Norwegian University of Life Sciences

Master's Thesis 2024 30 ECTS
Faculty of Landscape and Society

A Qualitative Case Study of Security Culture in Norwegian Small and Medium Sized Businesses

Kirsten Hov
International Relations

About Noragric

The Department of International Environment and Development Studies, Noragric, is the international gateway for the Norwegian University of Life Sciences (NMBU). Established in 1986, Noragric's contribution to international development lies in the interface between research, education (Bachelor, Master and PhD programmes) and assignments.

The Noragric Master's theses are the final theses submitted by students in order to fulfil the requirements under the Noragric Master's programmes 'International Environmental Studies', 'International Development Studies' and 'International Relations'.

Kirsten.hov@nmbu.no

Noragric
Department of International Environment and Development Studies The Faculty of Landscape and Society
P.O. Box 5003
N-1432 Ås
Norway
Tel.: +47 67 23 00 00
Internet: https://www.nmbu.no/en/research/groups/department-international-environment-and-development-studies-noragric

Declaration

I, Kirsten Hov, declare that this thesis is a result of my research investigations and findings. Sources of information other than my own have been acknowledged and a reference list has been appended. This work has not been previously submitted to any other university for award of any type of academic degree. Any errors are mine alone.

Signature.....Date.....

Acknowledgements

For K, N and T. the loves of my life.

I want to thank the informants for letting me take a peek into their security cultures. I want to express my gratitude to my supervisor Shai Divon for his constructive feedback, guidance and understanding over the years. I would also like to thank Kristi Stuvøy and Katharina Glaab for their master thesis seminars which helped me to get back into the academic world after years of absence. And last, but not least, I want to thank my former fellow student, Johanne Rokke Elvebakken, for her feedback and questions.

The last phase of working on the thesis whilst working full time and raising two small children has been tough. Thank you, Thomas, for your patience, love and support through it all, especially over these last months in which you've been running our Family Inc. yourself. I also want to thank my parents and parents-in-law for their help with the children, and to my employer for encouragement and flexibility to make space for the thesis. It takes a village.

Abstract

Every year intellectual properties worth millions of kroners are stolen from Norwegian companies. Intellectual property is important for both the companies' and the state´s economy, and for national economic security. The Norwegian state finds that small and medium sized businesses (SMBs) are at particularly vulnerable to theft of IP and trade secrets. How a company protects such economic information is called security culture. The aim of this thesis is to examine how SMBs understand securing their IP and trade secrets in Norwegian-Chinese business relations, and what informs their understandings. By exploring factors that influence the SMBs security cultures: media, state information sharing, knowledge, attitudes, and experiences, the thesis aims to give deeper insight into these influential factors. Through an analytical framework using concepts from Organizational studies, Information communications technology studies and security studies, this study qualitatively examines the knowledge dimension of security cultures within four small and medium sized businesses.

The thesis argues that the intelligence community has limited outreach to the private business sector. Only one of the four SMBs (one of the six informants) in the sample had read the governmental intelligence community's open threat assessments, and this informant did not find the information relevant, but found the same information in media. The state finds that their threat assessments are of importance to the private business sector, and also find the companies security cultures' important for national security. The sample does not believe they need more assistance or information from the state. The data indicates that media, and the informants own lived experiences are the most important sources for knowledge about economic and industrial espionage, and how intellectual property rights are dealt with in China, and how to protect their economic information.

Acronyms and Abbreviations

IP – Intellectual Property

IPR – Intellectual Property Rights

NHO – The Confederation of Norwegian Enterprises (Næringslivets Hovedorganisasjon)

NIS – The Norwegian Intelligence Service (Etteretningstjenesten, e-tjenesten).

NMBU – the Norwegian University of Life Sciences (Norges miljø- og bioteknologiske universitet)

NOU – National Assessments (nasjonale offentlige utredninger)

NSD – Norwegian Center for Research Data (Norsk senter for forskningsdata)

NSM – The Norwegian National Security Authority (Nasjonal sikkerhetsmyndighet)

NSR – The Norwegian Business and Industry Security Council (Næringslivets sikkerhetsråd)

POD – The Norwegian Police Directorate (Politidirektoratet)

PST – The Norwegian Police Security Service (Politiets sikkerhetstjeneste)

SMBs – Small and Medium Sized Businesses

WIPO – World Intellectual Property Organization

TABLE OF CONTENTS

1 Introduction

The Norwegian Police Security Service (PST) and the Norwegian Intelligence Service (NIS) have for several years expressed concerns about economic and industrial espionage against Norwegian public and private enterprises in their yearly threat assessments (Norwegian Intelligence Service, 2022; The Norwegian Intelligence Service, 2017; The Norwegian Police Security Service, 2017; The Norwegian Police Security Service, 2024). Economic espionage is when a state actor steals economic information, such as intellectual property (IP) and trade secrets, from foreign enterprises to strengthen its national business sector and national economy (Nasheri, 2005; Potter & Centre for Trade Policy and Law, 1998; Søilen, 2016; Thorleuchter & Van den Poel, 2013). When corporations or companies collect economic information from other companies it is called industrial espionage (Søilen, 2016). The value of the stolen IP affects the national economy and thus the national economic security of a country (Grabiszewski & Minor, 2019, p. 269). This thesis is concerned with espionage as "deliberate unwanted incidents" (Bergsjø et al., 2020, p. 19) meaning that someone deliberately conducts acts of espionage against the companies to steal economic information. Businesses are responsible for securing their economic information from theft (Jorem, 2019). Nasjonal sikkerhetmyndighet (2024, p. 33) are concerned that many small and medium sized businesses (SMBs) are vulnerable for digital deliberate unwanted incidents. This makes SMBs more vulnerable to industrial and economic espionage than large companies (Næringslivets sikkerhetsråd & Opinion, 2015; The Norwegian Intelligence Service, 2017).

How well the companies protect their economic information depends on the company's security culture. Security culture can be defined as a company's culture regarding securing its valuable or sensitive information, such as economic information. Security culture consists of several influential factors or dimensions that are expresses through the company's total security behavior (da Veiga et al., 2020; Malmedal & Røislien, 2016: 30; Roer & Petric, 2017: 42-43; The Norwegian National Security Authority, s.a.). The dimensions this thesis examines are the role of state assistance, media, experiences with IPR in China, and the employees' and leaders' knowledge and attitudes about industrial and economic espionage. The thesis examines these factors in four SMBs related to their Norwegian-Chinese business relations. Violations of intellectual property rights in China are a widespread problem for foreign enterprises (Brander et al., 2017; Li & Alon, 2020). Further, the Norwegian intelligence community stresses China as a specific threat actor that conducts high skilled economic espionage against Norwegian

companies (The Norwegian Intelligence Service, 2017; The Norwegian Police Security Service, 2017; The Norwegian Police Security Service, 2024).

1.1 Purpose and Objectives

The purpose of the thesis is to contribute to a deeper understanding of private Norwegian SMBs' security cultures in relations with foreign economic and industrial espionage in international trade, using the example of China. To do this the thesis aims to provide qualitative in-depth insight into SMBs knowledge and attitudes regarding securing their economic information in Norwegian-Chinese business relations. Because the thesis relies on the assumption that SMBs contribute to the state's economic security, the second purpose is to examine the state's role in influencing security cultures. To contribute to deeper understanding of these factors the thesis goes in-depth into a chosen selection of the dimensions of security culture: knowledge and attitudes, experiences, media and state assistance in the form of information sharing. Hopefully the thesis will contribute to the academic conversation about security culture in Norwegian companies by providing in-depth insights into SMBs knowledge and attitudes, how they think about securing their IP and trade secrets in China, about their experiences with dealing with securing their IP and trade secrets in their everyday Norwegian-Chinese business relations. The findings are also relevant for the governmental security community, such as PST and NSM, to inform their policies to improve the outreach of their open intelligence information with the private business sector, in particular to SMBs.

The thesis defines security culture as consisting of the influential factors of state governance & assistance, national culture, media, the company's security policies & compliance, security training, and the employees' and leaders' experiences, knowledge and attitudes, which are expressed through the organizations' total security behavior, meaning how they protect their IP and trade secrets from theft (da Veiga et al., 2020; Malmedal & Røislien, 2016: 30; Roer & Petric, 2017: 42-43; The Norwegian National Security Authority, s.a.). To limit the focus of the thesis, it focuses on the dimensions of knowledge and attitudes, state assistance, media, and experiences. The theoretical framework for this thesis comprises of concepts from Security Studies, Organizational Studies, and Information Communication Technology Studies. I aim to use these concepts to help explain the findings. Within the conceptual framework of security culture, the thesis seeks to meet the objectives through the following research questions:

- *How may media, state information sharing, experiences, knowledge and attitudes related to Chinese economic and industrial espionage influence SMBs security cultures?*
    - *How and from where do private Norwegian small and medium sized businesses obtain information and knowledge about industrial and economic espionage?*
    - *How do private Norwegian small and medium sized businesses relate to and understand economic and industrial espionage in their Norwegian-Chinese business relations?*
    - *How do private Norwegian small and medium sized businesses relate to the dimension of state information sharing?*

I aim to answer these research questions through a qualitative study of private Norwegian SMBs' security cultures specifically related to Chinese economic and foreign industrial espionage. The research is based on a literature review and qualitative semi-structured interviews with six representatives from four private Norwegian SMBs in which four informants are the companies' contact person in Chinese relations, two of these are also leaders, and the two last informants are two ICT Chiefs. The other informants are a representative for a trade and employer's association for technology enterprises (Abelia), and two officials from the Norwegian Police (POD). By examining empirical findings from semi-structured interviews, the thesis aims to explore how the factors of state assistance, media, knowledge and attitudes, experiences may influence the companies' security cultures. To answer the research questions and to analyze these findings several concepts are used.

1.2 Thesis Outline

The overarching objective/goal/aim of this thesis is to discuss how media, state information sharing, experiences, knowledge, and attitudes influence SMBs security cultures. Therefore, Chapter 2 presents information necessary to understand the topic. It will provide information about Norwegian, and other Western foreign businesses' experiences and challenges with doing business in China, and economic and industrial espionage against Norwegian companies in Norway and China. It also situates my thesis in the IR discipline. Chapter 3 reviews previous research on security culture. Chapter 4 presents the theoretical framework of the concept of security culture with a focus on the central sub-concepts. Chapter 5 presents the research design, and data collection, and reflects on the validity, reliability, challenges, and shortcomings of the

research, and Chapter 6 presents the findings along with the analysis. In Chapter 7 the findings are discussed. Chapter 8 presents the conclusion based on the analysis and discussion in Chapters 6 and 7.

2 Background

This chapter presents the contextual background, reviews relevant literature, and explains central concepts important to understand the thesis topic. The chapter is structured as follows: It begins by arguing why it is academically relevant in the academic field of IR to study SMBs security cultures in Norwegian-Chinese business relations. It explains SMBs' importance for the Norwegian economy, and it explains why SMBs are particularly vulnerable as targets for espionage. Supported by academic literature it also discusses why the Norwegian government stresses the significance of China as a threat actor. Then definitions and descriptions of economic and industrial espionage, intellectual property, and trade secrets are presented and discussed.

2.1 Why Study Norwegian SMB´s Security Cultures in the Academic Field of IR?

There are several arguments for giving more scholarly attention to SMBs´ security culture in the field of IR. A company's security culture affects how well it protects itself from espionage. Espionage is a topic in intelligence studies, a sub-discipline in IR, and security and culture are essential concepts in IR (Lantis, 2002). Further, SMBs are international actors in international trade, and they contribute to the Norwegian national economy, and as such to the national economic security (Grabiszewski & Minor, 2019: 269). Lastly, SMBs are academically interesting to study because they may be more vulnerable to industrial and economic espionage than large companies (Næringslivets sikkerhetsråd & Opinion, 2015; The Norwegian Intelligence Service, 2017). The next sections argue the relevance of these arguments.

Economic concerns are considered to be a relatively "new" security issue: Security has traditionally been considered military security, but today it also includes economic issues (Adler & Barnett, 1998). After the Cold War countries started to include economic prosperity in their national security framework because economic power contributes a state's international power. Economic security is also important to maintain or improve the standard of living within the country and for the stability of the nation (Potter & Centre for Trade Policy and Law, 1998). As SMBs produce almost half of the annual value creation in the Norwegian business sector,

close to 1182 billion Norwegian kroner[1], they are significant contributors to the national economy. Further, SMBs make up 99% of all companies in Norway, and 57% of the employees in the private sector work in an SMB (Næringslivets Hovedorganisasjon, 2024). As such the SMBs intellectual properties are important for both the companies and the nation's economy (Grabiszewski & Minor, 2019: 269). It is hard to estimate the financial loss from economic espionage because many companies do not know they have been attacked or they find out months or years after the attack (Moe & Lillevik, 2012). Still, economic espionage may harm Norway's potential for economic growth (Moe & Lillevik, 2012; NOU 2016: 19, 2016).

The private business sector is responsible for its own security and is dependent on having their own security systems and advisors. SMBs generally have few resources for security work, which lowers their ability to protect their IP and trade secrets from, and detect incidents of, theft of assets like IP and trade secrets, and other criminal actions (Etteretningstjenesten, 2017; Næringslivets sikkerhetsråd & Opinion, 2015). According to NSR the largest companies have security systems, but the SMBs often do not (Kibar, 2017; Næringslivets sikkerhetsråd, 2024). This makes them easier targets for economic and industrial espionage. In 2015, NSR found that only 5% of the private enterprises (large enterprises and SMBs combined) in the study had one or more employees who work full time with security and preventing crime. SMBs have an even lower percentage of employees who work with security and prevention of crime full time (Næringslivets sikkerhetsråd & Opinion, 2015: 10-11). Further, many companies do not sufficiently log their network traffic. Without this logging, "it is impossible to know how much data has been sent out of the company and to track the attacker IP-address for the period of time the attacker has had access to the computer systems" (Moe & Lillevik, 2012: 33). These factors make SMBs vulnerable for unwanted security incidents.

Now I have argued the relevance of studying SMBs. The next section argues why it is academically interesting to study Norwegian-Chinese business relations.

2.2 Why Study Norwegian-Chinese Business Relations?

To understand the business context in which Norwegian companies operate, this section presents relevant background information about IPR in China and Chinese industrial and economic espionage.

[1] I have not found statistics on Norwegian technology companies' contribution to the national economy.

Even though there exist international agreements that prohibit the theft of IP[2], and there are international patent systems, IP continues to be stolen by both states and competitors. Like Norway, China is a member of the World Trade Organization, and is bound by the TRIPS agreement which forbids theft of IP (World Intellectual Property Organization, 2019a). The TRIPS agreement "covers all intellectual property rights, patents, trademarks, copyrights, and trade secrets [and it also includes] copyright protection for computer software, [and] databases" (N. Mark Lam & John L. Graham, 2007, p. 317). Trade secrets can be defined as "both **technical information**, such as information concerning manufacturing processes, pharmaceutical test data, designs and drawings of computer programs, and **commercial information**, such as distribution methods, list of suppliers and clients, and advertising strategies" (World Intellectual Property Organization, 2019). Also "personal information, mapping of key persons, strategic plans, (…), descriptions of products or installations of critical importance to the enterprise"(Moe & Lillevik, 2012: 27)[3]. Having this information can strengthen one's own position during trade negotiations (Moe & Lillevik, 2012). Intellectual Property Rights (IPR) can be defined as "fictional rights created to encourage innovations and creativity by protecting the labor of authors and inventors while at the same time promoting dissemination of ideas and information and competition" (N. Mark Lam & John L. Graham, 2007: 314). Still, disrespect for IPR and patents in China has for decades been an issue for foreign companies operating in China (Brander et al., 2017; Jorem, 2019; Lam & Graham, 2007; Li & Alon, 2020). Lam and Graham (2007) explain that part of the reason for this is that the institution of IPR conflicts with traditional collective culture in China. In line with Confucianism, which is influential in Chinese culture, it is wrong for a few to own ideas. Instead, the ideas should be shared so that others can develop and improve it further, for the better of the group. Regardless of cultural differences, espionage has strategic advantages. Whitney and Gaisford (1996: 627) finds "that there may be indirect strategic benefits from spying that goes beyond the direct obvious direct benefits from access to valuable economic secrets. In such situations, economic espionage acts as a form of strategic trade policy that shifts profits from foreign firms to domestic firms and potentially improves national welfare".

[2] Intellectual Property Rights (IPR) is even proclaimed in the Universal Declaration of Human Rights (United Nations, 1948): Article 27, point 2: "Everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author".

[3] My own direct translation from Norwegian to English. All further quotes from this source are my translations.

Directly related to the SMBs in the sample, an IP can be the manufactural equipment used in a factory, or technology in the form of a software source code. "The term *software* refers to all operating systems, application programs and data that is used by products containing microprocessors" (The Linux Information Project, 2004). These products include computers, smartphones, and the applications (apps) on them, electronic equipment used in subsea drilling, marine technology such as underwater robots etc. The source code is 'the recipe' for how the software is made (The Linux Information Project, 2004). As such, for technology companies, such as the companies in the thesis' sample, the source code is a highly valuable IP. The economic value of IP makes economic and industrial espionage attractive. Countries that have world-leading knowledge and technology are attractive targets for economic espionage (Thorleuchter & Van den Poel, 2013). Blomberg (2020) claims Norway is such a country. To steal IP makes it possible for a state's domestic business sector to skip the expensive research and development stage and go straight to production, and this can strengthen the national business sectors' competitiveness in the global market (Canadian Security Intelligence Service, 1996, as cited in Nasheri 2005: 17).

China's resources to conduct economic espionage make it a particular threat to Norwegian companies. Although many foreign intelligence services seek to access new technology that can be used to strengthen their own state´s business sector (The Norwegian Police Security Service, 2017), China's economic, technological (Mattis & Hoffman, 2017, p. 6) and human capabilities (Lowenthal, 2014; Mattis, 2015) to conduct intensive espionage exceeds other non-ally countries' capabilities. According to (NOU 2015: 13: 59; Smith & West, 2012: 93) Chinese national intelligence services support the national business sector by collecting IP from foreign enterprises. This collection of foreign technology can boost China's economy (Mattis, 2015).

Companies in China have close bonds with the government (Nölke, 2014, p. 77; The Norwegian Police Security Service, 2024, p. 17, 81). A Chinese intelligence law passed in June 2017 (Mattis, 2017; Mattis & Hoffman, 2017) manifests the requirement of all Chinese citizens to assist and cooperate with national intelligence efforts (Bergløff, 2019; China Law Translate, 2017; Oksholen, 2018). This blurs the lines between economic and industrial espionage. For example, in the collection of foreign technology, China relies on Chinese populations in other countries, not only on professional spies, rather on scientists and engineers, who know what information is needed to improve domestic products (Lowenthal, 2014: 456-457; Mattis, 2015). Mattis (2015) claims "Beijing essentially has created market incentives for economic

espionage, at least in strategic sectors, and many Chinese nationals have seen state protection and support as a means of getting ahead".

2.2.1 National Security and China

Economic and industrial espionage of technology is also linked to national security. NIS claims that China has "succeeded in compromising Norwegian targets" (Norwegian Intelligence Service, 2020: 65) that produce high technology that can be used for both civilian and military purposes. PST (2024, p. 13) claims that China uses non-military technology and knowledge to develop its military technology. As such the technology in some of the SMBs in the sample could be used to further develop military technology.

Another aspect of private companies that matters for national security is foreign ownership. For years PST (2019, p. 12) has been concerned and warned about foreign states that "use investments and purchases as a means to influence (…) collect sensitive information and get access to technology or natural resources of strategic significance". As such the technology in some of the SMBs in the sample could be used to further develop military technology. Since I started working on the thesis foreign ownership related to national security has received increased political attention in the Norwegian government. In 2022 the government sat down an assessment committee who in 2023 delivered an Official Norwegian Report (NOU) which found that today's laws does not sufficiently control foreign direct investments in Norwegian companies that are not subject the Security Law (NOU 2023: 28; Regjeringen.no, 2023).

Digital espionage, through a computer intrusion, gives access to a certain network that the intruder can use for both collecting information and for sabotage. Sabotage can be taking control over a network that is critical to critical infrastructure, such as electricity. The Norwegian intelligence community (PST and NIS) considers it more likely that countries that Norway does not have security cooperation with, like China, are more likely to cause harm now or in the future (Etteretningstjenesten, 2017, p. 34; The Norwegian Police Security Service, 2018: 7). Even though it is difficult to reveal the origin of network operations (Moe & Lillevik, 2012; The Norwegian Police Security Service, 2018), Chinese actors have been identified as the actor behind attacks in Norway. The investigations of the attacks against the Ulstein Group in 2014 and Visma in 2017, indicate that Chinese actors were behind the sabotage (Bye Skille, 2019; Halsør et al., 2019; Mesna, 2024; Næringslivets sikkerhetsråd, 2016).

In addition, the reasoning behind China as a specific threat actor also regards global power. China challenges the prevailing world order with Western hegemony, led by the US (Lowenthal, 2014, p. 459). The stolen technology contributes to the economic and political rise of China because economic growth gives increased international economic influence, which again gives increased political power. This can rock the balance of power between states, as China challenges the positions of other powerful actors in the international sphere (p. 459). In agreement with Lowenthal, NIS (2019, p. 70-73) finds that China is becoming a traditional great power. NIS (p. 70-73) find evidence in how it uses its economic power (via capital exports and trade) as a tool to advance its interests and challenge American hegemony, the strengthening of its military, and its increasing willingness to interfere in other states' domestic matters.

These two previous sections argued the relevance in the academic field of IR to study security cultures in Norwegian SMBs' Norwegian-Chinese business relations. The next chapter reviews previous studies on security culture in Norwegian and foreign SMBs.

3 Former studies on Security Culture

This chapter reviews relevant literature on security culture in both Norwegian and foreign companies in the academic fields of Information Communications Technology (ICT), Organizational Studies and Security Studies. Because IP and trade secrets is information, the concept of 'information security culture' is of relevance for the thesis. da Veiga et al. (2020) reviewed several of the most cited journal articles on information security culture and gives an overview of various definitions of information security culture in both academia and industry. They find that the dimensions of security culture includes political and legal factors, national culture, management, security policies and compliance, security training and education, and human factors like behavior, beliefs, attitudes and knowledge (da Veiga et al., 2020, p. 35). In the literature the authors differ on which dimensions they study.

Since I started working on the thesis in 2017, more master theses have quantitively and qualitatively focused on security culture in Norwegian companies. Most of these studies are organizational in nature and examine cyber security culture, digital security culture, or information security culture (Hella, 2022; Strand, 2023). Strand (2023), for instance, looks at how cyber security risk mitigation and human factors influence the cyber security culture within

two large Norwegian maritime companies. Among the academic inquiries of security culture in Norwegian SMBs, Hamidi and Gaard (2023) quantitatively studied unwanted security incidents and the costs of these, and found that the average Norwegian SMB does not have adequate measures to protect the company from unwanted information security breaches. It was the companies that had experienced such breaches that increased investment in securing measures.

Most relevant to the thesis' topic are the studies of the knowledge dimension of security culture. There are numerous ways knowledge are studied related to protection of sensitive information. Rocha Flores et al. (2014) examines factors that influence sharing of knowledge inside an organization, (Van Niekerk & Von Solms, 2006) presents a framework for information security culture that shows how knowledge, attitudes and behavior are interconnected (this is used as one of the central analytical concepts of the thesis. See chapter 4.2), and Ben-Asher and Gonzalez (2015) examines the role of knowledge to identify cyber-attacks. Former studies on the knowledge dimension are often concerned about internal organizational factors like strong passwords, how to protect the information in their everyday job, and the significance of training, education and awareness campaigns to increase such knowledge. This thesis, however, looks at other forms of knowledge relevant to protect IP and trade secrets in international business relations: the national culture of the business partner, and the status of IPR in the other country, and about security warnings from the Norwegian state. This knowledge can be obtained through formal education, like one of the informants, but also through experience, like the majority of the informants in this study. Knowledge can also be obtained from state information sharing, which is absent in the sample's experiences. The thesis aims to contribute to the academic conversation on security culture by using concepts from more than one academic discipline in hope that this can give new perspectives and insights by focusing on these topics. Hopefully, this will contribute to increase the understanding of the security cultures dimensions of knowledge, of state assistance in the form of information sharing, and the dimensions of experiences and media.

3.1 Former Studies on Intelligence Communication to the Public

Literature on the information sharing from the Norwegian state security community to the private business sector finds that information that the Norwegian state shares is limited (Jorem, 2019). Thorsrud (2021) found that several of the Norwegian Police's business contacts disagreed with the police intelligence officer's classification of certain information as "exempt from public disclosure", and did not find valid reasons in the law not to share it with relevant

enterprises. The business contacts believed that a reluctance to share relevant information with the local businesses stems from a lack of understanding among the police intelligence officers that external actors are essential to prevent crime. Thorsrud (2021) found that the police traditionally are concerned with gathering of information to use internally, not sharing it with outsiders.

The intelligence information that is shared to the public, including the private business sector, includes the open threat assessments by PST, NIS, Økokrim, and reports by NSM, and publicly available advice for securing economic information on NSM's web pages. NSR's KRISINO reports (Næringslivets sikkerhetsråd & Opinion, 2015, p. 5; 2017, p. 6, 16; 2021, p. 6) continues to find that few businesses read the PST, NSM and other governmental threat assessments and security reports. For example, in 2021 only 20% of the sample (consisting of 2000 private and 500 public enterprises) had read the PST assessment. The survey series has over the years added questions regarding other governmental reports, such as Økokrim's threat assessment, but it does not include NIS's threat assessments. The 2021 report states that 40% of the sample had read one or more threat assessments (including an unspecified category of 'other threat assessments'). The assessments are more commonly read in public than in private companies, and in larger than in smaller companies.

This thesis aims to contribute to the discussion about security culture in Norwegian companies, more specifically SMBs, by offering insight into security culture's dimensions of state information sharing, media, knowledge and attitudes, and experiences. More specifically the thesis examines how individuals in SMBs thinks about securing their IP in their Norwegian-Chinese business relations. It presents insights into their experiences and how they deal with the risk of espionage in China. Hopefully this will gain new and deeper insights into how they think, and hopefully this information may be useful to increase understanding of SMBs' security cultures.

This chapter presented relevant literature on the topic and situates this thesis' contribution to the academic conversation on security culture. The next section presents the theoretical framework of the thesis: The concept of Security Culture.

4 The Concept of Security Culture

This chapter presents the analytical framework for the thesis. It presents security culture as the central concept of the thesis, with special attention to knowledge, state intelligence sharing, the role of media and experiences as sources of knowledge. Petersen (2011) argued that the IR discipline can use and include perspectives from other academic disciplines. In line with this, the thesis' definition of security culture, and the central sub-concepts are taken from Security Studies, studies in Information Communication Technology (ICT), Organizational Studies and Social and political psychology. These concepts can help to explain how the chosen dimensions of security culture can influence the overall security culture within an organization such as a company.

The chapter starts with presenting the concept of security culture and information security culture, and then the chosen dimensions, or sub-concepts of security culture that are relevant for the thesis topic: knowledge & attitudes (section 4.2), media and experiences (section 4.3), and State Assistance in the form of information sharing (section 4.4).

4.1 Security Culture

Before I define security culture it is necessary to define the concepts of security and culture. There are numerous definitions of culture. Culture can be regarded "as a broad label that denotes collective models of nation-state authority or identity, carried by custom or law. Culture refers to both a set of evaluative standards (such as norms and values) and a set of cognitive standards (such as rules and models) that define what social actors exist in a system, how they operate, and how they relate to one another" (Katzenstein, 1996, p. 6). Bergsjø et al. (2020, p.34) define culture as "a community of ideas, values, and norms that a group of people shares, and which they try to pass on to the next generation. […] [Norms] is a set of rules for how one does things in the group, and a compass that helps the individual to understand what is right and wrong, safe and unsafe". Finnemore and Sikkink (1998, p. 891) defines norms as "a standard of appropriate behavior for actors with a given identity". The next section presents security.

The introduction presented a state-centered security concept which includes economic security (Adler & Barnett, 1998). The thesis relies on the basic assumption that SMBs contribute to economic security for the state and focuses on (economic) information security for companies. Security can also be defined as "a condition of absence from unwanted incidents, fear, and

danger (NS, 2012 as cited in Bergsjø et. al 2020, p. 19). "Security is also used when referring to measures that contributes to removing this condition" (p. 19). Adding together security and culture we get a concept in which ideas, values, and norms contribute to creating a circumstance of "absence from unwanted incidents" (p. 19). The unwanted incidents of concern in the thesis are economic and industrial espionage. For the thesis, security means protecting economic information from such espionage. IP and trade secrets are valuable information, it is what the companies make profit from, and as such they are assets for the companies. This economic information is stored digitally and thus also concerns the concept of 'information security'. The next section explains this concept and its relevance to the thesis.

4.1.1 Information Security, ICT Security and Cyber Security

Information security, ICT security and Cyber security are central concepts to economic security and espionage. This section explains the differences between these concepts and explains the relevance to companies' security cultures.

'Information security' can be defined as the protection of all forms of information considered to be an asset. This valuable information can be stored and communicated both non-digitally, and digitally using Information and Communication Technology (ICT) (von Solms & van Niekerk, 2013, p. 100). ICT can be defined as "the infrastructure that processes, stores and communicates information" (p. 99). ICT security is about securing this technical infrastructure as an asset. Information security includes ICT security (p. 100). Information security and cyber security are often used as synonyms in the academic literature, but von Solms and van Niekerk (2013) define them as two different concepts. They regard cyber security as "an expansion of information security" (p. 101). They define cyber security to be about protecting "non-information based assets that are vulnerable to Threats via ICT" (p. 101). These assets are persons, societies, and nations. These assets "need to be protected because of the vulnerabilities that exist as a result of the use of the ICT that forms the basis of cyberspace" (p. 100). An example of a nation's asset is critical infrastructure. If an adversary attacks and takes over the electricity supply (non-information) via cyberspace, it harms society directly. If someone steels IP or trade secrets (information) it will indirectly harm the company with potential loss of income, or a weaker position during a trade negotiation. A core difference between the two concepts is the difference between the direct and indirect consequences of an attack (p. 98).

The thesis explores how SMBs think about securing their economic information regardless of whether it is processed or stored digitally or non-digitally. The SMBs information is stored digitally on computers and on clouds, and communication includes digital forms such as e-mails (ICT security). An e-mail may contain a sale agreement in which the price for the sale is written. Some companies may consider this a trade secret. Because I use an explorative research approach, I am open to all forms of processing and storing of economic information, and of communication, such as verbally shared information (information security). When the thesis uses the term 'security culture' it includes protecting economic information (IP and trade secrets), regardless of how or where it is processed or stored.

da Veiga et al. (2020) reviewed several of the most cited journal articles on information security culture and gives an overview of various definitions of information security culture in both academia and industry. Based on their research, they make an extensive definition of information security culture which synthesizes the influential dimensions of security culture they found in their study. The definition emphasizes the human factor of human behavior to protect information, and this behavior relates to compliance with organization's security policy, and to training and education of the employees and the management. Over time this behavior becomes a norm in the company among the employees and management because of their assumptions, beliefs, knowledge, and attitudes to protecting valuable information. The role of leader's management of the security policies is also emphasized (da Veiga et al., 2020, p. 35). They further find that "Information security culture is a dynamic phenomenon" (p. 4) and that organizations must adapt and continuously evolve to consistently protect the information in the everchanging setting in which they exist. They also find that security culture is influenced by external factors (p. 35) such as national culture and state laws and regulations. The thesis relies on an extensive definition of security culture, but due to the limitations of the thesis, only some dimensions are given scrutiny. Because the thesis argues that media can be regarded as an external influential factor to a company's security culture, this factor is added to the thesis definition of security culture. Below is a model of which the thesis relies.

The next sections present the central concepts of the study in the following order: knowledge and attitudes, media, experiences and state assistance in the form of information sharing.

4.2 Knowledge and Attitudes

This section presents the dimensions of knowledge and attitudes. They are human factors which are central in security culture theory (da Veiga et al., 2020; Van Niekerk & Von Solms, 2006). Some believe that employees that lacks knowledge is the highest threat to information security (Mitnick & Simon, 2002, p. 3 as cited in Van Niekerk & Von Solms, 2006, p. 1). Van Niekerk and Von Solms (2006, p. 1) argue that every employee "needs knowledge regarding their specific role in the security process. This knowledge can be provided via education, training and awareness campaigns". Van Niekerk & Von Solms' (2006) framework for information security culture states that knowledge, attitudes and behavior are interconnected. First, employees need to have knowledge about how to protect the information considered valuable. When they have this knowledge about how to protect the company's valuable information in their everyday work, they can contribute to a desired security culture. However, if their attitudes and believes does not align with the knowledge they have received through training, education and awareness campaigns, they are likely to behave in contradiction to the knowledge with the result that the information will be less protected. Attitudes can be defined as "Employees' feelings and emotions about the various activities that pertain to organizational security" (Roer, 2017, p. 42), it includes "What employees think about taking care of sensitive information" (Roer & Petric, 2017, p. 32). The thesis is concerned about both the knowledge and the attitudes (feelings and opinions) they express about espionage, the Chinese threat, and to securing their intellectual properties and trade secrets.

Van Niekerk & Von Solms' (2006) model is specific for knowledge about how to protect their information in their everyday job, for example password usage. It does not include knowledge about relevant non-organizational knowledge, for example knowledge about how IPR is practiced in other countries in which a company does business. Further, their model emphasizes training, education, and awareness campaigns as sources to knowledge. It does not include other sources of information, like media coverage and governmental information sharing. Still, I find the model's dynamics between knowledge, attitudes, and behavior applicable also for other types of knowledge, like relevant knowledge about business culture and potential threats in a foreign country in which a company operates, and for other forms of knowledge sources, like lived experiences, media and information from the government. The next three sections present these three dimensions of security culture as central concept in the theoretical framework. It starts with the dimension of media and experiences.

4.3 Media and Experiences

Media (newspapers, online articles, television etc.) are significant sources of information to the public about what happens in society and the world, especially true when it is topics the public does not have knowledge about or has not has experiences with it (Happer & Philo, 2013, p. 321). Media "are key to the setting of agendas and focusing public interest on particular subjects" (Happer & Philo, 2013, p. 321). Happer and Philo (2013, p. 321) "examines the role of the media in the construction of public belief and attitudes and its relationship to social change". They examine this dynamic between media content and the impact this media content has on public belief and attitudes across the themes of disability, climate change and economic development. The thesis argues that the way in which media influences belief and attitudes in the public is transferrable also to other themes, such as espionage against Norwegian companies and the China threat to Norwegian companies.

Happer & Philo (2013) find that the way the sender shapes the message, can influence the way in which the message is perceived, especially if there only are a few alternatives to the problem presented in the message (p. 328). They also found an increased effect of the message if it was repeated in the media over time (p. 332-333). But the public does not automatically accept the message (p. 328). They found that "a number of factors including direct experience, knowledge from other sources, logic and the generation of fear or anger contributed to the degree to which audiences accepted or rejected the media message"(Happer & Philo, 2013, p. 328). Happer and Philo (2013, p. 327) finds that when individuals have had direct experience with a topic covered in the media, they are more likely to be skeptical when they evaluate the message. How their direct experience aligns with the message or not, influences whether the person rejects or accepts the message as true or likely. Direct experience either increases or decreases the power of the media message (p. 327). They found that if the sender of a message in the media wants to create behavioral change the message needs to include solutions so that the audience can see the benefits of a changed behavior (p. 333). It is plausible that the effect of direct experience in their theory also is valid when it comes to other information sources than the media. da Veiga et al. (2020, p. 12) study also finds that individual factors like a person's belief system and experience "can influence how a person perceives intellectual property".

This section presents a theory of how media and experiences can influence knowledge. The next section presents concepts of Governmental communication to the public.

4.4 Governmental Information Sharing

The dimension of State Regulations and Assistance includes communication of security information, like intelligence information, between the government bodies and the private business sector. The state can be regarded as an influential actor to private companies' security culture because the information a state shares, can influence how companies protect their economic information. This section presents Petersen's (2019) three concepts of intelligence communication to the public.

Petersen's (2019) study of how intelligence communities in the US, the UK, and Denmark communicate intelligence information to the public found (as the title says) "Three concepts of intelligence communication: awareness, advice, and coproduction" of which all three concepts are present in all three countries' intelligence practices. Only the concepts of awareness and advice will be presented here. The concept of Communication as awareness is about democratic accountability to the public and argues the need for secrecy of the methods of the intelligence community. This concept is also recognized for sharing little information, and the intention of threat assessments is not to share information to engage the public as an agent of national security, but rather to meet a public interest in a topic (p. 319-320). In contrast, in the concept of communication as advice, the threat assessments and warnings give information so that the public can make informed decisions to take action to prevent or handle threats (p. 319). In this approach the intelligence agencies trust that the public is able to understand and use the provided information, and believes this will contribute to national security (Petersen, 2019, p. 321). In both concepts threat assessments do not include suggestions for necessary actions. Intelligence organizations must balance between the need for information sharing while also not "compromising national security" (p. 321).

Chapter 4 presented security culture as a concept and presented the selected sub-concepts of security culture that can contribute to enlighten and explain the thesis' findings. These concepts will be used in the discussion of the findings in Chapter 6. The next chapter presents the methodology and research design for the thesis.

5 Methodology and Research Design

This chapter presents and justifies the methodology used for this study. In the following, I will present the qualitative interpretative research design, methods of data collection, and data analysis. Finally, I will discuss the limitations of the thesis, and outline the ethical considerations applied during the research.

5.1 The Case Study Design

The method used for an inquiry must be suitable to answer the research questions (Gerring, 2017: 28). As the research question requires an answer that provides an in-depth description of security culture, a case study is suitable (Yin, 2018: 4). "A case study is an empirical method that investigates a contemporary phenomenon ("the case") in depth and within its real-world context" (Yin, 2018: 15). Gerring (2007: 19) defines a case as "a spatially delimited phenomenon (a unit) observed at a single point in time. It is a 'common case' where "the objective is to capture the circumstances and conditions of an everyday situation" (Yin, 2018: 50). I want to investigate the SMBs everyday ordinary security culture. In addition, Gerring (2007: 40) argues that a case study "may be useful when a subject is encountered for the first time or is being considered in a fundamentally new way". To my knowledge, Norwegian SMBs' security cultures directly related to foreign economic and industrial espionage has not been object to qualitative academic inquiry (see more in the literature review).

5.2 Interpretative and descriptive inference

Ontologically, the study is constructivist, as the security culture is shaped by interactions between the employees and by the larger context in which the informants live, in this case, the Norwegian society. On the epistemological level, the study is interpretivist as I examine the social world of the people within the companies, and I study the informants' interpretation of their world (Bryman, 2012: 380). I want to shed light on the topic with information that might give deeper understanding of SMBs security cultures. The study is a descriptive inference as I seek to "Answer questions about who, what, when and how" (Gerring, 2007: 213).

5.3 Reliability and Internal Validity

To obtain research quality, the data must be valid and reliable. That a study is reliable means that the research "can be repeated, with the same results" (Yin, 2018: 42). Although case studies

rarely are replicated, it is important to follow the reliability principle "to minimize errors and biases in a study" (Yin, 2018: 46). To strengthen the reliability of the research I have to the best of my ability transparently demonstrated how the research was conducted.

Internal validity refers to representativeness inside the sample that is studied. External validity refers to the representativeness of the sample to the broader unstudied population (Gerring, 2007: 43). As the conclusions are based on the particular opinions and viewpoints of the interviewees, and my interpretations of these accounts (Gerring, 2007) I aim for the study to have internal validity, in which it is visible how the conclusions are thoroughly based on data and sound argument (Jackson, 2010: 22). To do this I present longer quotes from the sample in order to gain deeper insights into their reasoning around securing their assets in their business relations in China, and the other topics of the thesis. To strengthen the quality of my research, I used triangulation in all research stages. I used more than one method or data source in the research to enable cross-checking of the findings (Bryman, 2012: 717). In the following sections, I demonstrate how I used triangulation in the study.

5.4 Choosing the Criteria for the SMBs in the Sample

I used a purposive sampling approach, meaning the research questions guided the sampling of participants (Bryman, 2012: 416). I used criterion sampling where I identified criteria the informants needed to hold to be relevant to answer the research questions (Bryman, 2012: 419). The criteria are based on analysis of secondary data and developed as I reviewed literature on the thesis topic. The four criteria chosen were that the companies needed to: 1) to have current trade relations with Chinese companies, 2) to be in a sector of strategic interest to China, 3) to be Norwegian-owned and based, and 4) to be a small or medium size business. The rationale for choosing these criteria is outlined in the next sections.

I chose to focus on SMBs that have trade relations with China (criteria 1) because NIS and PST claim China is the most significant threat actor for economic espionage against Norwegian private companies (The Norwegian Intelligence Service, 2017; The Norwegian Police Security Service, 2017), and because Norwegian companies experience challenges with respect to IPR while operating in China (Jorem, 2019). Further, I wanted a sample of companies that represented potential targets for Chinese economic espionage (criteria 2). To increase the likelihood of achieving this I cross-checked different sources and found that the sectors NIS and PST claims are specific targets for Chinese economic espionage correspond with business sectors highlighted by NHO and the research sectors in the Action Plan 2017-2020 to increase

cooperation between Norway and China in science (Etteretningstjenesten, 2017: 35; Gåsemyr, 2019; Lindvoll, 2017; Ministry of Education and Research, 2017; Politiets sikkerhetstjeneste, 2020; The Norwegian Police Security Service, 2017: 8). Lastly, some of the same sectors are also found in China's Five Year Plan to increase social and economic development (Brødsgaard, 2015; Yin, 2015). These interests include technology in sectors such as health, energy, oil and gas, marine, maritime, aerospace, environmentally friendly technology, and renewable energy. Only the SMBs called Red and Orange work in sectors that are two of the main focus areas pointed out in China's Five Year Plan (Brødsgaard, 2015; Yin, 2015): new energy to solve their pollution problems, and technology to effigiate the health sector. China has both an environmental challenge which they seek to solve with green technology, and a challenge with an aging population in which technology can effigiate care for the elderly. As such these two SMBs (Red and Orange) are in sectors that are of strategic interest to China.

Due to difficulties with finding people (leaders and employees who were the company's Chinese business contacts) in SMBs that agreed to participate in the short time frame of the first phase of working on this thesis, I chose to include foreign industrial espionage. As Norwegian companies that operate in China experience challenges with industrial espionage such as disrespect of IPR and patents (Eriksen Søreide, 2020; Jorem, 2019), it is appropriate to include also SMBs in other sectors than those NIC and PST claim as the most targeted sectors in Norway. Moreover, China's Five Year Plan also highlights "intelligent manufacturing" and "industrial upgrading" (Brødsgaard, 2015: 100) which makes it reasonable to assume that it may include the two remaining SMB's sectors: technology related to the oil and gas sector and factory equipment. When the companies within these sectors sell their products in China, there is an interest in their products and technology there. Even though these SMBs may not be exposed to economic espionage, they may still be exposed to industrial espionage when they operate in China. Further, as explained in Chapter 2 there are unclear lines between the state and the private enterprises in China, the distinction between economic and industrial espionage in China is a grey zone.

As for the third criterion, I defined a Norwegian company as one that is registered with an organization number in Norway at Brønnøysundregistrene, that has its main office in Norway, and whose mother company is also Norwegian-owned and Norwegian-based. To make the sample more comparable, I excluded companies that had foreign owners. However, there is one exception. One of the businesses has an individual Chinese shareholder, who also is their

business partner, who owns a small share of the company. I decided to keep this company in the sample because the foreign person owns a very small share, is not part of the leadership nor the board. As such, I considered this person's role to not be significant for this study[4].

Second, the decision to focus on SMBs' (criteria 4) rather than large companies, or both, is based on factors that were presented in the introduction. First, SMBs are important for the national economy (Grabiszewski & Minor, 2019: 269). Second, SMBs are considered more vulnerable for unwanted security incidents than large companies who has own security employees (Næringslivets sikkerhetsråd & Opinion, 2015; The Norwegian Intelligence Service, 2017). SMBs may be particularly interesting to get a deeper understanding of how people inside small companies think, especially because they often do not have security employees. Third, the combination of less priority of security and being suppliers of services and products to larger companies in sectors of strategic importance to China, makes SMBs an attractive target for successful collection of information.

5.4.1 The Sample

I identified relevant SMBs that held the criteria through online media in articles and from public participant lists from conferences and seminars. The website www.regnskapstall.no (Regnskapstall 1881 AS, 2017) proved useful in identifying companies within relevant sectors, organization numbers, and number of employees and identifying mother companies/enterprises. I used the Norwegian registry for enterprises and organizations, Brønnøysundregistrene, to double-check the organization number, and sector. Further, I read the information on the SMBs websites, and lastly, I asked all the companies I approached, either by e-mail or by phone, clarifying questions to ensure they met criteria of participants to this research.

The sample consists of four anonymized SMBs which are referred to as Red, Orange, Yellow, and Green. NHO (2018) defines small companies (1-20 employees) and medium sized companies (21-100 employees). Red, Green, and Orange were small companies. Yellow was a medium sized company. The number of employees in the sample ranges from 9 to 56. All SMBs have listed themselves as technology developers in Brønnøysundregisteret, but during the interview with Yellow, I found out that their product in Chinese relations was factory

[4] See suggestions for future research on the topic of purchasing shares in foreign companies to get access to technology in the concluding chapter 6.

equipment, not technology. Red and Orange consider that they are developing new technology. Green and Yellow consider their technology or products to be 'old' (i.e., patents are expired).

Based on the literature, I initially wanted to interview three specific respondents in each SMB: a leader, an individual with direct contact with Chinese customers, and a security employee. Leaders are responsible for the securing of the information in the organization and their involvement is crucial for the security culture within an enterprise (Nasjonal sikkerhetmyndighet, s.a.; Sjølstad et al., 2010). An individual with direct contact with the Chinese was important to investigate knowledge about China (the knowledge dimension of security culture). A security employee was relevant because they have the main responsibility for an enterprise's security. In correspondence with the professional literature, I experienced that employees in SMBs individuals fill several roles. Many SMBs do not have an employee who works exclusively with security, and start-up enterprises prioritize time strictly. These factors affected the sample. The respondents who have direct contact with Chinese customers have various positions within the singular SMBs. Two of these respondents were also leaders, the other two worked with sales and delivery. None of the enterprises had employees working exclusively on security, but the IT directors had the responsibility for digital security. I only got access to two IT directors (in SMBs Red and Green), as the IT director in SMB Orange declined due to time priority, and the fourth (SMB Yellow) had outsourced their IT services. I chose not to interview IT services about their perception of SMBs security because it would broaden the thesis too much.

5.4.2 Data Collection

The primary data was collected through semi-structured interviews with six informants (described in the previous section) who are representatives of the group of interest (the SMBs), and other informants with good knowledge about or related to SMBs' security culture (Jacobsen, 2005: 171). These other informants are Abelia which is an interest organization for technology enterprises, and they that advocate their business members' needs to the government with the aim that the government can create the best possible environment for businesses to thrive. The other informant is a government official from The Norwegian Police Directorate (POD).

5.4.3 The Qualitative Interviews

The primary data for the thesis is the six interviews conducted with the four SMBs. Two SMBs were interviewed in 2017. The other interviews were conducted in 2019. It is a weakness that the interviews were done two years apart because those I interviewed in 2017 could have changed i.e., knowledge, attitudes and security policies during those two years. Still, according to organizational theory culture changes slowly in an organization (Schein, 1992). Following this argument, the findings can still be considered valid.

Based on the literature review I prepared an interview guide (Appendix 1 with topics and sequenced questions that I wanted to cover during the interviews with the SMBs. Beforehand, I went through the interview guide with a friend to ensure understandable questions and logical sequencing. Still, experiences during the two first interviews required me to adjust the interview guide. Initially, the guide had the same questions with different wording to be certain the informant understood the question as intended, and that I understood the answer. However, this led to some superfluous questions, which I removed after each of the two initial interviews with SMBs. I also found the need to clarify and repeat that I defined security as the protection of the SMBs' economic information during the interviews. I changed the guide accordingly. The guide had both open and closed questions. I aimed to use the closed questions as follow-up questions to the open ones to ensure I got answers to factors I found in the literature to be important, especially on security behavior, where the literature has clear recommendations for how a company should protect itself from theft of information. Retrospectively, I should have made some of these questions more open. For example, question number 12 in the interview guide (appendix 1), would have been formulated better as "How do you protect your valuable information during travels?" instead of "Do you have any guidelines to protect your values from getting into the hands of others during travels?". Even though several questions should have been formulated better to be clearly open questions, they indirectly permitted open answers.

Even though I had an expropriative study approach, retrospectively I acknowledge that I had not limited the topic good enough. Although the data revealed a large volume of interesting information on several of the dimensions of security culture, it was too much to include in a master thesis.

Two of the interviews with SMBs were conducted in their own offices, the rest were conducted over the telephone or over Skype, of which one was over video Skype. POD and Abelia were interviewed over the phone. Phone and Skype interviews allowed me to reach relevant respondents and informants all over the country, and some informants preferred telephone interviews over face-to-face interviews. The differences in visual and non-visual communication cause differences in the interaction between the researcher and the interviewee, and thus the data retrieved from the interviews. In accordance with Berg and Lune (2012: 129-130), I took some precautions to improve the quality of the data retrieved from the phone and Skype interviews. I used the same interview guide (appendix 1) and sent the same informational letter (that I used for the face-to-face interviews. Further, I communicated with the informants prior to the telephone or Skype interviews, either over e-mail or on the phone to follow up on the emails with information I had sent them. This initial contact contributes to establishing a form of relationship, which could make me less alien to the interviewees (2012: 129-130). The advantages and disadvantages of these non-facial communication methods are described below.

The immediate anonymity given by the telephone or Skype (without video) can be effective when asking sensitive questions (Berg & Lune, 2012: 130). However, the lack of visual communication can also cause the informants to be more skeptic of the interviewer, and it can be easier for the informant to lie because they do not get a personal connection with the interviewer. During face-to-face interviews, it can be easier to gain the confidence of the interviewee because physical presence initiates personal contact with trust. A disadvantage with telephone interviews was that I could not observe the informants' body language and facial expressions, such as how they reacted to my questions, and I may have missed valuable observations. On the other hand, the lack of visual communication prevented me from affecting the respondent or informant with my facial expressions and body language (Jacobsen, 2005: 143-144).

Aside from the lack of visual communication, I still noticed differences in how the informants spoke when they had knowledge about what I asked and when they did not. For instance, when answering questions about Chinese culture their sentences flew with ease. But when I asked questions about what they knew about economic espionage, I noticed hesitance and insecurity when the sentences did not flow with the same ease. They needed to think before they answered. Sometimes the hesitance was because the informant did not understand my question. In such instances, I clarified the questions.

The semi-structured qualitative interview allowed me to follow a flexible process that provided me with detailed answers that gave insight into the interviewees' experiences, attitudes, knowledge, communications, all related to securing their assets, China, and economic and industrial espionage. I followed the interview guide but during the interviews, I also followed up on the participants' answers and topics and improvised new questions. If I was uncertain if I understood their answers correctly, I asked the interviewee confirmable questions. Further, I tested the intelligence reports' claims of SMBs' weak security culture by asking the interviewees questions using the same variables in the reports, i.e., if they have any security guidelines for protection of their values during business travels.

I audio-recorded the interviews with the SMBs based on their informed consent. An audio recorder "helps the natural limitations of our memories and the intuitive glossed that we might place on what people say in interviews" and it "allows for more thorough examination of the interviewees' answers" (Bryman, 2012: 482). During interviews with the other informants, such as government officials, I did not use the audio recorder because these interviews were more informative or related to the contextual background, or it did not feel natural to use it.

5.4.4 Secondary Data

Secondary data was necessary to learn about the research topic to fill my knowledge gaps. It consists of academic literature, news articles, commission assessments, governmental and non-governmental reports, and Abelia's written suggestions for the proposed regulations of the new Security Law. I sought to primarily use peer-reviewed academic literature to increase the quality of my research. Apart from Moe and Lillevik (2012), the academic literature on economic and industrial espionage against Norwegian companies, and security culture in Norwegian SMBs is limited. Therefore, I found it useful to include master thesis studying security culture, and non-academic literature to set the Norwegian context. These include threat assessments by PST and NIS, and reports by the Norwegian Business and Industry Security Council (NSR), a governmental by Malmedal and Røislien (2016) for the Norwegian Center for Information Security (NorSIS) in which they quantitatively examined the broader Norwegian society's national cyber security culture. Their different academic backgrounds in technology and social science give the research complementary insights. Official Norwegian

Reports (NOUs)[5] are also used. The NOUs' relies on the public PST' and NIS's reports regarding espionage against Norwegian companies. PST and NIS have a particular focus on economic espionage, whereas the others (NSR, NorSIS) include espionage along with criminal activity and sabotage in cyberspace. PST declined to participate in an interview. Instead, I use media interviews with the PST's Head of Counter Intelligence (Blomberg, 2020), and former Deputy Director (Kibar, 2024). In an interview I would have liked to ask them about their concern for Norwegian companies, and about limited outreach of the open threat assessments to the private business sector.

When reading reports by private companies and by government intelligence it is important to be critical, to understand that there is an agenda with the report, and to be aware of their audience. The intelligence reports are biased in the way that they are one-sided, focusing on interests and threats to Norway and Norwegian interests, which include threats of economic and industrial espionage. Søilen (2016: 53) claims "[a]ll services systematically exaggerate the dangers coming from other countries to obtain larger budgets and employ more staff". In a NUPI panel discussion, Lars Haugom, guest researcher at the Norwegian Institute for Defence Studies (IFS) said: "Never before has it been more challenging to get the decision makers attention"[6] (Haugom, 2019). I do not have the expertise to assess whether the Norwegian intelligence services are exaggerating or not, none the less it is important to be critical of their one-sidedness. In addition, some of the language in the reports is vague. For example, PST (2019: 12) writes "By purchasing shares in certain Norwegian enterprises, foreign actors could get insight into decision processes, preparedness plans or critical infrastructure". What they mean by 'certain Norwegian enterprises' is unclear. From this wording, one can assume it concerns enterprises within the fields of societal security (ref. 'preparedness plans') and infrastructure.

It is also important to understand that the intelligence reports assess the *likeliness* of future events, i.e., network operations against Norwegian enterprises. Assessments can be wrong. With these issues in mind, I critically assessed the claims and findings in the reports. I cross-checked claims and findings in intelligence and private company reports by contrasting the same topics across the various organizations' reports, and I cross-checked with academic peer-

[5] NOUs are ordered by either the government or a ministry to examine and "report on different aspects of society" (Government.no, n.y.).
[6] Original quote in Norwegian: "aldri før har det vært mer utfordrende å få oppdragsgivernes oppmerksomhet».

reviewed literature. Based on these cross-checks I find it appropriate to include information from these reports in the thesis.

5.5 Data Analysis

Immediately after an interview, I wrote down everything I found interesting or important as field notes. For the coding of data, I followed the strategy described by Bryman (2012: 576-577) in which I transcribed the voice recordings, and started to code the transcripts and field notes as soon as possible. The coding was done by making marginal notes in the transcripts and field notes about information I found important or interesting. From the marginal notes I found themes, concepts, trends, and deviations, and I put these into both premade and new categories. Prior to the data collection, I had made some categories based on the literature, like knowledge, to ensure I answered them. New categories, like media, were based on interesting findings. I also identified key quotes and translated them from Norwegian to English. It is possible that meanings did get lost in translation. I sent a summary of the interview to the contact in an interest organization for private companies so that the person could clarify that the quotes accurately express the person's meanings. Ideally, I should have done this to the companies too. Lastly, I considered how these categories related to the literature on the topic. I sought to tie the research questions, the data, and the theory together to properly answer the research question based on the data and theory. The analysis stage also included adjustments of the research question, data, and theories (Johannessen et al., 2018 p. 39).

5.6 Ethical Considerations

I followed the principle to cause no harm to the respondents (Berg & Lune, 2012). In accordance with Glesne (2006, p. 139): "although 'no harm' may be done during the research process, harm may result from making research findings public". To keep the SMBs' and the participants' identities confidential, the locations in which they operate are held confidential to ensure their anonymity in the thesis.

Because security culture is a sensitive topic it was important to show that I would protect the participant's anonymity and confidentiality. When I contacted the companies, I was clear about my intentions with the research – to get a deeper understanding of their security cultures. Further, I informed all participants that I would keep the transcripts from the interviews in a safe place and that I would delete the documents after the research was over.

Based on signed informed consent I audio-recorded the interviews with the SMBs. Audio recordings and transcripts were treated in line with the guidelines of the Norwegian Center for Research Data (NSD) and the Norwegian University of Life Sciences (NMBU) and approved by NSD. Copies of anonymized transcripts were temporarily stored and used on my personal computer for analysis purposes before I deleted them.

5.7 Limitations and Bias

5.7.1 Disruptions from the Research

As argued by Gerring (2007: 19) a case is "observed at a single point in time". The findings only represent the respondents and informants at that point in time they were interviewed. Unfortunately, the research was conducted with longer abruptions over a longer period (2017-2024), and it is likely that the sample's security cultures have changed during these years. According to (da Veiga et al., 2020 , p.4), information security culture is dynamic and the organization continuously adapts to the environment in which it exists. At the same time, others, like Schein (1992) claims that it takes time to change the culture within organizations, and as such it is possible that the sample has not changed drastically since the time of the interviews. This means that the thesis can still offer valuable insight into Norwegian SMBs reasoning around securing their economic information in general, and specifically in relation to their business operations in China. Regarding the factor of government information sharing, the main finding that the state does not reach private companies with relevant information, seems to still be the status quo, according to former deputy director of PST, Hedvig Moe, (Kibar, 2024).

Regarding the security culture's dimension of State Laws and Regulations, it is possible that the implementation of the Security Law may have affected the security culture in Norwegian SMBs since the interviews took place. At the time of the interviews (2017 and 2019) none of the SMBs were subject to the Security Law, and as such they were not subject to the specific security demands the law requires from the companies. The Security Law (2018) intends to meet present and future digital development and threats with the goal of improving the security of Norwegian society. It is likely that more private enterprises than before are now covered by the Security Law. If covered by the law, the enterprise is required to implement certain security measures, such as risk assessments and security clearances of employees (Sikkerhetsloven, 2018, 2018, §§4-1 - 4.5, §§8.1 - 8-17). Enterprises that violate the law can be penalized (Sikkerhetsloven, 2018 §§11-2 – 11-4), which may function as a strong incentive to improve

the security culture. For enterprises who are covered by this law it will influence their security cultures.

5.7.2 Few Respondents Included in the Study

Only six respondents are included in the study. Only interviewing one or two individuals cannot represent the entire SMB. The thesis' definition of security culture states that all employees' and leaders' knowledge and attitudes etc. together make the total security culture of that individual company. It only takes one individual's action to cause theft of IP or trade secrets. Thus, one can argue that every informant represents an accurate image of that SMB. Further, the findings may be skewed depending on whether the respondents are extremes within that particular SMB. I.e., the informants could have more or less knowledge than the rest of the employees within that company. Interviewing more people, or all, within the company could have increased the internal validity, but due to time restrictions that was not an option for this thesis.

5.7.3 Informants Bias

Informants' bias can include a natural desire to present oneself as knowledgeable to not lose face. I tried to limit informants' possible bias in the way I formulated the questions in the interview guide. I used both open and closed questions to cross-check answers. My intention was to first ask an open question, and then, depending on the answer received, I would follow up with more specific questions mentioning specific factors. For instance, I would start with "do you have guidelines for how to protect your enterprise's assets (IP and trade secrets) during business travels?" (I should have asked this question openly as 'how do you protect your values'). Depending on which security measures the informant answered, I would follow up with specific questions, such as "does your company lend you out borrowing phones and laptops for use on travels?". In this way, I could interpret their answers based on knowledge I gained from the literature.

5.7.4 The Researcher's Bias and Limited Understanding of Information Security

The research was also limited by me as a researcher and my bias. From conversations and from the non-academic literature (i.e., threat assessments and NSR's reports) I had a preconceived notion that SMBs generally have weak security cultures. This bias may influence the way I interpret the information from the informants and the way the questionnaire is formed. I have

to the best of my ability tried to keep an open mind and to keep the focus on exploring the data from the interviews with an open mind.

5.7.5 Possible Politization of China as a Threat Actor

I use China as a case because it is a country that Norwegian companies are particularly warned about by the Norwegian government. In the intelligence literature, there is agreement among scholars that China is conducting economic espionage (Lowenthal, 2014; Mattis & Hoffman, 2017). A Chinese intelligence law passed in June 2017 (Mattis, 2017; Mattis & Hoffman, 2017) manifests the requirement of all Chinese citizens to assist and cooperate with national intelligence efforts if asked to (Bergløff, 2019; China Law Translate, 2017; Oksholen, 2018). Of relevance to this thesis, it means that the SMBs' Chinese customers, partners, and owners may be asked, and in that case, they are obliged to, cooperate with the Chinese government to collect information about the Norwegian SMBs and their technology development, and pass it on to the Chinese intelligence services. The Chinese government has both denied and acknowledged the law's existence. In a comment to Universitetsavisa in April 2018 the Chinese embassy in Norway denied knowledge of the law (Heng, 2018), but in February 2019, a Foreign Ministry Spokesperson at the Chinese embassy in the Philippines, Geng Shuang, admitted that the law exists, and claimed that the West has a "wrong and biased interpretation of relevant Chinese laws". He points out double standards in Western state's criticisms of the law and states that "it is an internationally accepted practice to protect national security through legislation and require organizations and individuals to coordinate with a country's intelligence service". Lastly, he states that "China has not asked and will not ask companies and individuals to collect or provide data, information, and intelligence stored within other countries' territories for the Chinese government by installing "backdoors" or by violating local laws" (Shuang, 2019). Although the narrative of China as a threat actor might be politicized, there are credible academic arguments that strengthen the credibility of the Norwegian government's warnings about Chinese espionage against Norwegian companies, and I lean on those notions.

In the next chapter, I present the findings along with the analysis and discussion, using the analytical framework described in Chapter 4.

6 Findings and Analysis

This chapter answers the research questions and analyzes the findings. It provides insight into the security cultures in the sample by presenting data which reflects their knowledge, attitudes,

experiences regarding espionage, IPR in China and Chinese business culture, and ways to protect their economic information in their business relations with Chinese customers in China. The analysis is based on their answers, secondary data, and the theoretical framework presented in chapter 4. The analysis draws on selected concepts from literature in intelligence studies, organizational studies, and ICT studies. The chapter is divided into four sections. The first section, 6.1, presents knowledge and attitudes found in the data, 6.2 present findings about the state's information sharing, section 6.3 presents findings on how the SMBs obtain relevant knowledge, and section 6.4 presents findings on solutions the SMBs have found to navigate in China where they experience that IPR is a challenge. Because the dimensions of security culture are interconnected, some of the findings on these factors will overlap.

6.1 Knowledge about, and Attitudes to, Chinese Economic and Industrial Espionage

This section presents the findings about the SMB's knowledge of, and attitudes to, economic and industrial espionage. It includes perceived risks regarding IPR when operating in China, and about the Chinese political economy.

6.1.1 Varying Knowledge about Industrial and Economic Espionage

The SMBs use the terms 'industrial espionage', 'espionage', or 'to steal', and define these terms similarly. Two quotes represent their definitions well: "industrial espionage is when an external actor actively tries to steal sensitive commercial important information from another actor. Steal or use the stolen material" (SMB Orange China contact, 2017). SMB Red CEO (2017) defined industrial espionage as "systematic work to get access to intellectual property that is not yours. I think there are people out there who work systematically with puzzling together pieces of information".

Green and Red leaders knew little about methods used to collect IP and trade secrets. The knowledge of the other China contacts (Yellow and Orange) differed. SMB Yellow China contact (2019) knew little: "I don't know very much other than what I have read about. That someone can enter your computer if you are logged onto an unsecure network at a hotel or something like that. Both on mobile phones and computers". Orange on the other hand, and the IT chiefs had specific knowledge. The indicates that the IT chiefs had more knowledge than their leaders, especially about network exploitations. Only Green IT provided detailed descriptions of various ways to collect information:

> *the point is that the personal contact is what intelligence [officers] would have operated with. And they could also place a person inside the company as a legitimate employee, but then the company does not know that this is an agent. It could be one from our own country […] And then you have national intelligence organizations that are interested in everything they can get hold of. When it comes to intelligence, they will most often be interested in just reading, and not do too much because then they will reveal themselves. But they can use the information in the future. The perhaps largest danger that there has been talk of, is telecommunication and mobile senders and those kinds of things. One thing is that they can listen in, but it is fairly easy to discover those things. The largest danger is if they store a thing in these devices that will lay there for some time and then one day, they will send a commando that destroys the whole system. You will never find out before it is too late, that is the real very large danger, right* (SMB Green IT Director of Technology, 2019).

SMB Green IT Director of Technology (2019) further specified business competitors' network operations: "business who tries to get specific information. It is difficult to say if someone tries to take everything, if it is of more commercial it will often be very specific things they are after. One or more chosen companies, and they are after something special. I think it often is big companies in oil, gas and not least military".

6.1.2 Knowledge about Chinese intelligence and sectors of intelligence interest

All SMBs either knew (Orange, Yellow and Green IT Director of Technology) or was slightly aware (RED CEO and Red IT) that China is one of the countries the Norwegian intelligence services highlight as a threat actor to Norwegian enterprises. "China. As long as they are not western allied, you need to be on the alert" (Green IT Director of Technology, 2019). SMB Red was more uncertain: "it was said it was the Chinese who was behind the attack on Visma, so apparently that is an actor" (SMB Red IT Director, 2019), and "From the media I get the impression that China traditionally has been involved in industrial espionage, is that right?"(SMB Red CEO, 2017).

RED and Orange expressed knowledge about the challenges China faces in their respective sectors, health, and renewable energy. "China has an enormous problem with carbon footprint

and environmental pollution. The Chinese government is quite visionary and invests in and integrates renewable energy (SMB Orange China contact, 2017). “On the countryside there are no health services. So, offering a quality health service to their population is a large challenge. … They need to renew their health system and looks to Norway because we have a well-functioning primary health service” (SMB Red CEO, 2017). The national threat assessments in 2017 specifically mentioned these two sectors to be of particular interest for Chinese intelligence (The Norwegian Intelligence Service, 2017, p. 35; The Norwegian Police Security Service, 2017, p. 8). Orange considers espionage to be an issue in China (and elsewhere), and do regard the company as a target, whereas SMB Red CEO (2017) said “we have not heard about espionage in our sector”. As presented in chapter 6.1.2, Red CEO had not read national threat assessments, but had read in media that China was behind the attack on Visma.

Further, generally, the SMBs did not devote attention to who the actors behind espionage are, but rather to secure their IP and trade secrets from theft. SMB Orange China contact (2017) reasoned about the lack of focus on the actor: “Espionage happens everywhere, that’s why I don’t like to point out specific countries. It happens between all countries in all forms and to all degrees”. During the interviews, the others mentioned who they consider specific threat actors in China: Chinese universities (Green Leader), and business competitors in China (Yellow, Red CEO). Both IT Chiefs were concerned about network operations but differed in their knowledge about who is behind these operations. “It must be some hackers. Who they are I do not know” (SMB Red IT Director, 2019). Only Green IT Director of Technology specified threat actors behind network operations: “I think there are three categories: “amateurs who do it for fun, business who tries to get specific information. […] and national intelligence organizations”. He also describes insiders: «[an intelligence service] could also place a person inside the company as a legitimate employee“ (SMB Green IT Director of Technology, 2019).

Only SMB Orange China contact (2017) clearly said they consider economic and industrial espionage as a threat to them: “we consider it as a large problem and regard it as a threat”. The others express stealing of IP as something they protect themselves from, without referring to it as economic or industrial espionage. Besides Orange, the other companies seem to know that they need to be careful and protect their IP in China and that Chinese companies share information among themselves, and that the CCP is involved in every company, but the data indicates that they do not regard theft of IP as industrial or economic espionage. This is most evident in Green Leader’s contradicting reasoning around the fear that a Chinese university

would do reverse engineering and share it with the local government, but he also said that they do not believe the Chinese government would be interested in their products.

6.1.3 Attitudes to if the SMBs Considers themselves to be a Target for Espionage

The SMBs differ in their perceptions about how industrial or economic espionage relates to their companies. Only Orange clearly states it regards itself as a target for espionage. The other companies indirectly regarded themselves as targets for espionage, but they did not use that term, they used words like "to steel". Their attitudes can be linked to the size of the company and how the SMBs assess the attractiveness of their IP according to the IP's age.

Orange, Yellow, and Green express an impression that large companies are the main targets for economic and industrial espionage. I.e. SMB Green IT Director of Technology (2019) believed that network operations are used by "business who tries to get specific information. […]. One or more chosen companies, and they are after something special. I think it often is big companies in oil, gas, and not least military" (2019). Green Leader gave a deeper reasoning for why she/he does not consider SMB Green as an interesting target for state actors:

> *I see the problem for companies like Statoil or Aker Solutions because they have larger valuables. Development plans – it would be catastrophic for, let's say Aker Solutions, to be in a competition with a Chinese company for a mission worth hundreds of millions. If [the Chinese conducted] industrial espionage [and] managed to hack, to find documents with offers, meaning the type of documents who are sensitive for winning a contract – I see that [problem]. But the sums we handle, and if we would be of interest to Chinese government - no, I strongly doubt that. It's some million kroners, they will not bother.*
>
> *There must be something to gain if a foreign power should spy on us. Something they can use and something they would not have access to in another way. Defence, contracts, new types of technology. We don't represent new technology. We process technology that has been known for years. I cannot see what they would steal from us* (SMB Green Leader, 2019).

However, SMB Green Leader (2019) contradicted itself when she/he elaborated on why Green declined to enter a cooperation with a Chinese university that demanded access to the source code: "We are concerned about reverse engineering of our product and sharing of it. And concerned about if the state, the region, and the local university will share it with local industries, so that in ten years' time we might find our products made by Chinese producers in China without our consent". Here Green Leader specifically mentions the Chinese government's role in supporting the local industries, which is economic espionage. Lastly, although SMB Green process old technology which Green Leader says is not of interest to others, the informant also said that the source code is valuable and well protected. When they protect the source code, it implies a belief that others can have an interest in steeling it. The findings indicate that this informant does not see that steeling of intellectual property, for example through reverse engineering, is industrial, or economic espionage.

The sample regards the age of their IP to be of relevance of weather their company is a target for espionage. Orange and Red are newer companies and produce fairly new technology. Orange (2017), who considers espionage as a direct threat, said their product "is part of the key technology if we are to shift to renewable [energy]". SMB Red on the other hand did not see their company as a target for espionage, but as a target for competing companies who want their IP, which is industrial espionage. Further, Green Leader and Yellow do not consider their companies as targets for espionage because their products are older and because their companies are small, and. "I do not think we are big enough, there is a fairly limited market and a niche product. There is not any mass production or very large volumes, so I think it is less lucrative. At least that is my assessment" (SMB Yellow China contact, 2019). Yet, although SMB Yellow's patents are expired, meaning the product is more than 20 years old, as presented under chapter 6.3, Yellow had experienced industrial espionage in China when a Chinese client copied their 'old' product without Yellow's permission. Thus, this old IP is attractive for industrial espionage despite its old age.

This section, 6.1, had presented knowledge and attitudes found in the data. The next section presents one of the main findings of the thesis: The state's limited outreach of information sharing, and that the informants did not see the need for assistance from the government.

6.2 The State's Limited Outreach of Information Sharing

This section presents one of the thesis main findings: the state's limited outreach of information sharing of their threat assessments, and a view among the sample that they do not need information or assistance from the state.

As previously stated, the thesis defines state assistance to include the sharing of relevant information, including intelligence information, from the state to private enterprises. None of the SMBs received information from any government body about economic or industrial espionage, about the risks involved when doing business in China, or of the importance of protecting their assets. In Norway, NSM, NorSIS and the Police are the main entry points for private companies for reporting incidents and to receive support and information. PST gets involved if it is likely that a foreign actor is behind a network operation (both exploitation and attack) (Police Business Contact Coordinator, 2019). The contact with government agencies were limited. Orange experienced they received "very good support in projects abroad" from Innovasjon Norge (SMB Orange China contact, 2017). Red had on their own initiative invited a team from KRIPOS who did a digital security check of their systems, and SMB Green Leader (2019) said «we have not received any approaches from the government if we should be in a risk group". So, the sample did not have any contact of significance with any government body.

Further, the sample expressed that they do not need or desire to receive more information from the state or found the information in the annual threat assessments irrelevant. Two of the SMBs did not see the need for the government's guidance and information about threats: "No, I feel these types of things are covered in media. And I participate in IKT Norge's health forum. I know NSM exists and that they are a resource I can contact if it should be necessary, if we discover we are hacked and cannot figure out what has happened […] No, I think it is more important to pay attention internationally, because all our servers are in another country. It must be assessed from case to case" (SMB Red IT Director, 2019). "No, we know where we can find people if we get a problem. The police and the like" (SMB Green Leader, 2019) It seems these two respondents regard the contact with the government as relevant only after an unwanted incident is revealed, and not as a part of preemptive measures. This corresponds with the Police Business Contact Coordinator (2019) who says the police are contacted after incidents more often than to prevent incidents. In contrast to its leader, Green IT Director of Technology (2019) was positive to receiving information, *if* it was specific IT technical information that they could use in their work. SMB Orange China contact (2017) was the only one that had read threat

assessments and found PST's threat assessments superficial because he/she obtained the same information from international media, and the technical updates from their technical employees.

The sample's view conflicts with the views expressed by Abelia. Abelia is a trade and employers' association for technology companies. It believes that enterprises need government guidance and information about threats and finds that the government fails or is unwilling to share information with enterprises (Abelia, 2018, p. 3-4). Moreover, they urge the authorities to strengthen the sharing of security information, such as threat assessments, to both private and public enterprises. Some information must be shared immediately "to make quick countermeasures" (p. 4). "It is important that relevant actors be informed so that serious incidents are not given a greater scope than necessary due to the lack of will or ability of the Government to share information" (p. 4). Abelia further states that some "relevant businesses have pointed out that it is difficult to obtain relevant information from the NSM" (p. 3). Abelia further wrote that Abelia "recommends that NSM and other relevant agencies be obliged to share relevant information. … The new regulations must also make clear demands on the specific threat assessments and other safety information to be shared. It should also be stated by regulations how this type of information should be conveyed (oral, paper, electronic) to the recipient" (p. 4). Abelia's requests were not included in the Security Law (Sikkerhetsloven, 2018). It does not give clear directions for when governmental agencies must share information with private enterprises.

Næringslivets Hovedorganisasjon (2019), Abelia (2018) and NOU 2015: 13 found that there is a need for improved collaboration between the government and the business community to improve the national digital security, and as the later discussions highlights, this thesis supports that notion. Abelia acknowledges the threat of economic espionage and acknowledges that "The distinction between what is an attack against Norwegian society and what is an attack against individual businesses may be unclear" (Abelia, 2018: 3). In their written suggestions to the proposed regulations to the new Security Law, Abelia (2018: 3) states that "the business community … is entirely dependent on support from the Norwegian authorities in the form of ongoing information exchange in order to be able to eliminate or limit harm to the society". Næringslivets Hovedorganisasjon (NHO) (2019) called for a strengthening of the exchange of threat assessments and other information between the government and the business community to prevent unwanted digital security incidents. (NOU 2015: 13, p. 297) found a need for

increased awareness and security demands specifically for SMBs, and a need for the government to offer SMBs guidance and help with information security. However, the government attention is directed to SMBs only in sectors considered critical for national security functions. Private companies and enterprises are responsible for securing their own information from theft (Gjesvik (2019). Gjesvik (2019) found that the best prevention against cyber security incidents (regarding companies in the sector of critical infrastructure) is done by companies themselves by "updating software regularly, adopting better practices and training the employees. Still, the public sector has a role to play in providing information, regulating and setting standards, as well as raising awareness in the companies" (Gjesvik, 2019: 31).

There are governmental informational resources open available for anyone interested online. These include PST's threat assessments and NIS annual world assessments. NSM's web pages have practical real-life guides for protecting the companies' assets. The Norwegian Police Security Service (2017; 2018) specifically emphasizes their threat assessments' relevance for Norwegian enterprises to use in their own security work. They dedicated significant space in their threat assessments of 2017 and 2018 to public and private businesses in which they, among several factors, describe how foreign intelligence officers' approach Norwegian citizens for recruitment, and how network exploitation operations are conducted. However, none of the SMBs in the sample collect nor read these. This findings supports findings in NSR's KRISINO reports (Næringslivets sikkerhetsråd & Opinion, 2015, p. 5; 2017, p. 6, 16; Næringslivets sikkerhetsråd, 2021, p. 6) which found that few businesses read the PST, NSM and other governmental threat assessments and security reports. From 2017 to 2021 the companies reading of PST's open threat assessment increased from 16% to 20% of the sample, and the reading of NSM's risk assessment was stable 10-12%. The 2021 report concludes that the information in the governmental assessments does not reach the business community well enough, with the likely result that the business community is not well informed about the threat landscape they operate in (p. 34). The thesis data can provide insight into why some SMBs do not read these threat assessments. SMB Green IT Director of Technology (2019) elaborated:

> *No, I have not read them [PST's or NIS' threat assessments or NSM reports]. I see what is written in the media. It could be interesting to read just to see if it really is what I think it is like. I do not think it is very interesting, it sounds like there is a lot of obvious information - like that*

> *China is a threat. There is much information they cannot publish. We need technical information that we actually can use … I would like to receive technical information from them [(the government)]. But they cannot give too much information.*

Abelia (2018) expressed dissatisfaction with the government's information sharing, especially information from the intelligence services. Their claim corresponds with Gjesvik (2019: 32) finding that "the limited tradition of sharing intelligence in Norway hamper[s] the ability of intelligence agencies to provide relevant information". (Police Business Contact Coordinator, 2019) said that the police can improve their communication: "The police can give information that is so detailed that the enterprises may recognize themselves in it. Enterprises have given feedback that, for instance, the reports by PST need more detailed descriptions about for instance vulnerabilities and what measures they must implement". "We recommend companies to seek memberships in organizations like NSR [which cooperates with POD]. They can guide and give information. They have information that is within easy reach" (Police Business Contact Coordinator, 2019).

The data and findings from NSR reports indicate that PST and other governmental security related organizations at the time did not reach parts of its audience with their information. A recent interview with the former deputy director of PST, Hedvig Moe, indicates that this is still a challenge. She said: "besides the assessments of the secret services there are extremely few guidelines from the government". (…) It is hard for the business sector to operationalize the threat and know how they should handle it in their everyday lives. Because there is a lack of a policy on China and guidelines from the government" (Kibar, 2024).

This section analyzed the findings that the sample does not read or find the open threat assessments relevant and related this finding to existing literature on the topic. The next section presents ways in which the SMBs obtain relevant security information, such as information about espionage.

6.3 Media and Experiences: The Main Sources of Information and Knowledge about Chinese Economic and Industrial Espionage

The section presents the findings on how the SMBs obtain security information regarding espionage and how to protect their assets in Chinese business relations. The data suggests that media, experiences, and ICT suppliers are the most important sources of information about espionage and protection of economic information. These factors contribute to setting securing of economic information on the companies' formal and informal agendas. In addition, the data suggests that the SMBs have learned about Chinese culture around IPR through interactions and experiences when doing business in China. The first sub-section presents the importance of media, and the second sub-section presents the SMBs experiences and shows how 'learning by doing' has increased their knowledge about Chinese business culture and shaped their view that IPR is less valued in China than in Norway.

6.3.1 Media

The SMBs mentioned TV news, news websites, and newspapers as main sources of information about economic and industrial espionage, and about China (Green IT Director of Technology, 2019; Orange, 2017; Red IT Director, 2017; Yellow, 2019). Orange and Red emphasized international news such as BBC and Bloomberg. SMB Orange China contact (2017) "pays close attention to China on a daily basis" also through reading Chinese and Asian newspapers. The IT directors prefer information sources for IT professionals, such as IT-specific journals, websites (www.digi.no, the Register), and forums i.e. Facebook, subscriptions for updates from national Computer Emergency Response Teams (CERT), such as US-CERT and NorCERT2. These sources give technical details of security incidents that are relevant in their work with digital protection of the companies' information and other assets. They experience that the mainstream media does not give them this information. The thesis does not focus on the technical protection methods, but it is relevant to present the sources of such technical information that informs the IT directors knowledge.

Media coverage of larger security incidents and scandals put espionage in general on the SMBs' agendas (Yellow, Green and Red). These issues presented in the general everyday Norwegian media (i.e. TV2, NRK, VG, Aftenposten) became conversation topics during lunches and leader meetings and turned their attention to their own securing measures (SMB Yellow China contact, 2019). Respondents specifically mentioned the media coverage of the network attack on Visma, and when former Minister of Fisheries, Per Sandberg, traveled to Iran with his government mobile phone. Quotes from SMB Red represent the sample well. For instance, "if there is a case in the media about ten million e-mails being leaked, then I might use the incident to

forward the article to the employees and tell them to change their passwords or other things, such as making sure the two-step authentication is in place for certain accounts" (SMB Red IT Director, 2019). SMB Red CEO (2017) confirms this: "The IT Chief sends us e-mails with links to articles that say for example this company was exposed because they did not have good password routines - to remind us to change our passwords and be cautious" (2017). SMB Yellow China contact (2019) said: "we assess things from media, and there has been focus on securing information lately, on travels with both politicians and business sector". As such, information from the media can also contribute to improving security behavior. For example, (SMB Yellow China contact, 2019) said:

> *the media's focus on the Sandberg case[3] has put the issue [of securing information] on the map. We have discussed if we should use barrowing phones[7] when we travel. We used it for a brief period of time but ended it because the values are stored in the cloud, not on the phone or the computer. It might be that we should have taken even better precautions. I will admit that lately I have deleted more drawings and models that I have had on my PC prior to travel. In addition, I use common sense. Although it may not be secure enough if you are logged onto a hotel Wi-Fi and such things.*

The SMBs answers corresponds with Abelia's experience: "when there are cases in the media, we experience an increased interest and attention among our members to their own company's the value chain and the actors and the information in the different parts of the chain" (Abelia, 2019).

The data presented above indicates that media coverage of security incidents can contribute to putting security on the SMBs agenda, raising awareness and increase knowledge about threats and protection of assets. Thus, media can be considered an influential factor in the SMBs' security cultures. Other important sources of security info and threats are their suppliers of cloud services, cloud servers, and their IT systems, which give specific information about digital security (SMB Yellow China contact, 2019). (SMB Red CEO, 2017) also said they "received lots and lots of warnings about keeping information to ourselves […] from Chinese who sympathize with us and what we are trying to do in China, and from Norwegians familiar

[7] "Barrowing phone" is a direct translation for the Norwegian word «lånetelefon». It means a phone without access to sensitive and valuable information.

with China". The last quote can nuance the one-sided available information in NIS's and PST's open threat assessments about the threat of Chinese espionage.

This section presented how media plays an important role in informing about espionage, and how it can contribute to setting the topic of Chinese espionage, and methods about how to secure information during business travels on the companies' agendas. The next section presents how the companies own lived experiences, (and for one SMB also research) with disrespect for IPR in China has shaped their attitudes and knowledge.

6.3.2 Experiences and Research as Sources of Knowledge about Chinese Business Culture and Political Economy

The data indicates that Yellow, Red and Green have accumulated knowledge about Chinese business culture, and the status of IPR in China through years of practical experience. In addition to experience, Orange, distinguishes itself by its thorough research prior to entering China. SMB Orange China contact (2017) told, "we analyze political, economic, social, technical and legal questions before reach out to local companies in new countries". In addition, informant Orange has formal education in Asian cultures and Mandarin language and says he/she follows Chinese politics: "Mainly the Five-Year Plan, which is a political tool they have used since [the Chinese communist state was established]. The policies outlined in the plan are always implemented" (SMB Orange China contact, 2017).

Further, SMBs Red and Yellow perceived Chinese companies to be nationalistic. SMB Red CEO (2017) said "they have a different culture for seeing themselves as a part of the society. They are more nationalistic. Most Chinese [have an attitude that expresses] 'we contribute to the building of China'". Yellow (2019) elaborated:

> *It surprises me how much information they [(Chinese companies)] share between themselves – despite that they are competitors. […] If we offer something to a customer then he knows what a competitor has paid. Information and employees float between companies. We do not experience this in other cultures to the same degree. […] I think they are very concerned about helping each other against the West. 'Here we stand together to be able to compete with the*

> *Western companies so then we must cooperate to find best practice'"* (SMB Yellow China contact, 2019).

All SMBs knows that China is an authoritarian capitalistic one-party state and are aware of the Communist Party of China's (CPC) influence and power in international trade relations in China. Two quotes represent this knowledge well: "A Chinese company does what the government tells them to do. They cannot do anything without permission from the government. The governance is extremely strong. I have had good leads [(sales options)] that were stopped by the Party" (SMB Red CEO, 2017). SMB Green Leader (2019) experienced that all their customers had a representative of the CPC and understands this as a requirement for Chinese companies to be able to succeed with doing business in China. (SMB Yellow China contact, 2019) told "There is a tight relationship. We see that it is important for our customers to have good relations with especially local government ".-Green Leader expressed a belief that Chinese universities are more likely to steal IP than Chinese companies are:

> *If you have the right people, you can make something equivalent based on our manual. Sooner or later, someone will program a product equivalent the functionality our product, but I do not think this will come from [Y - anonymized Chinese state-owned company (SOE) that is their customer], but from a university. But this is done all over the world, independently of China. … I think a large company like [Y] would have a problem with being a serious international company if they stole technology from others* (SMB Green Leader, 2019).

> *We can buy a license of their product, that they developed, and they can buy a license from us. It sounds scary to send a license over the Internet to install software on their machines in China. You might think that is sending the technology straight into the lion's cave – that they copy it and sell it around the world. If they had the resources the CIA has to do reverse engineering, it would be possible. Of course, they sign an agreement, and it might be that they do not stick to it. I think a large company like [Y] would have a*

problem with being a serious international company if they stole technology from others" (SMB Green Leader, 2019).

The informant's attitude differs from both academic literature and threat assessments that states that Chinese intelligence have one of the most advanced intelligence systems in the world, and the willingness to use this to steel technology (Lowenthal, 2014; Mattis, 2015; Mattis & Hoffman, 2017; The Norwegian Police Security Service, 2017).

6.3.3 Experiences with IPR and Industrial Espionage in China

This section presents how experiences has informed the informant's knowledge and attitudes to Chinese espionage and IPR in China.

The sample expressed a perception that IPR is regarded and practiced differently in China than in Norway and Western countries. As explained in the introduction, IPR is based on Western individualistic thinking which collides with China's more collective thinking. Red CEO's elaboration on the issue represents the sample well:

We are aware that we must be a little extra careful in China. They have a different culture for what it is to steal intellectual property. We call it that, and they call it, what is it they call it … 'to learn from the best' is what they call it. So, the culture around that is very different, we are aware of that. The cultures in the Nordic countries are very similar, and to a certain degree also in England. […] In Norway I experience that people respect our IP and knowledge, whereas in China you understand that they want to learn and copy what you have (SMB Red CEO, 2017).

Only SMB Yellow informed that had been victim of industrial espionage in China. A Chinese client, a factory, copied their factory machine without Yellow's permission and used it for production:

They are completely open about that they have copied us. The machine looks like ours, but it does not work optimally, because

> *now the customer has come back to us and ordered a new machine from us. We have seen other incidents like this previously. This was a customer where the factory has copied us, that is a threat to us, but it is less of a threat than if a supplier [(other suppliers are Yellow' competitors)] did it. We have also seen a Chinese supplier that copied equipment from us, and they still deliver to some clients, but the quality is lower so the only places they can sell this equipment is mostly to those factories that delivers end products of lower quality, and who cannot afford to buy the best equipment* (SMB Yellow China contact, 2019).

Green and Red shared what they experienced as blunt attempts to steel their IP. SMB Green Leader (2019) said they are skeptical to requests form Chinese universities because they feared reverse engineering and shared an experience: "they [(the university)] say getting access to the source code is a requirement for cooperation, but of course we refuse". (Red CEO, 2017) shared an experience: "It's funny, they wanted to establish a demo center over there [in China], then they said, 'we have bought a server so you can just download all your software here on our server so that we can demonstrate it locally'. Ha! Like that was going to happen!". Even though Orange and Green IT had not discovered any theft of their IP or security breaches, they expressed possibilities of undiscovered incidents. A quote from SMB Green IT Director of Technology (2019) sums it up well: "I cannot say I have never seen anything like that, I can say I have never revealed anything like that. That's how you must think if you really want to prevent it".

To sum up sections 6.1 and 6.3: The data indicates that media, ICT suppliers, and the individual SMBs' experiences are the main sources of information and knowledge about espionage in general and in China, and about how to protect the company's assets in business relations in China (and elsewhere), and digitally. Orange distinguishes itself by having formal education and that the company does research before they enter a new country. Section 6.2 presented how the sample does not receive information or other assistance from the government, and also that they do not find a need for such assistance. The next section presents various ways in which the

companies try operating successfully in China whilst also protect their IP and trade secrets in Chinese-Norwegian business relations.

6.4 Coping Mechanisms for Dealing with the Risk of Espionage in China

As presented in previous sections the SMBs are aware of risks of theft of their IP when operating in China. To deal with these issues the SMBs use different strategies. These include non-disclosure agreements and joint ventures. The sample's answers indicates that the SMBs are precautious in these matters, and their decisions are based on rational assessments. To have a Chinese citizen involved in the company is used for two reasons, one is for protection of their economic information, the other is to successfully operate in a foreign business culture.

All SMBs have a Chinese citizen involved in their company because they find that it gives them an advantage for doing business in China. One has a shareholder, two have a Chinese citizen wholly or partially employed, another has an active Chinese investor, a Chinese private company (Orange), meaning the person participates in some board meetings, but do not get access to the source code of the SMB's IP. These persons know the Chinese culture and the political system, the do's and don'ts for making successful business in China. SMB Green Leader (2019) elaborated on the advantages: "[Our Chinese citizen contact person] knows Chinese and European business culture, is fluent in English, used to European code of conduct. [The person] is concerned about risks [(talk to the right persons, do they have money, is the contract legal, anti-corruption in China)] and is two steps ahead of us, is our mentor and it is essential to have such a person. There is no doubt that [the person] is the reason for our success in China".

One of the ways to involve Chinese persons with the company is through joint ventures (JVs). Orange has entered, and Red tried to enter, JVs in China with Chinese companies. A JV can be an economic cooperation in which two or more parent companies establish a company of which they both/all share ownership (Sætermo, 2015). The objectives for entering JVs are often "entering new markets, exploiting learning opportunities, and joining forces with local partners in research and development and innovation (Bidault, 2012; Ghauri, Cave, & Park, 2013; Inkpen, 2008; Mahmood & Zheng, 2009)" (Nguyen et al., 2019). Red experienced the process of establishing a joint venture as challenging and expensive, and they ended it because they discovered a lack of market expansion strategy with the Chinese company: "They had no

thoughts, no resources, zero content, they just wanted exclusive rights [(to distribute Red's product in China)] … There was a lot of mess around this" (SMB Red CEO, 2017). On the other hand, Orange entered a joint venture with their Chinese investor, a Chinese private company that they had known for a year. SMB Orange China contact (2017) expressed joint ventures as a strategic tool for protection in the Chinese market: "Now I speculate, but it is possible that if you go to bed with a Chinese actor, a partner company, it may make you less of a target. One of the reasons we enter a joint venture is that we need protection in the Chinese market from a Chinese partner that has a stake in us, right. So that is an important part of the strategy". SMB Green IT Director of Technology (2019) elaborated on how she/he thinks about espionage through cooperation:

> *"(…) you also have to look at it from both sides. Is it only we who are open and give them access to things, or do they also give us access to their things? When it is mutual it makes us more comfortable with the cooperation. And the companies you cooperate does not necessarily know what their own national government is doing. That goes for us too, what the Norwegian intelligence [services] do, or American or Chinese*".

Another strategy to protect IP is through use of Non-Disclosure Agreements (NDAs). Use of NDAs are common securing measures in businesses in general and within the sample. Orange and Yellow had differing experiences with NDAs in Chinese relations. Orange said they used NDAs when negotiating to protect their information. Yellow, on the other hand, perceived NDAs as difficult in Chinese relations:

> *Today a Chinese client asked for a copy of the program in one of the machines we supply them with. We considered if we should ask them to sign a non-disclosure agreement so they would not spread the information, but we know that such agreements are not worth much, and it can be experienced as an insult in that we don't trust them. The alternative was to give a protected formatted copy of the program, and not bother with a signature on a non-disclosure agreement. We decided on alternative two* (SMB Yellow China contact, 2019).

The data further indicates that all SMBs have an awareness, and are cautious, about what information they share when they are in China.

> *I work very closely with them [(the Chinese investor, a Chinese private company)]. […] I trust them to the degree that, of course, I double check things if I am uncertain. For example, when I use their platform. Then I am careful. But we have tested it, and it is alright. And we know that we can work closely with them, so then the dynamic is different. […] They want us to succeed. We are entering a joint venture with them in China to be able to operate there* (SMB Orange China contact, 2017).

SMB Green Leader (2019) told:

> *People in my wider circle working in the security sector tells us that during negotiations they sit across the table from you and tap your computer and watch what you are writing. We are very careful in the way that if we are writing an e-mail than we do not do this while sitting at the same table. We work with documents that are known for them and we have the same copy that we discuss the content in. Then we go home and work more on it. If I use my computer, I use VPN. We have researched to find the VPN we consider the best.*

As presented previously Yellow experienced that a customer had copied one of their factory machines. The following quote shows how they handled this unwanted incident, and how they reason around their choices for coping with this challenge:

> *We communicate with these actors. We have considered cooperating with them to try to limit it. But obviously we might lose some jobs because they can buy cheaper products, but at the same time we think that those companies that buy from competitors that has copied us would not have the resources to buy from us anyways. But clearly, they do destroy a part of the market. But as said, we have tried to limit it through delivering superior equipment with larger precession, and the Chinese who has tried to copy us up until now have struggled with reaching the same precision and quality in*

> *the material. There is not really much we could do with this. We have not tried to follow any legal steps or anything like that. We have this with copyright, but the patent is expired, so there isn't much we else we could have done than to keep our cards close to the chest and visit those customers who have bought this [illegally copied] equipment and hear how it is working and try to track how successfully they are in copying us. And to convince the customer that it is not just the equipment, but follow-up and service and know-how that they also get if they buy from us* (SMB Yellow China contact, 2019).

Chapter 6 has presented and analyzed the data. The next chapter discusses these findings through the concepts presented in Chapter 4.

7 Discussion

This chapter discusses the analyzed data presented in chapter 6 using the theoretical framework from Chapter 4 to explain the findings. The chapter is divided into three sections. The main research question: *How may media, state information sharing, experiences, knowledge and attitudes related to Chinese economic and industrial espionage influence SMBs security cultures?*, is answered in the different sections. Section 7.1 also answers the question *How do private Norwegian small and medium sized businesses relate to and understand economic and industrial espionage in their Norwegian-Chinese business relations?*. Sections 7.2 answers the question: *How and from where do private Norwegian small and medium sized businesses obtain information and knowledge about industrial and economic espionage?*. Section 7.3 answers the question *How do private Norwegian small and medium sized businesses relate to the dimension of state information sharing?*.

7.1 Knowledge and Attitudes

This section discusses how knowledge and attitudes can influence behavior, and as such security culture. It also answers the question: *How do private Norwegian small and medium sized businesses relate to and understand economic and industrial espionage in their Norwegian-Chinese business relations?*

Van Niekerk and Von Solms (2006) framework for information security culture states that knowledge, attitudes and behavior are interconnected. First, employees need to have knowledge about how to protect the information considered valuable. When they have this knowledge about how to protect the company's valuable information in their everyday work, they can contribute to a strong security culture. However, if their attitudes and believes does not align with the knowledge they have received through training, education and awareness campaigns, they are likely to behave in contradiction to the knowledge with the result that the information will be less protected.

The data indicates that the SMBs have gained relevant knowledge through education (Informant in SMB Orange) and the others through lived experiences, media coverage and ICT suppliers. The analysis revealed that the informants had good knowledge about Chinese culture, and the heavy presence and influence by the CCP in Chinese companies. According to Van Niekerk and Von Solms (2006) knowledge and attitudes must align in order for persons to behave in a way that protects the information. The information from media and experiences matches the experiences and attitudes they have had with disrespect for IPR in China. According to Van Niekerk and Von Solms (2006) this would lead to higher possibility that the employees protect their information in a desired way.

The SMBs have knowledge and attitudes that IPR is a challenge in China. To deal with this threat they have found ways to operate to protect their IP. These ways are behaviors. It varies how successful they find these coping mechanisms. SMB Orange entered joint ventures as a strategy for protection in the Chinese market. SMB Red failed with joint ventures. SMB Green enter cooperation with skepticism and assesses the degree of how much the other part are willing to share in a cooperation.

According to Van Niekerk and Von Solms (2006) knowledge is crucial for protection of information. Among the sample it seems like there is a piece of a puzzle that is missing: knowledge and understanding about how their technology and security culture matters for national (economic) security. Except from Orange, the others do not see themselves as targets for espionage, even though three of them have either experience industrial espionage or what they perceived as blunt attempts to it. One of the findings is that the there is an attitude among the informants that they do not see a need for information from the government about espionage, and about how to protect their information because they find this information elsewhere, like

media, and ICT suppliers or relevant forums for IT security. Næringslivets Hovedorganisasjon (2019), Abelia (2018) and NOU 2015: 13 find that such state assistance is crucial for the companies own securing of information, and also for the companies' role in protecting information that is of importance to national security. As such one can say that some of the informants in the sample might lack knowledge regarding security threats which could be applicable for their industry which could be, and that is essential for the proper securing of information when they are in China. According to Van Niekerk & Von Solms' (2006) framework the SMBs that lack knowledge will negatively affect their behavior, meaning how they protect their information. A such a lack of knowledge will negatively affect the company's security culture.

However, it might be possible that they do find the same information in the open threat assessments other places. They perceived that they found the information that is practically needed in their everyday lives through the everyday news in media.

The data revealed that only one SMB has a clear understanding that espionage is a threat to them. The three others revealed a weak understanding of what espionage is. They call it "theft" of IP, instead of calling it espionage, and except for SMB Orange the data indicates that some of the informants see this as two different things. It seems they think large companies with larger income are the main targets for espionage. This attitude was present even though they all had experienced what they considered blunt attempts to steal their IP, SMB Yellow had experienced industrial espionage. This finding indicates a lack of knowledge that also SMBs are targets for espionage. According to Van Niekerk and Von Solms (2006) a lack of relevant knowledge can lead to poor protection of information.

7.2 How Media and Experiences Can Influence Security Culture

This section discusses how media and experiences can influence knowledge, attitudes and behavior, and as such security culture. The data indicates that for the sample media is an important source of information about espionage, about China and about ways to secure information. Media also contributed to putting the topic of securing information on the agenda. This corresponds with Happer & Philo (2013) the who states that media is an important source of information, and it contributes to setting topics on the agenda. Happer & Philo (2013) argues that the effect the media message has on individuals' attitudes, depends on whether the individuals' lived experiences either confirms or dismisses the message in the company. The

less knowledge the individual has the more likely it is that they accept the message, and this shapes the attitude on the subject. For example, the data indicates that Red CEO had little knowledge about China as a threat actor for espionage, but the informant said that he had heard about it in the media. According to Happer & Philo (2013) this informant is more likely to accept the message of China as a threat because SMB Red have little knowledge about the topic, and they had not experienced industrial espionage. However, they had very clear knowledge that IPR is regarded differently in China than in Norway and other countries. This way their experience would increase the likeliness of accepting the message, because it confirms their experience. For the informant in SMB Orange, who was educated in Asian studies, and well-read in international newspapers, the media coverage in the Norwegian news about Chinese espionage would likely confirm what she/he already knows from other sources, and she/he would likely also accept the message.

SMB Yellow China contact (2019) mentioned how the "Sandberg case" (former minister travelled to Iran with his government work phone) influenced them to discuss the topic of using "barrowing phones" on travels to China, and they even implemented the use of these phones. Following Happer & Philo (2013) theory the media message that included the topic "use of barrowing phone is smart" was accepted by SMB Yellow, and it influenced their attitudes and even changed their behavior. At the time of the scandal, the Sandberg case reoccurred often in the news. According to Happer and Philo (2013), when a message is repeated several times, it increases the likelihood of shaping attitudes. SMB Yellow's experience with industrial espionage inn China might also be considered a lived experience that would increase their perception of the media message as it being true. The challenges the SMBs have met with a lack of alignment with IPR in China revealed that these experiences informed their understanding and knowledge about Chinese culture around IPR, and also about the Chinese political economy in which the state and/or CCP is involved in alle companies and in all final decisions.

This section has applied Happer & Philo's (2013) theory about how media can shape attitude and influence behavior. It helps to explain how media can be regarded as an influential factor to a company's security culture because media messages can shape attitudes and behavior regarding protection of information.

7.3 State Information Sharing

The data from the interviews found that the sample does not have significant contact with any governmental body, except form SMB Orange who said they received very good support from Innovation Norway (Innovasjon Norge). None of the informants, except SMB Green IT Director of Technology who was open to receive specific technical information, saw the need for information from the state. The intelligence community's main information to Norwegian private and public enterprises are the threat assessments, and these documents have provided information specifically to this audience. Only one of the informants had read this (SMB Orange), but she/he found it irrelevant because it contained the same information as she/he read in international news, and the technical updates she/he received from their technical employees. This finding supports the findings in NSR's reports that only 20% of the enterprises read PST's threat assessment (Næringslivets sikkerhetsråd & Opinion, 2015, p. 5; 2017, p. 6, 16; Næringslivets sikkerhetsråd, 2021, p. 6). This indicates that the intelligence community has a challenge with outreach to the private business sector. The annual threat assessments PST and NIS publishes can be seen as examples of Petersen's (2019) concept of communication as advice. The threat assessments are openly available for the public online. According to the concept of communication as advice the intelligence community trusts the public to find and use the information (Petersen, 2019). If the intelligence community really wants the private business community to understand their role in national security, it must improve its communication methods to actually reach the private business community. The intelligence community is concerned that China can use soft technology from Norwegian companies to develop military technology (Norwegian Intelligence Service, 2020: 65; The Norwegian Police Security Service, 2024, p. 13). This means that civilian technology like SMB Orange environmental technology, and SMB Red's health technology can be used to develop military technology. If the state intelligence community really believes that they need the private business sector to increase national security, then it needs to improve their information sharing, and also possibly the content of the threat assessments. Although the thesis' findings cannot be generalized, the findings, supported by Happer & Philo (2013), indicates that media can be useful as a strategic tool for governments to inform the public and to shape opinions and influence to change behavior about topic of choice.

7.3.1 The Content of the Threat Assessments

SMB Orange did not find what was written in the threat assessments as relevant. Gjesvik (2019, p. 32) and Thorsrud (2021) find that the intelligence community is reluctant to share intelligence with the public. Næringslivets Hovedorganisasjon (2019), Abelia (2018) and NOU 2015: 13 has also called for more relevant information from the state. A central question is why the intelligence community does not share more relevant information with the business community? The intelligence services balance the need for information in the public against the risk of risking national security Petersen (2019). This statement is common in the concept of communication as awareness (Petersen 2019) – in which the intelligence reports defend why the intelligence services must be secretive. Is it possible for intelligence services to share more without compromising national security? In his thesis, Thorsrud (2021) found that the police business contacts disagreed with the police intelligence officers' decisions of keeping information "exempt from public disclosure". Perhaps the strong tradition of keeping secrets reflects also other agencies in intelligence community, like PST, and NSM.

The sample regards having a Chinese person involved in the company essential to being successful in China. As presented in the introduction, PST (2019, p. 12) is concerned about the risk that foreign states that Norway does not have security cooperation through ownership and investments can get access to technology that is of strategic importance. PST (2024, p. 13) claims that China uses non-military technology and knowledge to develop its military technology. As such the technology in some of the SMBs in the sample could be used to further develop military technology. This information is openly available in the threat assessments, and potentially could increase awareness among the SMBs in the sample. But the SMBs I the sample do not read these. According to the findings in NSR's reports this is true for 80% of private and public enterprises (Næringslivets sikkerhetsråd & Opinion, 2015, p. 5; 2017, p. 6, 16; Næringslivets sikkerhetsråd, 2021, p. 6).

The knowledge in the companies could have been better if the relevant information from the intelligence community reached the businesses and if the information is relevant in their everyday work and business relations with China. The espionage threat and disrespect for IPR in China is consistent, and China continues to be an important for Norwegian trade. As such the companies could use information about how to deal with the threat whilst continuing doing business. Specific and relevant information from the intelligence community could increase knowledge in the companies. Combined with the attitudes the sample has from their

experiences it could strengthen the ways in which they protect their economic information in their Norwegian-Chinese business relations.

8 Conclusion

The analysis revealed that media is an important source of information about economic and industrial espionage. Further it was revealed that the state does not reach the private business sector with their open threat assessments. The knowledge the SMBs have about espionage came from media, ICT suppliers and experiences. The challenges they have met with a lack of alignment with IPR revealed that experiences informed their understanding and knowledge about Chinese culture around IPR, and also about the Chinese political economy in which the state and/or CCP is involved in alle companies and in all final decisions.

Using Van Niekerk and Von Solms (2006) framework for information security culture the analysis and discussion explained how knowledge, attitudes and behavior are interconnected. Having or lacking relevant knowledge about securing economic information, and about how IPR is handled in a foreign business country affects can influence behavior. Happer and Philo (2013) theory helped explain the finding of the importance of media to security culture. By applying this theory, the discussion demonstrated how media can be a source of knowledge, and how it can change attitudes and influence a change in behavior. This discussion also included the importance of lived experience in the shaping of attitudes. The analysis and discussion find that the state intelligence community has a challenge with its outreach of information to the public. Only one of the six informants in the sample had read threat assessments. Næringslivets Hovedorganisasjon (2019), Abelia (2018) and NOU 2015: 13 find that such assistance in essential for the private business sector to contribute to national security through their everyday work, but the sample does not see the need for information from the state security services. Also, only one of the SMBs saw espionage as a direct threat to them. The other companies seemed to differentiate between “to steel” information and espionage.

The analysis found that media and experiences are influential factors to security culture in the way that the sample gained relevant knowledge that they could use in their everyday lives to protect their economic information in Chinese business relations. For one of the SMBs (Yellow) media coverage even influenced changed behavior when they decided to try out using “borrowing phones” instead of the cell phones they used every day.

The analysis demonstrated that the dimension of state assistance is recognized by the intelligence community which does not reach the private business community with their threat assessments, which are their main information to the public. The data from this thesis and previous research indicates that NSM, PST and NIS must find better ways to communicate the important information in a way that reaches the business community, especially SMBs. It is not enough that there are open treat assessments and relevant reports available on the Internet if the business community does not know about it, or do not find the information relevant for them in their everyday lives. China will continue to be an important market for Norwegian businesses, and the espionage threat will not disappear. Norwegian SMBs need guidance for how they should navigate in this environment.

8.1 Suggestion for Further Research

I experienced that much of the literature on security culture is related to technical information about information security and cyber security. With my background from social science, I experienced that my understandings of that field were limited. Like Malmedal and Røislien (2016), I believe that collaborations between IT and social sciences in security studies would complement each other's knowledge gaps and create valuable new knowledge about security culture in both academic fields.

Bibliography

Abelia. (2018). *Høringssvar fra Abelia 01.10.2018. Forskrifter til ny sikkerhetslov.* Answer to hearing: Abelia. Available at: https://www.regjeringen.no/no/dokumenter/horing---forskrifter-til-ny-sikkerhetslov/id2606681/?uid=e634e1c1-acae-483c-8184-a7e2a4a19baf (accessed: September 16, 2019).

Abelia. (2019). *Interview with representative from Abelia* (November 11, 2019).

Adler, E. & Barnett, M. (1998). Security communities in theoretical perspective. In Adler, E. & Barnett, M. (eds) *Security Communities*, pp. 3-28. Cambridge: Cambridge University Press.

Ben-Asher, N. & Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. *Computers in human behavior*, 48: 51-61. doi: 10.1016/j.chb.2015.01.039.

Berg, B. L. & Lune, H. (2012). *Qualitative research Methods for the Social Sciences*. 8th ed. USA: Pearson Education Limited.

Bergløff, **C. B.** (2019). Kinas ambassade kaller PST-rapport «latterlig». Available at: https://www.nrk.no/urix/kinas-ambassade-kaller-pst-rapport-_latterlig_-1.14415139.

Bergsjø, H., Windvik, R. & Øverlier, L. (2020). *Digital sikkerhet : en innføring*. Oslo: Universitetsforlaget.

Blomberg, H., Head of Counter Intelligence in PST. (2020). *Slik jobber spioner i Norge*. Zaman, K. (ed.). Norge bak fasaden. https://www.tv2.no/a/11129077/: TV2.

Brander, J. A., Cui, V. & Vertinsky, I. (2017). China and intellectual property rights: A challenge to the rule of law. *Journal of international business studies*, 48 (7): 908-921. doi: 10.1057/s41267-017-0087-7.

Brødsgaard, K. E. (2015). China's 13th Five-Year Plan: A Draft Proposal. ***The Copenhagen Journal of Asian Studies***, 33 (2): 97-195. doi: 0.22439/cjas.v33i2.4968.

Brønnøysundregistrene. (2017). *Nøkkelopplysninger fra Enhetsregisteret*. Available at: https://w2.brreg.no/enhet/sok/index.jsp.

Bryman, A. (2012). *Social Research Methods*. 4 ed. New York: Oxford University Press.

Bye Skille, Ø. (2019). *Tvil om hvem som står bak dataangrepet mot Visma*: Norsk rikskringkasting. Available at: https://www.nrk.no/norge/tvil-om-hvem-som-star-bak-visma-hackingen-1.14420262 (accessed: Feb. 8, 2019).

China Law Translate. (2017). *National Intelligence Law of the P.R.C. (2017)*. Available at: https://www.chinalawtranslate.com/en/中华人民共和国国家情报法/ (accessed: 04.01.19).

da Veiga, A., Astakhova, L. V., Botha, A. & Herselman, M. (2020). Defining organisational information security culture - Perspectives from academia and industry (draft version). *Computers & Security*, 92: 101713–101723. Available at: https://repository.up.ac.za/bitstream/handle/2263/76240/DaVeiga_Defining_20

20.pdf;jsessionid=8F78C9B9A72CDF954081697F9F765F88?sequence=1. doi: 10.1016/j.cose.2020.101713 (accessed: February 16, 2024).
Eriksen Søreide, I. (2020). *The China Challenge. Remaking the Landscape of Transatlantic Security*. Norwegian Ministry of Foreign Affairs (ed.). https://www.regjeringen.no/no/aktuelt/kina_utfordring/id2688732/.
Etteretningstjenesten. (2017). *FOKUS 2017*.
Finnemore, M. & Sikkink, K. (1998). International norm dynamics and political change. *International Organization*, 52 (4): 887-917.
Gåsemyr, H. J. (2019). A Norwegian perspective on Nordic-China Cooperation. In Forsby, A. B. (ed.) *Nordic–China Cooperation: Challenges and Opportunities*: NIAS Press. Available at: https://www.nupi.no/Publikasjoner/CRIStin-Pub/A-Norwegian-perspective-on-Nordic-China-Cooperation. doi: 978-87-7694-277-5 (accessed: January 3, 2020).
Gerring, J. (2007). *Case Study Research. Principles and Practices.* New York, USA: Cambridge University Press.
Gjesvik, L. (2019). *Comparing Cyber Security. Critical Infrastructure protection in Norway, the UK and Finland*. NUPI Report.
Glesne, C. (2006). *Becoming Qualitative Researchers: An Introduction*. 3 ed. Boston: Pearson/Ally & Bacon.
Government.no. (n.y.). *Official Norwegian Reports*. Available at: https://www.regjeringen.no/en/find-document/norwegian-official-reports/id1767/ (accessed: January 7, 2020).
Grabiszewski, K. & Minor, D. (2019). Economic Espionage. *Defence and Peace Economics*, 30 (3): 269-277. doi: 10.1080/10242694.2018.1477400.
Halsør, M., Bye Skille, Ø., Vestrum Olsson, S., Vartdal, Å. & Døvik, O. (2019). *Granskarar: Kina hacka norsk selskap*. Urix: Norsk rikskringkasting. Available at: https://www.nrk.no/urix/granskarar_-kina-hacka-norsk-selskap-1.14418026 (accessed: Feb 6, 2019).
Hamidi, S. & Gaard, A. (2023). *Information Security Assessment of the Norwegian SMB-Sector: A Study of Culture, Leadership and Cost*. Master Thesis. Stavanger: University of Stavanger. Available at: https://uis.brage.unit.no/uis-xmlui/handle/11250/3089882 (accessed: February, 15, 2024).
Happer, C. & Philo, G. (2013). The Role of the Media in the Construction of Public Belief and Social Change. *Journal of social and political psychology*, 1 (1): 321-336. doi: 10.5964/jspp.v1i1.96.
Haugom, L. (2019). *Etterretningsanalyse i den digitale tid*: Norwegian Institute of International Affairs.
Hella, I. (2022). *En studie av en digital sikkerhetskultur i en organisasjon*. Stavanger: University of Stavanger. Available at: https://hdl.handle.net/11250/3024573 (accessed: February 4, 2024).
Heng, L. (2018). *«We're both surprised and confused by their irresponsible and baseless accusation»*. Available at: https://www.universitetsavisa.no/utenriks/were-both-surprised-and-confused-by-their-irresponsible-and-baseless-accusation/142156.

Jackson, P. T. (2010). *The conduct of inquiry in international relations: philosophy of science and its implications for the study of world politics.* New York Routledge.
Jacobsen, D. I. (2005). *Hvordan gjennomføre undersøkelser? : innføring i samfunnsvitenskapelig metode*. 2 ed. Kristiansand: Høyskoleforlaget.
Johannessen, L. E. F., Rafoss, T. W. & Rasmussen, E. B. (2018). *Hvordan bruke teori? : nyttige verktøy i kvalitativ analyse*. Oslo: Universitetsforl.
Jorem, M. (2019). Business and entrepreneurship. In Forsby, A. B. (ed.) *Nordic–China Cooperation: Challenges and Opportunities*: NIAS Press. Available at: https://www.nupi.no/Publikasjoner/CRIStin-Pub/A-Norwegian-perspective-on-Nordic-China-Cooperation. doi: 978-87-7694-277-5 (accessed: January 3, 2020).
Katzenstein, P. J. (1996). Introduction: Alternative Perspectives on National Security. In Katzenstein, P. J. (ed.) *The Culture of National Security: Norms and Identity in World Politics*, pp. 1-32. New York: Columbia University Press.
Kibar, O. (2017). Slår alarm om næringslivets Kina-tur. ***Dagens Næringsliv***. Available at: https://www.dn.no/nyheter/2017/05/21/1957/Handel/slar-alarm-om-naeringslivets-kina-tur? (accessed: 06.12.2017).
Kibar, O. (2024). Tidligere PST-topp: - Næringslivet mangler verktøy for å håndtere Kina-trusselen. *Dagens Næringsliv*. Available at: https://www.dn.no/politikk/tidligere-pst-topp-naringslivet-mangler-verktoy-for-a-handtere-kina-trusselen/2-1-1617159 (accessed: March 27, 2024).
Lam, N. M. & Graham, J. L. (2007). *China Now*. United States: McGraw-Hill.
Lantis, J. S. (2002). Strategic Culture and National Security Policy. *International Studies Review*, 4 (3): 87-113. doi: 10.1111/1521-9488.t01-1-00266.
Li, S. & Alon, I. (2020). China's intellectual property rights provocation: A political economy view. *Journal of International Business Policy*, 3 (1): 60-72. doi: 10.1057/s42214-019-00032-x.
Lindvoll, E. (2017). NHO opplever massivt Kina-trøkk. *E24*. Available at: http://e24.no/naeringsliv/nho/nho-opplever-massivt-kina-troekk/23983176 (accessed: 08.09.2017).
Lowenthal, M. (2014). *Intelligence. From Secrects to Policy.* . 6 ed. US: CQ Press.
Malmedal, B. & Røislien, H. E. (2016). *The Norwegian Cyber Security Culture*: Norwegian Centre for Information Security (NorSIS). Available at: https://norsis.no/publikasjoner/ (accessed: August 3, 2017).
Mattis, P. (2015). *A Guide to Chinese Intelligence Operations," War on the Rocks*: War on the Rocks. Available at: https://warontherocks.com/2015/08/a-guide-to-chinese-intelligence-operations/ (accessed: October, 14, 2017).
Mattis, P. (2017). *Everything We Know about China's Secretive State Security Bureau*. The National Interest. Available at: https://nationalinterest.org/feature/everything-we-know-about-chinas-secretive-state-security-21459 (accessed: Sept. 13, 2019).
Mattis, P. & Hoffman, S. (2017). *Chinese legislation points to new intelligence co-ordinating system*. Jane's Intelligence Review: IHS Markit. Available at: https://www.janes.com/images/assets/183/74183/Chinese_legislation_points_to_new_intelligence_co-ordinating_system.pdf (accessed: Sept 13, 2019).

Mesna, M. (2024). *Da Visma ble rammet av cyberangrep*. Available at: https://www.vismasoftware.no/artikler/da-visma-ble-rammet-av-cyberangrep (accessed: March, 15, 2024).
Ministry of Education and Research. (2017). *Increased science cooperation with China*. Press Release No: 125 - 2017. Available at: https://www.regjeringen.no/en/aktuelt/increased-science-cooperation-with-china/id2568845/ (accessed: September 4, 2017).
Moe, M. & Lillevik, E. (2012). Digital spionasje – En trussel for verdiskapingen i Norge. *Praktisk økonomi & finans*, 28 (2): 27-35. doi: 10.18261/ISSN1504-2871-2012-02-05.
N. Mark Lam & John L. Graham. (2007). *China Now*. United States: McGraw-Hill.
Næringslivets Hovedorganisasjon. (2019). Ni forslag til økt digital sikkerhet for bedriftene. Available at: https://www.nhobyggenaringen.no/arkiv-over-artikler/2019/ni-forslag-til-digital-sikkerhet/ (accessed: 01.07.19).
Næringslivets Hovedorganisasjon. (2024). *Tall og fakta om SMB*. Available at: https://www.nho.no/tema/sma-og-mellomstore-bedrifter/tall-og-fakta-om-smb/ (accessed: March 28, 2024).
Næringslivets sikkerhetsråd & Opinion. (2015). *Kriminalitets- og sikkerhetsundersøkelsen i Norge 2015*. KRISINO. Available at: https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/krisino (accessed: June 22, 2017).
Næringslivets sikkerhetsråd. (2016). *Mørketallsundersøkelsen*. Available at: https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/morketallsundersokelsen (accessed: June 22, 2017).
Næringslivets sikkerhetsråd & Opinion. (2017). *KRISINO 2017*. Kriminalitets- og sikkerhetsundersøkelsen i Norge. Available at: https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/krisino (accessed: June 22, 2017).
Næringslivets sikkerhetsråd. (2021). *KRISINO 2021*. Kriminalitets- og sikkerhetsundersøkelsen i Norge. Available at: https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/krisino (accessed: April 25, 2024).
Næringslivets sikkerhetsråd. (2024). *Strategi 2024-2027*. Available at: https://www.nsr-org.no/produkter-og-tjenester/publikasjoner/rapporter-og-veiledere (accessed: April 25, 2024).
Nasheri, H. (2005). *Economic Espionage and Industrial Spying*. Cambridge, UK: Cambridge University Press. Available at: http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=129304&site=ehost-live (accessed: Aug 22, 2019).
Nasjonal sikkerhetmyndighet. (2024). *RISIKO*: Nasjonal sikkerhetmyndighet,. Available at: https://nsm.no/getfile.php/1313477-1707733210/NSM/Filer/Dokumenter/Rapporter/Risiko%202024.pdf (accessed: April 4, 2024).
Nasjonal sikkerhetmyndighet. (s.a.). *Sikkerhetskultur*. Available at: https://nsm.no/fagomrader/sikkerhetsstyring/sikkerhetskultur/ (accessed: January 4, 2024).

NHO. (2018). *Fakta om små og mellomstore bedrifter (SMB)*. Available at: https://www.nho.no/tema/sma-og-mellomstore-bedrifter/artikler/sma-og-mellomstore-bedrifter-smb/ (accessed: 06.12.18).

Nölke, A. (2014). Private Chinese Multinationals and the Long Shadow of the State. In Nölke, A. (ed.) International Political Economy Series, *Multinational Corporations from Emerging Markets : State Capitalism 3.0*, pp. 77-89. London: Palgrave Macmillan UK : Imprint: Palgrave Macmillan.

Norwegian Intelligence Service. (2020). *Focus 2020*. Focus: Norwegian Intelligence Service. Available at: https://www.etterretningstjenesten.no/publikasjoner/fokus/focus-english/Focus%202020%20english.pdf/_/attachment/inline/6d9bcff6-48f1-423e-b13e-036d6ad4556a:d282e733ce4f5697c9e4a7afc5a63c16dab6c151/Focus%202020%20english.pdf (accessed: January 4, 2024).

Norwegian Intelligence Service. (2022). *Focus 2022. The Norwegian Intelligence Service's assessment of current security challenges*: Norwegian Intelligence Service,. Available at: https://www.etterretningstjenesten.no/publikasjoner/fokus/focus-english/Focus2022.pdf/_/attachment/inline/da948a6e-a831-492c-8a70-f52ee75cf164:df10b1758adb85a99d3a370081ef8222dd947b07/Focus2022.pdf (accessed: February 24, 2024).

NOU 2015: 13. *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*. Available at: https://www.regjeringen.no/no/dokumenter/nou-2015-13/id2464370/ (accessed: March 25, 2018).

NOU 2016: 19. (2016). *Samhandling for sikkerhet*. Available at: https://www.regjeringen.no/no/dokumenter/nou-2016-19/id2515424/ (accessed: August 3, 2017).

NOU 2023: 28. *Investeringskontroll — En åpen økonomi i usikre tider*. Available at: https://www.regjeringen.no/no/dokumenter/nou-2023-28/id3016161/ (accessed: January 4, 2024).

Oksholen, T. (2018). *Akademisk frihet i Kina: Ny lov forbyr «krenking av martyrer»*. Universitetsavisa. Available at: https://www.uniforum.uio.no/nyheter/2018/05/akademisk-frihet-i-kina.html.

Petersen, K. L. (2011). Risk analysis - A field wihin security studies? *European Journal of International Relations*, 18 (4): 693–717. doi: 10.1177/1354066111409770.

Petersen, K. L. (2019). Three concepts of intelligence communication: awareness, advice or co-production? *Intelligence and national security*, 34 (3): 317-328. doi: 10.1080/02684527.2019.1553371.

Politiets sikkerhetstjeneste. (2020). *Trusselvurdering 2020*. Available at: https://www.pst.no/alle-artikler/trusselvurderinger/nasjonal-trusselvurdering-2020/ (accessed: February 17, 2020).

Potter, E. H. & Centre for Trade Policy and Law. (1998). *Economic Intelligence and National Security*. Ottawa: MQUP. Available at:

http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=625424&site=ehost-live (accessed: October 18, 2019).
Regjeringen.no. (2023). *Investeringskontrollutvalget*. Available at: https://www.regjeringen.no/no/dep/nfd/org/etater-og-virksomheter-under-narings--og-fiskeridepartementet/styrer-rad-og-utvalg/midlertidige-styrer-rad-og-utvalg/investeringskontrollutvalget/id2942014/ (accessed: January 4, 2024).
Regnskapstall 1881 AS. (2017). *Regnskapstall.no*. In Ohr, A. (ed.). Digitale Medier 1881 AS Kistefoss AS. Available at: https://www.regnskapstall.no.
Rocha Flores, W., Antonsen, E. & Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & security*, 43: 90-110. doi: 10.1016/j.cose.2014.03.004.
Roer, K. (2017). Sikkerhetskultur og måling trenger ikke være så vanskelig. *Computer World*. Available at: http://www.cw.no/artikkel/kronikk/kronikk-sikkerhetskultur-maling-trenger-ikke-vaere-sa-vanskelig (accessed: 10.02.18).
Roer, K. & Petric, G. (2017). *Indepth insights into the human factor: The 2017 Security Culture Report*: CLTRe North America, Inc. Available at: https://www.researchgate.net/publication/316715557_Deep_insights_into_the_human_factor_-_the_security_culture_report_2017 (accessed: August 4, 2017).
Schein, E. H. (1992). *Organisational Culture and Leadership: A Dynamic View*. San Francisco, CA: Jossey-Bass.
Shuang, G. (2019). *Foreign Ministry Spokesperson Geng Shuang's Regular Press Conference on February 18, 2019*: Embassy of the People's republic of China in the Republic of the Philippines. Available at: http://ph.china-embassy.org/eng/fyrth/t1638791.htm (accessed: 02.18.2019).
Sikkerhetsloven. (2018). *Lov 6. juni 2018 nr. 24 om nasjonal sikkerhet*. In beredskapsdepartementet, J.-o. (ed.). LOV-2018-06-01-24. Available at: https://lovdata.no/lov/2018-06-01-24 (accessed: January 18, 2019).
Sjølstad, T., Høie, T. A., Gulbrandsen, R. & Daler, T. (2010). *Håndbok i datasikkerhet : informasjonsteknologi og risikostyring*. 3. utg. ed. Trondheim: Tapir akademisk.
SMB Green IT Director of Technology. (2019). *Interview by Skype with IT Director of Technology in SMB Green,* (March 2019).
SMB Green Leader. (2019). *Interview by Skype with leader in SMB Green,* (March 31, 2019).
SMB Orange China contact. (2017). *Interview with China contact in SMB Orange* (2017).
SMB Red CEO. (2017). *Interview with CEO in SMB Red* (November 2017).
SMB Red IT Director. (2019). *Interview by phone with IT Director in SMB Red* (February 2019).
SMB Yellow China contact. (2019). *Interview by phone with China contact SMB Yellow* (February 2019).
Smith, I. C. & West, N., Mmnmmauthor,. (2012). *Historical dictionary of Chinese intelligence*: Lanham [Md.]: Scarecrow Press. Available at: http://web.b.ebscohost.com/ehost/detail/detail?nobk=y&vid=3&sid=c23ba678-dd74-496c-8ea9-

cbeffec1bbf0@sessionmgr103&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ==#AN=463901&db=nlebk (accessed: August 27, 2019).
Søilen, K. S. (2016). Economic and industrial espionage at the start of the 21st century – Status quaestionis. *Journal of Intelligence Studies in Business*, 6 (3): 51-65. doi: 10.37380/JISIB.V6I3.196.
Strand, S. S. (2023). *An investigation into cyber security risk mitigation and the human factor in developing a cyber security culture. A comparative analysis of two maritime companies in Norway.* Master Thesis. Faculty of Technology, Natural Sciences and Maritime Sciences: University of South-Eastern Norway. Available at: https://hdl.handle.net/11250/3076275 (accessed: March 1, 2024).
The Linux Information Project. (2004). *Source Code Definition*: The Linux Information Project. Available at: http://www.linfo.org/source_code.html (accessed: February 16, 2020).
The Norwegian Intelligence Service. (2017). *Focus 2017. The Norwegian Intelligence Service's assessment of current security challenges*. Available at: https://www.etterretningstjenesten.no/publikasjoner/fokus/focus-english/Fokus%202017%20english.pdf/_/attachment/inline/ff8c43ea-5d89-4504-8438-0a643557c23f:6fd3d3056a6ee63cfe521ab912e7736db91203f2/Fokus%202017%20english.pdf (accessed: September 25, 2017).
The Norwegian Intelligence Service. (2019). *Fokus. The Norwegian Intelligence Service's assessment of current security challenges.* Available at: forsvaret.no/fokus.
The Norwegian National Security Authority. (s.a.). *Sikkerhetskultur*. Available at: https://nsm.no/fagomrader/sikkerhetsstyring/sikkerhetskultur/ (accessed: January 4, 2024).
The Norwegian Police Security Service. (2017). *Annual Threat Assessment 2017*. Oslo, Norway. Available at: https://www.pst.no/alle-artikler/?v=1615541701893&FilterByValues=2&PageNumber=2 (accessed: December 12, 2017).
The Norwegian Police Security Service. (2018). *Threat Assessment 2018*. Oslo, Norway. Available at: https://www.pst.no/alle-artikler/?v=1615541701893&FilterByValues=2&PageNumber=2 (accessed: December 20, 2018).
The Norwegian Police Security Service. (2019). *Threat Assessment 2019*. National Threat Assessments. Oslo, Norway. Available at: https://www.pst.no/alle-artikler/?v=1615541701893&FilterByValues=2&PageNumber=2 (accessed: August 10, 2019).
The Norwegian Police Security Service. (2024). *National Threat Assessment 2024*. Available at: https://www.pst.no/globalassets/2024/ntv2024/nasjonal-trusselvurdering-2024_engelsk_web_.pdf (accessed: February 12, 2024).
Thorleuchter, D. & Van den Poel, D. (2013). Protecting research and technology from espionage. *Expert Systems with Applications*, 40: 3432–3440. doi: 10.1016/j.eswa.2012.12.051.
Thorsrud, E. B. (2021). *I hvilken grad opplever politiets næringslivskontakter begrensninger når det kommer til informasjonsdeling til eksterne aktører?*

Master Thesis. Oslo: Politihøyskolen. Available at: https://hdl.handle.net/11250/2827103 (accessed: Macrh 15, 2024).
United Nations. (1948). *Universal Declaration of Human Rights*. Paris: United Nations.
Van Niekerk, J. & Von Solms, R. (2006). *Understanding information security culture: a conceptual framework.* In Proceedings of: Information Security South Africa (ISSA2006), 1-9. South Africa. Available at: https://d1wqtxts1xzle7.cloudfront.net/37961810/21_Paper-libre.pdf?1434914548=&response-content-disposition=inline%3B+filename%3DUnderstanding_information_security_cultu.pdf&Expires=1715434279&Signature=H9knGTzBa~HeNuaskxXSbu26J-iXJ9B-pZagymPGoHbvaRgJ3WqJgmKHNnA5qNox8XNYTScVzXnGXaSBAPczRPj64jmJvntuCaY95lk-gXC3GR36tXUSXnGBhJeHGpZo7FXumpDdwQqZ8dat0~E1sOhA6kiNWW8PCTLplHt1zHgIX-o8q5UZh9tNp0ImC2FxvD7txG7xKT0T5bvll-qGd5C2oH5x2PD~Y5wHIAmCvV~ayOxlpaaTBXnJfer9VIAajM0D6EGEq17SNwL6LdtpPeieQb8KpvlCI~JuUO1X2t648AAxeUEtukLHjBjQhi3L98mrYSIoNWEfwdlaoUU08g__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA (accessed: April 16, 2024).
von Solms, R. & van Niekerk, J. (2013). From information security to cyber security. *Computers & security*, 38: 97-102. doi: 10.1016/j.cose.2013.04.004.
Whitney, M. E. & Gaisford, J. D. (1996). Economic Espionage as Strategic Trade Policy. *The Canadian Journal of Economics / Revue canadienne d'Economique*, 29 (Special Issue: Part 2 (Apr., 1996)): 627-632. doi: 10.2307/136121.
World Intellectual Property Organization. (2019). *What is a Trade Secret?* Available at: https://www.wipo.int/tradesecrets/en/ (accessed: Aug. 19, 2019).
Yin, P. (2015). Mapping Out Success New five-year blueprint lays down specific objectives for a prosperous China. *Beijing Review*, 58 (45): 12-17. Available at: http://www.bjreview.com/Nation/201511/t20151102_800041666.html (accessed: 11.08.17).
Yin, R. (2018). *Case Study Research and Applications: Design and Methods*. 6 ed. Los Angeles, USA: Sage.

Appendix 1

Intervjuguide SMBs

Intro:
Lette, høflige spørsmål for å få informanten til å slappe av. F.eks:

- Når startet dere bedriften? Har du vært med fra starten?
- Hvor fikk dere ideen om selskapets produkter fra?
- Anser du dere som et globalt selskap?
- Hva kan dere tilby verden som den trenger?
- Teknologien deres – utvikler dere den selv?
- Dere har mange samarbeidspartnere – hva går disse samarbeidene ut på? (Deler dere deres teknologiprodukter?)
- Hvor mange ansatte har dere?

Sikkerhet
Objective: å få innsikt i hvordan de oppfatter sikkerhet, og hva som gjelder dem

- Hva legger du i begrepet sikkerhet for deres bedrift?
- Hvem har ansvaret for bedriftens sikkerhet?
    - Har dere en egen sikkerhetsansvarlig?
    - (føler dere et felles eierskap til sikkerhet?)
- Hvordan deles sikkerhetsinformasjon i bedriften? (På hvilken måte? (er det IT-personen som gir noen retningslinjer,) hva slags info er det som deles? ”Husk sikkert passord”.
- Synes du sikkerhet en integrert del av hverdagen din?
    - Hvordan/hvordan ikke?
- Ser du noen trusler for deres bedrift?
    - Har dere definert noen trusler?
- Har dere noe dere anser som sensitiv informasjon (info som kan skade dere på noen måte - økonomisk, omdømme) i deres bedrift? (ja/nei spørsmål – vil ikke ha info om hva)
    - Hvordan beskytter dere teknologien deres? Har dere noen tiltak eller retningslinjer som skal beskytte teknologen og verdiene deres?
    - Har dere patent på deres teknologi? I Norge, i EU, globalt? (sjekk nettsidene til hver enkelt bedrift) kina – da de hadde noe å gjøre med dem?

- Vet du hva risikovurdering er? Foretar dere interne risikovurderinger?
(kartlegge interne verdier/teknologi, sårbarheter og trusler knyttet til dette og hvordan det kan sikres)
- Er dette noe alle deltar på?
    - Hvi ja: Hvordan inkluderes alle/flere? (Blir alle informert eller er det sikkerhetsansvarlig sitt område?)
    - Hvis nei: hvem da? Hvorfor ikke flere?
- Har dere noen sårbarheter?
    - Har dere en plan for hvordan dere kan beskytte dere?
- Hva er deres største utfordring sikkerhetsmessig?

- Har dere retningslinjer/regler for sikkerhetstiltak under jobbreiser?
    - Er det ulike regler for ulike land?
- Gjennomfører dere interne risikodiskusjoner/vurdering knyttet til kunder og handelspartnere?

Ansatte

- Alle norske statsborgere?
- Har dere taushetsplikt i bedriften? Har dere klausuler i avtalen med de ansette om konfidensialitet om i.e. teknologiutvikling.
- Er ansatte underlagt taushetsplikt om teknologier dere utvikler og produkter dere holder på å utvikle?
- Er det noen karantene for tidligere ansatte før de kan jobbe i hos en konkurrent.
- Hvordan sikrere dere teknologi/verdi når dere ansetter nye folk? (bakgrunnssjekk)
- Kontoer i andre land – bakgrunnssjekk der også?

Investorer:

- Har dere kinesiske investorer?
- Et det statlig eller privat selskap/person?
- Hva går denne avtalen ut på?
- Inngår rettigheter, innsyn til produksjon, teknologi etc.?
- Har dere investorer fra andre land?

Partnere:

- Hva går partnerskapene ut på?
- Får de tilgang til sensitiv info? F.eks. teknologi/hvordan produktet er laget?
- Plan for å sikre sensitiv info?

Hacking

- Hvordan forholder dere dere til hacking? (ser de på det som en trussel, har de rutiner)
- Har dere hørt om noen norske bedrifter som har blitt hacket og mistet verdier/blue prints? (i.e. Ulsteinvik gruppen som gikk ut offentlig)
- Har dere retningslinjer/regler for bruk av PC på ubeskyttede nett? (i.e. for å komme på intern server så må du være på et sikkert nett med brukernavn og passord.)
    - Hvorfor/hvorfor ikke?

Om de selv aktivt oppsøker instanser, info, arrangementer for å sikre egen bedrift, og/eller å lære

Objective: To get an idea of how conscious they are of security issues that is relevant for them.

- Hvordan tilegner dere kunnskap om sikkerhetstrusler?
    - Pleier du/dere å lese og orientere dere sikkerhetsmessig ut ifra PST, etterretningstjenesten, Nasjonal Sikkerhetsmyndighet sine rapporter/trusselvurderinger?
    - Hvem er det sitt ansvar? Hvem er det som evt. leser dette?
    - Er det noe dere har behov for? Hvorfor/hvorfor ikke? Hvorfor gjøres det ikke?
- Sikkerhetstiltak: hvordan skaffer dere info og kunnskap om mulige sikkerhetstiltak?

    - Hvorfor gjør dere det ikke?
    - Hvis ja: hvem i bedriften?
- Er dere med i noe forum eller organisasjon for bedrifter?
    - Tas sikkerhet opp som tema her?
        - Hvis nei: hvorfor tror du det er slik.
        - Hvis ja: Hvilke sikkerhetstemaer da?
    - Hvem, hvilken stilling i bedriften, i deres bedrift deltar på disse typer arrangementer/forum?
- Pleier dere å delta på sikkerhetsrelaterte arrangementer? (frokostseminarer etc.)
    - Hvis ja: Har dere deltatt på noen sikkerhetsrelaterte arrangementer i år?
    - Hvis nei: hvorfor ikke?
    - Hvem er det som deltar? IT/person eller sikkerhetsansvarlig?
- Har du hørt om Sikkerhetsmåneden? Vet du hvem som arrangerer den? (Nasj sikkerhetsmyndighet og NorSis. Kampanje for å øke kunnskap om digital infosikkerhet. Både offentlig og privat sektor.)

Kina – kunnskap om kultur, guanxi, politikk, styresett

- Er det kun du som har kontakt med de kinesiske handelspartnerne/kundene?
- Snakker du kinesisk/mandarin?
- Har du eller andre studert asiatiske kulturstudier eller lignende? Hva gjorde deg interessert i Asia?
- Hva synes du kjennetegner kinesisk kultur generelt? Og spesielt? (i.e. basert på dine opplevelser)
- Hva synes du kjennetegner kinesisk handelskultur?
- Hva vet du om det kinesiske styresettet?
- Hva vet om utfordringer Kina har?
- Vet du hva kineserne er interessert i av teknologi?

Tillitt

Objective: to get an idea of the general level of trust among the companies.

- Hva går deres forhold til Kina ut på?
- Hvilke produkter er det dere selger til deres kinesiske handelspartnere?
- Hvor mange kinesiske bedrifter eller selskaper har dere kontakt med?
- Hvor lenge har dere hatt relasjoner med deres kinesiske handelspartnere?
- Vet du om de er privat eid eller statlig eide?
    - Evt. Synes du det er forskjell på dem? Evt hvordan?
- Føler du at du kjenner de godt? Hvordan er stemningen under møter, er det veldig formelt, uformelt? Hva gjør dere når dere møtes? (Er det kun møter og forhandlinger om pris på produkter?)
- Hvor møter dere de kinesiske handelspartnerne?
    - (i Kina eller i Norge eller begge deler?)
    - Tar dere noen sikkerhetsmessige forbehold når dere møter dem?
        - Hvorfor/hvorfor ikke?
        - (i.e. når dere drar til Kina)

evt ulikheter mellom Kina og andre land

- Hvilke land hører selskapene/bedriftene dere har handelsrelasjoner til?
- Synes du det er noen forskjell når det gjelder å gjøre business med de ulike? Evt hvilke forskjeller?
- Gjør dere ulike forberedelser når der gjelder møter og avtaler med kinesiske selskaper enn med selskaper fra andre land? Evt. hva/hvordan?
- Føler du deg komfortabel under møter og kommunikasjon med kinesiske selskaper?
    - Er det noe du føler du må justere/tilpasse når det gjelder kontakt, møter og avtaler med dem?
- Hvordan er tillitten din til de kinesiske kundene/businesspartnerne?
- Er det annerledes enn til andre kunder fra andre land? Annerledes enn med norske kunder? Evt hvordan?

Kontrollsp.m. tillitt:

- hvordan synes du tillittsforholdet mellom nordmenn er? Tillitsnivået i norge generelt er? Hva tenker du om tillitt det norske samfunnet? Til folk, politi, myndigheter etc.?
- Merker du noen forskjell på grad av tillitten mellom norske og utenlandske handelspartnere? Hva er likt, eller annerledes?

Kunnskap om de tette båndene mellom staten Kina og statlig eide bedrifter, og også mellom private kinesiske bedrifter og staten.

Objective: to determine the level of knowledge about governance in China, and about Chinese industrial espionage

- Hva vet du om forholdet mellom staten Kina og kinesiske selskaper?
- Er det forskjell på å gjøre handel med kinesiske private og statlige eide selskaper?
- Har du hørt om industrispionasje? Hva legger du i begrepet? Hvor har du hørt om det?
- Vet du hvem PST og etterretningstjenesten utpeker som trusler for norsk næringsliv?
- Vet du hvilke sektorer kineserne er interessert i?
- Vet du hvorfor Kina er interessert i din sektor?

- Hva tenker du om NSR sin bekymring for norske små og mellomstore bedrifter sin sikkerhetskultur?

Helt til slutt, er det noe du vil legge til? Noe du synes jeg burde spurt om?

Appendix 2

Intervjuguide The Norwegian Police Directorate (Politidirektoratet) (POD)

1. Kort om min oppgave
2. Få underskrift på samtykkeskjema. (gir tillatelse til å bruke navn og stillingstittel på informanten).
3. Spør: Vil du ha oppgaven tilsendt til gjennomlesing før jeg sender den til trykk? Evt. at jeg sender deg de delene hvor jeg har brukt informasjon fra dette intervjuet?

Om samarbeidsordningen mellom politi og næringsliv

1. Hvor lenge har du jobbet med næringslivet?

2. Når ble et slikt samarbeid etablert? Var det politiet, næringslivet eller politikere som etterspurte et slikt formelt samarbeid?

3. Hva går samarbeidet ut på?

4. Har det vært en endring i hvor ofte eller hvor mange bedrifter som kontakter dere etter at det ble etablert et formelt samarbeid mellom politi og næringsliv i hele landet?

5. Hva slags saker er det næringslivet kontakter dere om? Hva slags saker henvises videre til PST eller KRIPOS eller andre?
    a. Hva slags saker er det mest av?
        i. Etter kriminell hendelse eller forebyggende? Noen endring?
    b. hacking?
    c. illojale innsidere/ansatte?
    d. Sikkerhet på reisen?
    e. Patentrettigheter i utlandet?
    f. Har noen henvendt seg til dere om utenlandsk spionasje mot sin bedrift? (hacking, stjålne mapper, elektronisk utstyr, lekkasjer om bedriftshemmeligheter eller annen sensitiv informasjon?)
        i. Hvilke land har det vært mistanke om?

6. **Hvilket inntrykk har du av sikkerhetskulturen blant norske bedrifter? Hvorfor tror du det er slik?**
    (sikkerhetskultur = holdninger, kunnskap, motivasjon, adferd hos ansatte som igjen uttrykkes i bedriftens totale sikkerhetsatferd – def. fra NSM)

    a. Hvordan er kunnskap om:
        i. Om utenlandsk industri- og bedriftsetterretning? At det angår norske bedrifter.
        ii. spesielt Kina? (båndene mellom stat og bedrifter, at alle kinesere i inn- og utland er pålagt av den kinesiske staten å bidra med informasjonsinnhenting der som staten ber dem om det. At Norge år

etter år utpeker Kina (og Russland) som de største etterretningstruslene mot Norge. Særlig Kina som bedrifts- og industrispion.)

   b. Er det mer utfordringer hos noen bedrifter enn andre? Hva slags type bedrifter er det? Noen forskjell på sikkerhetskulturen blant store og de små og mellomstore bedriftene?
   c. Ser du noen forbedring/forverring?

7. Hvordan synes du satsingen på samarbeid mellom politi og næringsliv går?
   a. Hva mangler/kan gjøre den bedre?
   b. Mørketallsrapporter og KRISINO(?) hevder at mange bedrifter ikke rapporterer f.eks hacking fordi de ikke tror politiet kan løse saken, og at den blir henlagt. Stemmer dette?

8. PST sin årlige trusselvurdering for 2018 viet en stor del til norske bedrifter – jeg har ikke sett dette i tidligere trusselvurderinger- hvorfor gjør de det nå?

Norge generelt – for å se hvordan POD oppfatter norsk kultur

9. Noen akademiske teorier hevder at nasjonal kultur påvirker sikkerhetskultur en i organisasjoner/bedrifter/grupper innenfor et land. Hvordan tror du norsk kultur påvirker sikkerhetskultur blant organisasjoner/bedrifter/grupper i Norge?
10. Hvordan synes du sikkerhetskulturen er generelt i Norge, også utenfor næringslivet? (hva slags holdninger, motivasjoner, kunnskap og adferd har vi generelt?)
11. Hvorfor tror du det er slik?

Om utlandet

12. Har dere i politiet samarbeid/utveksling av erfaringer med politiet i andre land om deres samarbeid med næringslivet?
13. Hvilke land?
14. Er utfordringene forskjellige?
15. Har du noe inntrykk av hvordan sikkerhetskulturen blant næringslivet er i samarbeidsland? Har deres utenlandske kollegaer andre type utfordringer enn dere? Hva er de?

16. Har dere noe samarbeid eller kontakt med USA? Vet du noe om samarbeid mellom politi og næringsliv i USA?

17. **Noe mer eller noe annet du vil nevne som jeg ikke har spurt om**? Noe viktig jeg bør ta med meg videre i forskningen?

Norges miljø- og biovitenskapelige universitet
Noregs miljø- og biovitskapelege universitet
Norwegian University of Life Sciences

Postboks 5003
NO-1432 Ås
Norway