (GNSS), Ground-Based Interferometric Synthetic Aperture Radar (GB-InSAR), Satellite-Based Interferometric Synthetic Aperture Radar (SB-InSAR), laser, total station, extensometer, tension rod, tilt-meter, weather station, borehole instrument, seismic and webcam. The metering data is transmitted with the use of fiber cables, ADSL/DSL, wireless communication and satellite, where the communication goes through routers and switches distributed on the mountain [7].

The measuring instrument sends out data each day with updated information about the condition and any movements that may occur for the unstable mountain. It is essential that data collected is both correct and on time, because of NVE task to conduct 24/7 surveillance. These instruments must perform and be redundant for outer intervention so thorough investigation is needed into which factors that could potentially be the cause to the loss of data that must be presented on the website varmson.no. NVE ensures redundancy with the placement of at least three of more instruments together on the unstable mountain that measures the same risk object. However, these instruments are vulnerable to different types of influence and therefore it is important to identify these vulnerabilities. From earlier studies on these instruments, four main categories can be noted that causes vulnerabilities, these are interference, climatic challenges, maintenance of instruments and destruction of instruments [19].

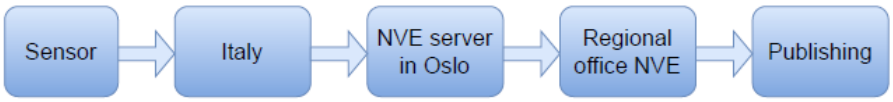

Fig. 1. Illustration of the transnational digital value chain for mountain landslide warning.

In Fig. 1, the transnational digital value chain is presented. Data is collected from GBInSAR, SB-InSAR and borehole instruments metering data, and this is transmitted from the mountain to Italy where metering data are being processed and transmitted to a cloud server in Oslo. From the cloud server, NVE can collect the metering data and present and publish the analyzed data as alerts to their site called varsom.no. The website varsom.no is operated by NVE in collaboration with the State Highway Authority and Meteorological Institute and is a notification portal that the Norwegian population can use to consider whether it is safe to travel or stay in landslide-prone areas [7]. If this site was to be compromised and give wrong information about the condition on landslide-prone areas, people staying or traveling in these areas may be at risk.

3 Risk analysis approach

Risk refers to an unknown outcome related to an activity in the future. The process to mitigate risk is called *risk management* and involves a set of activities to identify, analyze and manage risk. It is common to think of risk as a combination of value, threat

and vulnerability better known as the three-factor model [20]. This paper combined the three-factor model with ISO 31000 - Risk Management as the baseline and framework for implementing risk analysis. However, in risk management, the person responsible for conducting the risk analysis will influence the outcome of the analysis. The influence is affected by the person's intuition, also called risk perception. Risk perception describes how we see and understand risk, in other words risk perception is a biased interpretation based on different parameters like experience, knowledge and uncertainty [21].

This study used an *abductive* research approach (forming a conclusion based on the information that is gathered) and combined several qualitative methods to determine how NVE can secure their digital and cloud-based value chain for mountain landslide warning [22]. The main advantage for using an abductive approach was that it allows the data gathered through interview and document analysis to guide the direction of the study. It also allows us to omit sensitive information that would have made the study difficult to publish.

To follow the abductive scheme, semi-structured interviews and document analysis are two qualitative methods that were considered suitable for this study where little or no literature was available. To evaluate risk in a value chain, several informants from different parts of the value chain needed to be interviewed. The selection of informants was done in collaboration with NVE and all informants was introduced to the topic with a summary of the context. The interviews lasted from 40 minutes up to 2 hours. In addition, the risk analysis required that the informants possessed essential knowledge about cyber-security and the metering value chain. Another important factor to why semi-structured interview was the preferable choice was the implementation of risk analysis. In order to reflect the reality in the best possible way, the interview guide had to give room for follow-up questions and allow informants to talk about their own experiences [23].

The interview guide was developed along with the process of conducting interviews. The first two interviews made the foundation for developing the interview guide and adjusting the context from each informant towards their position in the digital and cloud-based value chain. However, some questions remained the same to reflect on different points of view to gather a more holistic understanding on the topic. Each risk perception was captured and combined into making the risk analysis to preserve the holistic approach as realistic as it can be. Whenever contradiction occurred, documents gathered from national threat assessment was utilized as a support on how to evaluate risks in the risk analysis. This was done to reflect the risk perceptions to informants, whether or not they could be affected by their position in the digital value chain. This method also allowed us to some degree to confirm some information from the literature study and reduce the uncertainty towards the results from the risk analysis.

However, uncertainty is always present when reflecting on future risk and also on the potential consequences of cyber-attacks. To minimize this uncertainty an extensive research on potential threats and also earlier incidents was utilized when making the interview guide to develop the answers needed.

4 Risk Analysis and Results

Results from interviews and document analysis works as the foundation for this risk analysis. These methods combined were used as references to score the probability and consequence for each incident. Fig. 2 below shows a summary of the risk analysis in the digital and cloud-based metering value chain for NVE. In total 60 incidents were selected together with NVE and evaluated for each link in the value chain shown in Fig. 1 above with four main incidents: loss of connection, unstable access, loss of data, and compromised data. These risks were chosen out of knowledge and experience from the contingency department from NVE. They have collected data from earlier incidents and know what type of events is most likely to occur and how it will impact the value chain. Out of 60 incidents, 14 were evaluated as high-risk incidents, 30 incidents evaluated with medium risk, while the remaining 14 incidents were considered as acceptable risk. Concerning the criteria for evaluating the severity of each risk, this study used mostly qualitative data collected through the documents both handed out from NVE and public threat assessments from national departments. Through eight interviews with informants along the value chain, the outcome of the analysis showed that high risk incidents occurred most often in the transnational supplier. This observation corresponds with statements from informants regarding the lack of control over suppliers in other jurisdictions. Further results from the risk analysis showed similar features to those evaluated as high-risk incidents. These factors can be summed up into six categories: dependency to supplier, insufficient control over supplier and sub-supplier, deficient risk analysis, deficient framework for information security, insufficient user education and insider threats.

Link in the Value Chain	Technology	Internal Supplier	Norwegian Supplier	Transnational Supplier
Data Collection	Digital	2	2	2
Data Transmission	Fiber, ADSL/DSL, Wireless, Satellite, etc	1	5	5
Data Processing	Internet	5	4	5
Data Transmission	Cloud computing	3	4	5
Data Presentation	Varsom.no	3	3	3

Fig. 2. Summary of Risk Analysis Results

Fig. 2 represents a summary of the risk analysis results where each value represents a risk acceptance criterion based on NVE internal procedures on level of acceptance. The figure shows that the digital sensors are all within the acceptable risk. This is because the instrument located on the unstable mountain have redundant solutions if one were to fail, and if one of the instruments should be compromised or fail to work other instrument could still measure the same metering data and still be operative. However, for data transmission and data processing the risk is high for both Norwegian supplier and transnational supplier. The reason is the rising uncertainty connected to the suppliers and the limitation to monitor how the data is handled through the other suppliers.

The service level agreement was the only way to ensure that metering data from external suppliers still had integrity and that it was available at the given time.

In addition to the limitation of monitoring the metering data, the implementation of cloud computing technology into an already complex and tangled value chain increases the risk of human error. When employees are not able to understand the technology and the following consequences or the technology that they are utilizing, they are posing risk towards the integrity of not only the metering data, but in a worstcase scenario, the lives of the population close to landslide-prone area. Several informants also pointed out the challenge that NVE is organized in silos and the communication across sectors is not common. The risk carried by moving the value chain to the cloud was emphasized when three of the informants mention that cloudcomputing could potentially led to more confidential information being compromised because of not understanding how to share information in the cloud. NVE also had challenges in creating a unanimous overview on how to characterize valuable assets. This causes more challenges when sharing information into the cloud. They also did not agree whether NVE published too much information to the public or not. NVE wants their service to be as transparent as possible, and this had led to a large amount of their data being made openly available on their website. This amount of public information might carry a risk of undesired consequences. Attackers could reconnaissance the public information for making attacks more targeted according to one of the informants. But transparency also creates trust in the population towards their decision-making. Since NVE wishes to maintain the transparency while also protecting their assets, the countermeasures need to be well thought out, and the countermeasures themselves must be seen as a part of a digital value chain for a critical infrastructure.

There is no doubt that human error is still a dominant risk factor for the value chain, one informant said that human error was the leading cause for 20-50% of security breaches. In addition, it was mentioned that the most likely event to occur was the insider. However, informants did not agree upon the human capability for preventing threats. Some believed there is always going to be human error and the only countermeasure is to invest in hardware and software barriers. The argument was that cyberattacks are today very advanced and targeted, making the detection task beyond challenging, and that the employees needed to be experts in cyber-security, "*just*" to detect a phishing email. Other said human knowledge was irreplaceable. They are the weakest link, but at the same time they are also the strongest safeguard according to several informants. The argument behind this statement was based on an example on monitoring mountain landslide, where the hardware system could be compromised, telling the monitoring center they need to evacuate the area because of high movements in the mountain. In fact, the mountain was steady with no movements, so they investigated why the device was giving false measuring data, and then detected that some device was compromised by another entity.

Overall, the new technology is safer and gives opportunities beyond what was previously imaginable. Still, NVE may feel that they are pushed into the digital transformation because "everyone else is doing it". Some are welcoming the new technology, others not so much. They understand that cloud-computing eventually will change the way they are used to work and that they need much time and knowledge to adjust to

this change. One interesting observation on some informants welcoming technology and others not, was the position of these informants. Informants from the monitoring center was skeptical towards new technology because they understood the severity of loss of metering data. Informants working in the regional office was welcoming the new technology and was excited to start using it. Another contributing factor was the knowledge about the technology and how it works. Cloud-computing had at the time (2019) no adequate servers within Norwegian borders, which made it impossible for employees to accept the solution as safe because of their duties to conduct 24/7 surveillance and 0% downtime for their instrument. They could not risk sending their metering data outside Norway where they had no control on how the data was being managed. The only way they could accept a cloud-based value chain was through implementing another on-site solution in the cloud to keep it under surveillance at all times. Implementing yet another system into the digital value chain can potentially create more vulnerability, in addition to expanding the attack surface. But this was according to the informants from monitoring center, the only way they would agree upon a cloud-based value chain, which now is more semi-cloud-based. The solution is a compromise between wanting to digitalize and remaining the same level of security, but solution like this could be more vulnerable because the two systems are not made to communicate with each other, so again they are forced to trust that the suppliers of the cloud service is able to manage the integration.

5 Discussion

Open communication and cooperation throughout the value chain may in some cases be impossible because of trade secrets or other conflicts of interest. However, in order to protect their assets, NVE should consider the organizational countermeasures mentioned in the previous section, in order to obtain a holistic approach rather than a sector-based approach. It is no longer enough to rely on trust in the agreements as their safeguard towards suppliers and sub-suppliers in the value chain. The information flow and communication with suppliers should be prioritized to reduce the risk of attacks with lateral movement from sub-supplier into NVE's server, from where attackers might gain even more access throughout the value chain [5].

To manage the digital and cloud-based metering value chain one cannot simply say that it needs to be managed centralized or decentralized. Because on one hand you can create the holistic overview by centralized management of the value chain but missing important details due to lack of expert knowledge on each part of value chain. On the other hand, you can obtain detailed information about your part of the digital value chain when managing it in a decentralized manner, but this misses the overview of the value chain and minor risk events could potentially cascade into more serious incidents when seen as a part of a the digital value chain. Today they use trust between actors as their main way of ensuring that the value chain is secured. But when informants were asked on how they can ensure that suppliers actually fulfill this requirement, they could not provide good answers. This type of uncertainty causes room for attackers to exploit. It is only a matter of time before a more serious attack happens to the critical value

chain, and when it does, should it be handled from a centralized or decentralized perspective? Have NVE communicated sufficiently the risk between the value chain actors, and do the suppliers know their role if they are under attack? The answers to these questions may be found in further research on this topic. It is important that each supplier know their role and are ready to collectively manage an attack on the digital value chain.

Consensus between suppliers in a digital value chain is important, both for knowing what exactly they are working on and for a shared understanding of the importance of cyber security to protect the critical infrastructure. If NVE have trouble defining what type of information should be sensitive and what should be public, the information loses its integrity and confidential information may find its way to the public. Even though this is a result of human error, this could be mitigated by raising awareness towards sensitive information and how to handle these types of data. Humans may be the weakest link as some informants may indicate, but they are also the strongest when it comes to complex decision-making, and this cannot yet be replicated by artificial intelligence. Despite humans being dependent on technology, technology also depends on humans to understand it to operate in the way we intendent it to work. In any case. the digital transformation is inevitable and replaces analogue work whether we like it or not.

Cloud-computing causes interdependencies to an already interdependent value chain. NVE is investing in a solution provided by the suppliers of the cloud service and they thereby invest in another system to be integrated into the cloud. NVE becomes dependent on this one supplier, making it more difficult to change cloud service if needed. NVE need to have a backup plan for the event that the cloud service stops working. They cannot be dependent on cloud suppliers committing to the 0% downtime that NVE is regulated to have.

One of the most important actions to protect NVE's digital and cloud-based value chain is to pay attention on the connection between the existing and new countermeasures to avoid dependencies between safeguards. Dependencies thorough the digital value chain could potentially lead to a domino-effect between stakeholders when an incident occurs. Still, the technology of cloud computing that NVE plan to implement will create dependencies and the focus to implement strict procedures and service level agreements will be important contributing factors to obtain a secure value chain. However, these should not be the only countermeasures. Organizational countermeasures that will be important to prioritize include awareness, training, communication, response, surveillance and anticipation. The technical countermeasures considered efficient for digital and cloud-based value chains are as follows: segregated networks, user restrictions, log analysis, pen-testing, security by design/security by default, end-to-end encryption, computer generated passwords and two-factor authentication.

In addition, a general framework for implementing cyber-security for metering value chain should be considered to ensure secure implementation of cyber-security for suppliers and sub-suppliers. Most importantly, performing risk analysis with a *holistic* approach. The framework could potentially help employees on how to assess sensitive information across sectors and make the assessment more coherent. An important aspect to this framework is that is must be communicated not only to internal employees but also to external actors in the digital value chain. To secure the digital value chain,

they first need to focus on how to raise awareness on cyber security and the technology that NVE wishes to utilize. The framework should emphasize that NVE conducts risk assessment and provides courses with focus on cyber security and what responsibility an employee possesses when handling sensitive data. Through risk assessment and preventative activities like log-analysis, penetration testing and intrusion detection systems, NVE will be able to work proactive rather than reactive on cyber security incidents. Even though password policy can sometimes work as a recipe for attackers, NVE must influence employees about the importance of making passwords hard to crack. Multiple factor authentication should be a part of their password policy because they are responsible for critical infrastructure.

Results from the risk analysis will be affected by the knowledge, experience and uncertainty of the person conducting the analysis, but also the chosen approach to the risk analysis [21]. When choosing an approach of risk analysis, one must be aware of the results other risk analysis may lead to. There exists benefits and limitation towards all risk analysis, and one must decide which approach is the most suitable for the answers you seek. For this study, the purpose was to understand how best secure the digital and cloud-based metering value chain for the critical infrastructure mountain landslide warning. Based on extensive research on multiple other risk analysis ISO 31000, NIST Cybersecurity framework, ENISA- Cloud Computing, Security Risk Assessment, NSM Foundational principles in ICT-safety the preferable choice was eventually ISO 31000 because this was the most holistic approach which the study needed in order to understand how to secure the value chain. However, the risk analysis results are based on assumption and assumption always contains uncertainty. It is inevitable to omit the uncertainty when referring to something that may happen in the future. But some historical events and expert knowledge will be the best foundation for the risk analysis. On the other hand, expert knowledge will again be influenced by the risk perception, not only to the expert but also the one conducting the risk analysis.

An unbiased risk assessment should not be the objective of a risk assessment in critical infrastructure. Assets that are critical for some may not be critical for others, and therefore NVE is recommended to cooperate and communicate with their suppliers to understand the different approaches to risk. This can help them into making the risk analysis more realistic by involving each supplier. NVE should be the initiating part and they should be open for sharing their analysis with the value chain so that the suppliers have the opportunity to influence the analysis the way they assess the risks.

6 Conclusions

We find that the risk is significantly higher for the transnational digital value chains. The recommended risk mitigation is a combination of organizational and technical countermeasures. To secure the digital and cloud-based value chains, NVE should invest resources to continuously control suppliers and sub-suppliers. The most important countermeasures will be developing a framework for cyber-security that should be distributed throughout the value chain to ensure implementation of important activities to prevent/protect, detect, handle and act on attacks against the value chain. Trust is an

important factor but trust alone is not enough to ensure that the critical infrastructure is protected.

The existing literature on security in cloud-based digital value chains is rather limited, providing a good opportunity for further research in this area. To further investigate the vulnerabilities existing in a chain of suppliers and sub-suppliers would be necessary in order to further elaborate of the activities needed to secure the value chain. This would also help in evaluation of risk levels. It would also be very interesting to explore the concept of resilience as a foundation to secure the digital and cloud-based value chain.

Acknowledgements

Thanks to Janne M. Hagen for good and useful advice on this paper which is a short summary of a master thesis. Thanks also to Arne Bjørn Mildal for contribution to the thesis and to the informants from NVE for bringing insight to this topic. Thanks to Eva Brekka at NC-Spectrum for this opportunity to participate in this research.

References

1. European Commission: Evaluation of council directive 2008/114 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, European Commission, Brussel (2008).
2. Gjesvik, L.: Comparing cyber security, Norwegian Insitute of International Affairs, Oslo, (2019).
3. Proactima: Kartlegging av bruk av tingenes internett (IoT/IIoT) i norsk kraftforsyning, Nr.2/2020, Norges vassdrag- og energidirektorat , Oslo, (2020).
4. NVE: Om NVE, 18 12 2020. Available: https://www.nve.no/om-nve/?ref=mainmenu.
5. DSB: Risikostyring i digitale verdikjeder, Direktoratet for samfunnssikkerhet og beredskap, Tønsberg, (2020).
6. NVE: Åknes," 08.01.2020. Available: https://www.nve.no/flaum-og-skred/fjellskredovervaking/kontinuerligovervakede-fjellpartier/aknes/ (2020).
7. NVE: Fjellskred - overvåking og beredskap, Nr. 5/2017, Norges vassdrag- og energidirektorat , Oslo, (2017).
8. NOU 2015:13: Digital sårbarhet - sikkert samfunn, Regjeringen, Oslo, (2015).
9. Mohammed, A., Altmann, J., Hwang, J.: Cloud computing value chains: Understanding businesses and value creation in the cloud, Economic models and algorithms for distributed systems, pp. 187-208 (2009).
10. Simatupang, T. M., Pioonrungroj, P., William, S.: The emergence of value chain thinking, International Journal of value chain management 8(1), 40-57 (2017).
11. Stanoevska-Slabeva, K., Talamance, C. F., Thanos, G. A., Zsigri, C.: Development of a Generic Value Chain for the Grid Industry, Veit D.J., Altmann J. (eds) Grid Economics and Business Models. GECON 2007 Lecture Notes in Computer Science, vol. 4685. Springer, Berlin, Heidelberg (2007).
12. Giannakis, M., Spanaki, K., Dubey, R.: A cloud-based supply chain management system: effects on supply chain responsiveness, Journal of Enterprise Information Management, (2019).

13. Büyüközkan, G., Göçer, F.: Digital Supply Chain: Literature review and a proposed framework for future research, Computers in Industry 97, 157-177 (2018).
14. Ageron, B., Bentahar, O., Gunasekaran, A.: Digital Supply Chain: Challengens and future directions, Supply Chain Forum: An International Journal 21(3), 133-138, July, (2020.
15. Pau, M., Patti, E., Barbierato, L., Estabsari, A., Pons, E., Ponci, F., Monti, A.: A cloud-based smart metering infrastructure for distribution grid services and automation, Sustainable Energy, Grids and Networks 15, 14-25 (2018).
16. Mylrea, M., Gourisetti, S. N. G.: Blockchain for Supply Chain Cybersecurity, Optimization and Compliance, Resilience Week (RWS), pp. 70-76 (2018).
17. NSM: Risiko 2020, Nasjonal sikkerhetsmyndighet, Oslo (2020).
18. NorSIS: Nordmenn og digital sikkerhetskultur, Norsk senter for informasjonssikring, Gjøvik (2019).
19. Norsk Romsenter: Vurdering av sårbarhet ved bruk av globale satellittnavigasjonssystemer i kritisk infrastruktur, Norsk Romsenter, Oslo, (2013).
20. NOU 2006:6: Når sikkerheten er viktigst, Regjeringen, Oslo, (2006).
21. Slovic, P.: The Perception of Risk, Science 236, 280-285, 11 July (2014).
22. Josephson J. R., Bharathan, V.: An Abductive Framework for Level One Information Fusion, In: Information Fusion, Italy, (2006).
23. Magnani, L.: Abduction, Reason and Science: Processes of Discovery and Explanation, New York: Springer US, (2001).