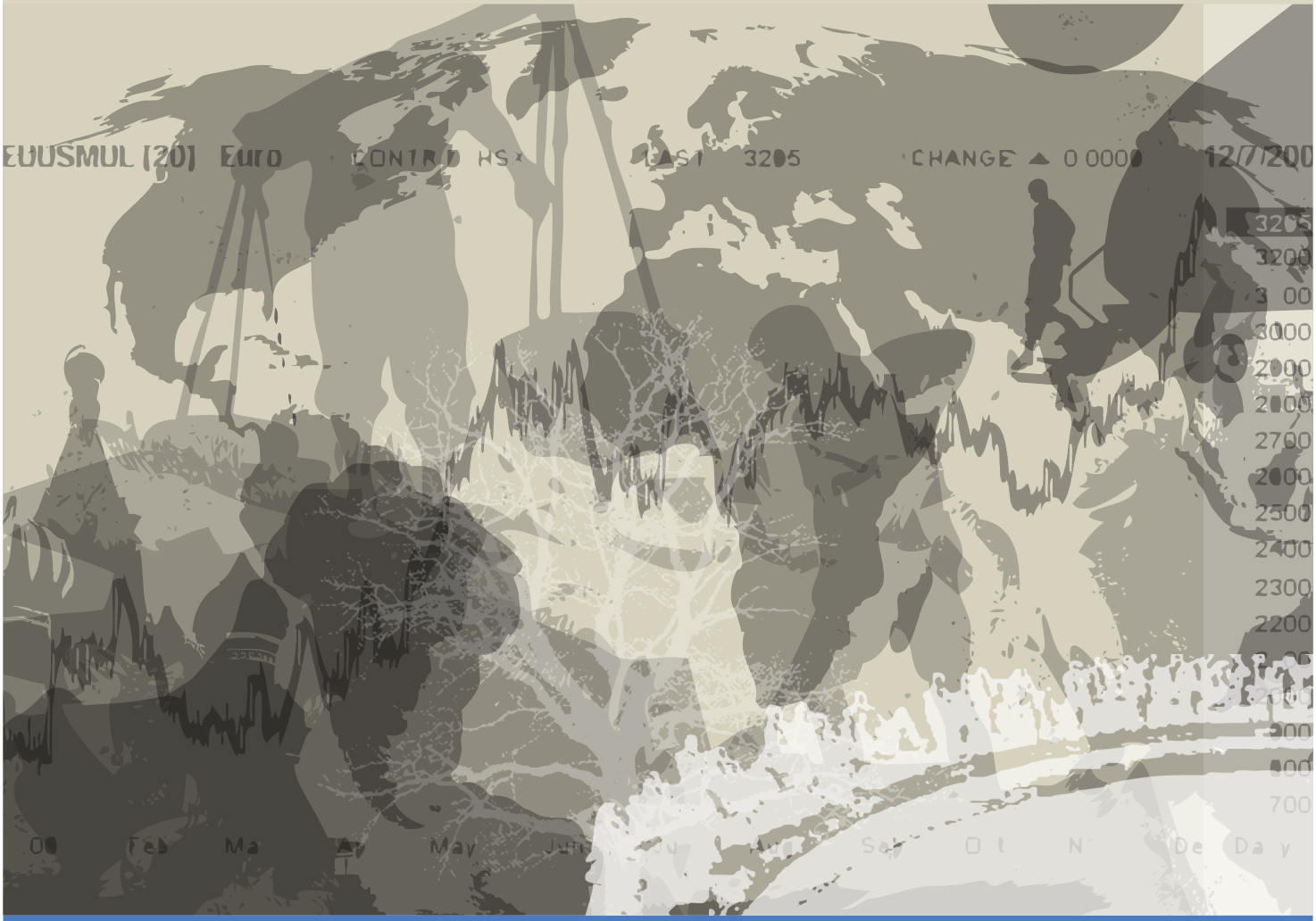
Norwegian Institute of International Affairs

Comparing Cyber Security

Critical Infrastructure protection in Norway, the UK and Finland

Lars Gjesvik



NUPI Report
[5 / 2019]

Publisher: Norwegian Institute of International Affairs

ISSN: 1894-650X

Visiting address: C.J. Hambros plass 2d
Address: P.O. Box 7024 Dep.
NO-0130 Oslo, Norway
Internet: www.nupi.no
E-mail: post@nupi.no
Fax: [+ 47] 22 99 40 50
Tel: [+ 47] 22 99 40 00

Comparing Cyber Security

Critical Infrastructure protection in Norway, the UK and Finland

Lars Gjesvik

Published by the Norwegian Institute of International Affairs

Contents

Foreword and acknowledgments

Cyber security is a topic of growing importance. Modern societies are rapidly becoming more digitalized, increasing our dependence on the security of various digital devices. As societies are becoming more vulnerable to digital attacks, improving the efforts to provide cyber security is vital.

An area where cyber security is particularly important is the protection of critical infrastructures. Securing critical infrastructures is of great importance for any modern society. If these were to fail the implications are potentially disastrous. Ensuring that digitalization does not result in unacceptable risks and vulnerabilities is therefore paramount.

In 2018 NUPI published a report on cyber security for the petroleum sector. This project builds on that publication, expanding the topics examined in two ways. Firstly, by broadening the sectors examined to telecommunications and energy. Secondly, by comparing the work on cyber security in Norway with that in the UK and Finland. By expanding the empirical material this report will hopefully provide added value to anyone working on providing cyber security.

Doing so is a challenging exercise, and various stakeholders might hold differing or conflicting perceptions. In order to provide accurate descriptions balancing these views is crucial. The aim of this report is not to provide definite answers but offer some clarity on a complex and multifaceted issue.

This report would not have been possible without financial support by the Norwegian Water Resources and Energy Directorate (NVE), Statkraft and Telenor. NUPI would also like to thank all the organizations and individuals participating in the interviews, or otherwise providing information and ideas relevant for this report.

Summary

Cyber security and protecting critical infrastructures from digital harm are of increasing importance for governments around the globe. Tackling this issue is challenged by two distinct features of cyber security in Western states: Firstly, the transnational nature of digital risks and threats necessitates cooperation and engagements beyond the state, through international and regional organizations and institutions. Secondly, the considerable extent of private ownership forces states to rely on and engage with private companies, through regulation or public–private partnerships (PPP). Through comparative analysis of the approaches taken to PPP and European cooperation for energy and telecommunication in Finland, Norway and the UK, this report examines how states engage with these issues.

The greatest difference is found to lie between the two Nordic states and the UK. This is not the result of divergent national perceptions and understandings, but of the more centralized and intelligence-centred approach taken by the UK in contrast to the whole-of-society trust-based approach of the Nordic states. Both approaches entail distinct benefits and drawbacks. The major concern in the Nordic states is the lack of public resources and capacity, as well as the fragmentation of responsibility and capabilities. Realizing the importance of culture, context and history in shaping how public authorities respond to cyber-security concerns is of vital importance for enabling better policies. This report concludes by presenting a set of best practices identified in the three case countries.

Introduction

In recent years, cyber incidents have grounded airline traffic (Haugli et al. 2019), halted surgeries and taken down health services (Wiedeman 2019), entailed expensive damages as well as disrupting global commerce (Greenberg 2018) and even caused short-term blackouts (FireEye 2018a). From the humble beginnings of connecting various universities in the USA in the late 1960s, the Internet has now become a world-spanning network underpinning modern society (Klimburg 2017). Highly digitalized states like Norway are increasingly dependent on communications technologies for providing a long list of services that its citizens rely on and expect. As critical infrastructures become digitalized, cyber security is also becoming an issue of societal security.

Increasingly, governments are realizing that this new security risk poses a stark challenge and threatens to undermine the gains made by digitalization. In fact, cybersecurity is not only a new security challenge – it also raises difficult questions regarding the role of the state and the functioning of the international system (Kello 2017: 23–58). Responding to the rapidly developing cyber landscape requires novel ideas, new forms of cooperation and original initiatives on the part of the public authorities (von Solms & Van Niekerk 2013).

This report presents the results of a pilot study mapping how selected states have gone about dealing with this challenge. This was done through a comparative study of approaches taken in the UK, Finland and Norway as regards the energy[1] and the telecommunications **s**ectors. Three research questions provided a framework for the analysis:

1) How is the threat and risk landscape changing for critical infrastructures? What are the main developments of recent years, and where is the landscape heading?

2) How does the public and the private sectors divide responsibility for preventing and responding to cyber-security incidents?

3) What is the consequence of varying integration within the European Union? Is the EU considered to be a relevant actor in the

[1] For the Norwegian context, the petroleum and gas industries are dealt with separately from the electricity sector, and it is this latter group that this report addresses.

provision of cyber security, and how do the states engage with the union differently?[2]

This report starts off with a brief description of the methodology utilized and the limitations and challenges identified during the project. Secondly, it offers a description of the changing landscape and risks to critical infrastructures, in general and in the two industries chosen for study. Moving beyond the developments on threats and risks, the report then enquires how states attempt to meet the new challenges of cyber security. The national structures and approaches in Finland, Norway and the UK are described, serving as the basis for the subsequent analysis. Drawing on interview findings, the report notes some commonalities and divergences in the three case countries. Finally, challenges in preventing and responding to incidents in Norway are described, along with relevant practices and policies identified in the two other case countries.

Cultural and contextual factors, along with path-dependency, are found to explain most of the differences among the three case countries. Major perceptions of the challenges and limitations are the same, as are the limitations for the state as a provider of cyber security. Also similar are the chief issues identified: such as improving security for small and medium-sized companies (SMCs), and managing supply chains. Norwegian efforts at preventing security incidents have been broadly on par with, or better than, those of the two other states, but there are distinct challenges as regards responding to and managing potential crises.

The main finding concerns the impact that size and resource base have on state approaches. Smaller states face distinct challenges in providing cyber security, while also enjoying certain advantages. Identifying comparative strengths and weaknesses can prove useful in guiding future efforts at improving cyber security. In Norway, regional collaboration and cooperation have been an underutilized resource, in particular the potential for even closer Nordic collaboration to deal with the challenges facing smaller states with less resources.

[2] I am grateful to all participating respondents and interviewees. Special thanks are due to the Norwegian Water Resources and Energy Directorate (NVE), Statkraft and Telenor for financing this project.

Methodology and limitations

This report draws primarily on two types of empirical research. On the one hand, extensive desktop studies have been conducted – analyzing, comparing and mapping the development of various government strategies, publications and statements in all three countries. These desktop studies have subsequently been enhanced by a review of the relevant literature, to identify key challenges as well as hypotheses that have been put forward. This documents-based analysis makes up roughly half of the data utilized in this report.

The second source has been 23 semi-structured interviews conducted between November 2018 and February 2019. In Norway, the interviewees were senior public officials as well as senior employees in relevant private firms. For Finland and the UK, the respondents were senior public officials as well as researchers and independent experts with significant experience in the field. These semi-structured interviews were partly open-ended in order to identify issues and challenges and were partly based on findings from the desktop review. A final source of data, complementing the semi-structured interviews, has been participatory observations in various forums in Norway and the UK, as well as informal conversations with experts from the three countries.

This study is meant as a preliminary analysis to refine and improve hypotheses for further research. The aim was not to draw causal claims, nor was this designed to be an in-depth study of the various research questions. That would have required a more comprehensive format with a wider interviewee base, to avoid biases and overreliance on too few sources. Rather, the present study is intended to inform subsequent research, and should be utilized accordingly.

A final limitation of this study has been the rapidly shifting landscapes in all three countries examined. Both Finland and Norway are developing new strategies and establishing new institutions, but the most significant challenge by far has been the still-ongoing Brexit negotiations. This was a challenge as regards arranging interviews; as a result, the empirical basis for the UK was smaller than in the other two states. This was sought remedied by greater reliance on secondary literature and documents, but the relative paucity of interviews remains a weakness of this report.

Cyber security and critical infrastructures

Cyber security as a term encompasses protection of various systems and functions from digital threats. It is a broader term than information security, which only refers to the digital systems themselves, by incorporating the role these systems play in societies or companies. Cyber security, therefore, is a sprawling term that encompasses everything from criminal activity to the use of digital technologies in warfare. A common typology further divides cyber security into three different parts: cybercrime, cyberwar and cyberespionage/disruption. Cybercrime is simply criminal activity through cyberspace, most breaches and incidents are the work of various criminal group looking for monetary gain. Cyberwar covers the use of digital tools in war and is rare to the extent that some argue it does not really exist. Finally, espionage and disruption include a broad group of events which at times might overlap with the other two categorizations (See: Rid 2013). For the protection of critical systems, the concern is not necessarily espionage and criminal activity per se, but the risk that digital technologies would be used to destroy and disrupt their functionality. It has long been argued that the same vulnerabilities that enable cybercrime and espionage can be leveraged for more destructive purposes, namely sabotage or disruption by political agents (Ibid).

As critical systems and functions are digitalizing the threat of cyber-attacks moves from a fringe concern to one of national security (DSB 2019). The use of cyber tools as means of influence in political conflict, 'cybered-conflict', has been a growing concern in modern societies for some time (Demchak 2012). During the last decade, high-profile incidents like the 2010 discovery of the Stuxnet worm and the 2013 Snowden revelations thrusted digital vulnerabilities into the spotlight. As these real-world cases illustrated the potential and utility of exploiting digital vulnerabilities, states increasingly use digital tools for political gain and influence (See: Kello 2017; Sanger 2018).

The implications of this shift have been the subject of numerous analysis and academic research, as it is argued to represent a significant shift in the distribution and use of power in the international system (See: Kello 2017; Klimburg 2017). One of the most concerning developments has been the increased use and targeting of private companies in political conflicts, with the misuse of civilian companies

and infrastructures for political gain upending the state-centric international system (See: Egloff 2017; Kello 2017). This shift towards targeting or misusing private companies as a means of harming societies takes various forms, yet one of the most persistent concerns has been the fear of attacks targeting the industrial control systems of critical infrastructures.

Attacks targeting of industrial systems are rare, yet they still happen. A recent incident occurred in November 2017 when a Middle Eastern industrial facility was the target of an attempt at digital sabotage (Dragos 2017; FireEye 2017). The malware, found in the summer of 2017, targeted the Schneider Electronics Triconex industrial fail-safe system installed. These fail-safe systems are intended as emergency safeguards in the event of equipment malfunction, to prevent widespread damage and contain incidents. Investigators of the incident stated that the likely goal of the attack was the disabling of the fail-safe systems, making a subsequent attack on the industrial machinery far more destructive (FireEye 2017). Instead of disabling the failsafe, a misconfiguration in the attack triggered the failsafe mechanism, forcing the plant to stop (Dragos 2017; FireEye 2017).

Later investigations indicated that the attack had been ongoing since early summer 2017, and that the attacker had been active in the networks at the plant since possibly 2014. The incident caused widespread alarm among experts as the targeting of fail-safe systems could result in the failure of industrial machinery and possibly loss of human life. It was thus interpreted to be the first cyberattack where widespread physical destruction and possible injuries was the ultimate goal (Bing 2018). While not attributing the actor to any state, a subsequent report by security firm Dragos described the working of new threat actor XENOTIME, thought to have been active since 2014, as the culprit. The Xenotime group was also seen active in other industrial control systems globally (Dragos, 2018), contrasting earlier statements that the malware was limited to the one incident (Dragos 2017).

While large-scale destructive attacks against critical infrastructures are frequently established as worst-case scenarios, they remain rare and are likely to remain so. A primary reason for this is technical: In order to conduct any such sabotage operation, an adversary would have to have in-depth access and knowledge about that system. Launching such an attack is also likely to require long-term operations spanning several months and possibly years. Getting that kind of access requires a range of custom-made tools, methodologies and significant resources which in

sum makes it close to impossible to scale to multiple sites at once (Larson 2019). Further decreasing the likelihood is the firm political stance against these types of attacks taken by states, where the targeting of critical infrastructures is considered sufficient for an Article 5 response in NATO as an example (NATO 2017). As such scholars have argued that there is a norm emerging against these types of attacks (Nye 2017). Destructive attacks that cripple critical infrastructures are therefore likely to only occur during high-level conflicts and war, even though counter-examples do exist.[3]

Yet, the issue for critical infrastructure providers is not just targeted attacks crossing the threshold of cyber conflict. The interconnected nature of digital systems makes the risk of collateral damage and unintended consequences a serious concern. While sabotage operations and physical destruction require highly specific tailored malware, generalizable off-the-shelf malware can still cause significant harm if security practices are lacking. In fact, the malwares that have caused the most widespread harm to date (and are publicly known) have not been custom-built tailored tools but those that utilize common weaknesses to spread rapidly in less-secure systems. While these types of attacks generally have less severe impacts than the more advanced operations, they can still cause significant harm in any company they infect (Greenberg 2018). The threats towards critical infrastructures thus span from highly targeted and sophisticated attacks to collateral damage and unintended side-effects. A noted example in this regard is the WannaCry incident, when a misconfigured ransomware crippled a third of the UK health service resulting in roughly 20.000 cancelled appointments, including surgeries (UK National Audit Office 2017).

Cyber security is not a uniform practice: different companies and industries have different concerns and risks. Some commonalities exist but examining the threat landscapes for the different sectors investigated in this report can shed further lights on context-specific issues.

Threat landscape for energy companies

Like for any modern company cyber incidents is increasingly part of the business-as-usual in the energy sector. While negative incidents in some

[3] The most relevant counter-example being the shutdown of a German Steel Mill in 2014, which admittedly is not critical infrastructure. While very little is publicly known about the incident one hypothesis is that the shutdown was the result of an espionage campaign gone wrong. See: Zetter 2015 for more on the case.

form are growing increasingly common, attacks targeting or threatening to harm the energy supply remains rare. Most incidents cause damage in administrative IT systems, with consequences ranging from almost none to quite severe (NVE 2017). Still, the criticality of the electric grid means that any incident that causes significant downtime could have large societal implications (Smith 2018). It is therefore important to differentiate between two distinct concerns: For individual companies the most significant risk to business continuation is the continuous development of cybercriminal activity targeting easy-to-reach administrative systems. For societal security, however, the largest concern is targeted attacks against industrial control systems (ICS). These systems are particularly vulnerable as they tend to be old and outdated with little or no security. Security practices therefore centre around segregating them from the administrative systems through various layers of firewalls and demilitarized zones. Attacking these industrial control systems are increasingly executed through a two-pronged attack: initial probing and breach of office systems use common tools deployed over long periods of time in a manner consistent with Advanced Persistent Threats (APT). Once a firm foothold has been established the subsequent targeting of the industrial systems themselves use advanced tools custom-made for each industrial system (Slowik 2018). A final concern and vulnerability noted in the interviews regarded large-scale disruptions of the digital systems supporting the energy market. While attacks on individual companies' administrative systems was unlikely to result in significant harm, the situation would change if the scale was large enough. Questions was raised of the resilience of the energy system against attacks that disrupted the market itself, as companies would struggle with managing an increasingly complex system of supply and demand.

Threat landscape for telecommunications

Telecommunications role in societal security has changed drastically over the last decades. While maintaining lines of communication has always been of vital importance for states, digital infrastructure increasingly underpins a variety of societal functions. While telecommunication providers at all levels of the digital infrastructure might be targets of cyber incidents and attacks, the societal implications might vary greatly. The by far most serious concern involves the core digital infrastructure on which all other telecommunication providers rely upon. Consequently, the company(ies) running said infrastructure are vital for broader societal security (NOU 2015: 13). The most primitive, albeit sometimes effective vector of attacks are Distributed Denial of Service (DDoS) attacks, where networks are flooded with

inauthentic requests. A noteworthy case in this regard is the Mirai botnet, which leveraged poorly secured IoT devices to launch a DDoS of unprecedented scale at Internet infrastructure owner Dyn (Krebs 2018). While the rise of IoT might make DDoS attacks even more powerful in the future, tools and services that mitigates the attacks exist and are largely effective. More targeted and sophisticated attacks are a bigger threat, yet the high level of security in the industry as well as the complex systems bars anyone but the most advanced actors from succeeding (Kaspersky 2016). Yet, the role of telecommunications in carrying sensitive data makes them a lucrative entry point for more sensitive targets. Supply chain attacks and sophisticated espionage campaigns are therefore significant concerns for large telecommunication companies (Ibid).

The challenges of providing cyber security

The developments above highlights several of the trends that make the provision of cyber security such a challenging proposition for states. One of these challenges is the increased targeting and utilization of private companies in the name of state interests. In the TRISIS case the target was a petrochemical facility and the attack vector the machinery delivered by a private company. Both the target and the attack vector are difficult for states to address as it challenges the lines between state security and private business. The dependence on global suppliers, which can be critical for niche systems like Industrial Control Systems, limits the ability of single states to intervene and secure their systems. The global and interdependent nature of digital communications systems results in a high degree of *complexity* in meeting these challenges. This socio-political complexity is further exacerbated by technical complexity and the rapidly shifting landscape: vulnerabilities and novel attack vectors are continuously discovered and exploited, necessitating continuous labor to stay ahead of developments. The existence of undisclosed Zero Days, or vulnerabilities that are not known to the wider security community, ensures that a certain level of *uncertainty* remains. It is therefore argued that while security practices can significantly reduce the probability of something going wrong, complete digital security is impossible (Lysne 2017).

Furthermore, the difficulties in attributing attacks complicates the efforts to deter politically motivated incidents (Rid & Buchanan 2015; Libicki 2009: 41–52; Singer & Friedman 2014). The Trisis case offers a clear example of the difficulties involved in linking incidents to political actors. The sophistication of the attack, as well as the long-term probing in the years leading up to the attack, both indicate a well-resourced state actor (Dragos 2018). This hypothesis is strengthened by the target and

geopolitical context for the incident, which also implied political motivation: While initial reports did not attribute the attack, subsequent information revealed that the target had been a Saudi Arabian petrochemical facility (Bing 2018). This led to further speculation regarding the attacks, with several experts pointing the finger at Iran. To date the incident has not been conclusively attributed to any actor, yet it has been asserted that the malware was 'most likely' built at a Russian research institution (FireEye 2018b). The persistent issues in attributing attacks and making actors answerable for their actions continues to be a challenge, even if a string of western states have taken a firmer stance in attributing incidents over the last year (US Department of Justice 2018).

As deterring, and thus avoiding, politically motivated attacks remains dogged by the persistent issues in holding states accountable for their actions online, focus has been centred not just on preventing attacks from taking place but limiting their effect. Resultingly, the majority of the work on protecting critical infrastructures from threats has been centred on practices of risk management and *resilience* or minimizing the possibility that an incident will occur while simultaneously enhancing the ability to manage any disturbance (Libicki 2009). This is not to say that resilience is the only paradigm in managing digital risk, both prevention and deterrence are crucial pillars of state approaches, yet it is arguably the most efficient way of providing cyber security at a societal as well as company level (Singer & Friedman 2014: 169–180).

Approaches to cyber security are not uniform, however. While the broad terms and concepts describing cyber security are common for most states, the resources they have at their disposal and other contextual factors impact the different approaches taken. In the subsequent section a comparison will be made of the structures and institutions involved in Norway, Finland and the UK.

National approaches and structures

The provision of cyber security is affected by a multitude of different factors. Firstly, the sector and companies to be secured may differ: for instance, large multinational companies require a different approach from that suitable for small family-run ones. Mapping the various sectors in the three case countries is therefore important, to indicate why and if the approaches might differ. Secondly, context, history and culture all influence how the problem is perceived and solved. If states have diametrically opposing ideas about cyber security, their security practices and policies are likely to differ as well. Finally, cyber-security institutions are not necessarily built from scratch: existing institutions and organizations create path-dependencies that must be taken into consideration. This chapter offers a brief outline of the energy and telecommunications sectors in the three countries before describing the main organizations involved in the provision of cyber security, as well as the most important documents and strategies. This will then form the empirical basis for the subsequent comparison and analysis.

Energy sector

Finland, Norway and the UK all have rather similar energy sectors, divided into three components. Generating electricity is done by multiple companies, which sell their electricity on the free market as a commodity. The criticality of these producers depends on their size. Ensuring that electricity producers and consumers are connected is done through the electricity grid, the national transmission grids being by far the most important. In all three states, these transmission grids are run by a single entity responsible for stable nationwide coverage. Various regional distribution networks – either separated into regional and distribution grids (as in Norway and Finland) or run as an integrated distribution network (the UK) – then connect the national grids with end-consumers.

For Norway the primary source of electricity is hydropower, supplying 97% of its electricity demand (IEA 2017). The Norwegian transmission system is run by Statnett, a state-owned enterprise under the Ministry of Petroleum and Energy (Statnett 2019). Many companies are involved at the distribution level, with a total of 146 companies of various size

owning or operating regional and/or distribution networks (NVE 2016). In the UK, electricity production is undertaken by widely differing actors, ranging from large multinational companies to family-style producers. As of 2016, electricity generation was generated primarily through gas (40%), nuclear plants (20%) and wind (10%), with various other sources contributing to the rest (HM Government 2017). Energy supply in the UK has been dominated by six companies – the 'big six' – who had a market share of roughly 75% for electricity (and gas) supply in 2019. The electricity transmission system in the UK is run by the National Grid plc, a private company. The regional distribution networks are run by 14 different companies operating as licensed monopolies, while the retail market is dominated by a large number of companies of various sizes (OFGEM 2019). In Finland, electricity generation stems primarily from nuclear energy, hydropower and biomass, responsible for 34%, 22% and 18% respectively (IEA 2018). Finnish power production is also diverse, involving over 150 different companies (Energy Authority Finland 2018). Connecting the power plants with regional systems and consumers is the national transmission grid, run by Fingrid (Fingrid 2019). While various retail companies operate in a free market to provide electricity, maintaining the security and functionality of Finland's regional and distribution grids is the responsibility of licensed monopolies, the major ones being Caruna, Elenia and Helen Electricity Network Ltd (Energy Authority Finland 2018).

Telecommunications sector

For Norway the telecommunications market is dominated by Telenor, which runs and maintains the core national network. Dependence on this core infrastructure, and the lack of viable alternatives, has been identified as an issue for Norwegian societal security (NOU 2015: 13). While the telecommunications market involves several different actors, their dependence on the services provided by Telenor makes the latter dwarf any other as regards societal criticality (NKOM 2017). By contrast, in UK various companies run national networks, the largest ones being the BT group, Level 3 Communications, Virgin Media and Cable & Wireless. Although BT has historically played a critical role in running the core network nationally, with other companies utilizing the BT network to reach areas to which they lacked access, this has been diversified in recent years (EC-RRG 2011). Due to their role in running critical digital infrastructure nationally, Cable & Wireless, KCOM and BT are officially incorporated in security preparedness (HM Government 2015; EC-RRG 2011). Thirdly, Finland has taken a proactive stance to the development of fibre-optic cables and has encouraged cooperation

among network operators in developing broadband networks. Within this market, most national networks are centred around four companies: DNA, Elisa, Finnet and Telia Sonera Finland; these run the majority of fixed and mobile networks, and are responsible for 98% of the fixed broadband coverage in Finland (Traficom 2019)

In sum, the sectors in the three case-study states are broadly similar when it comes to societal security, albeit with some differences. The criticality of Norway's core Telenor network for telecommunications does not have a parallel in Finland or the UK. Similarly, the regional and distribution networks in Norway are run by a more diverse set of companies than in the other two countries. However, these do not add up to a dramatic difference as regards their criticality or the importance of the sectors.

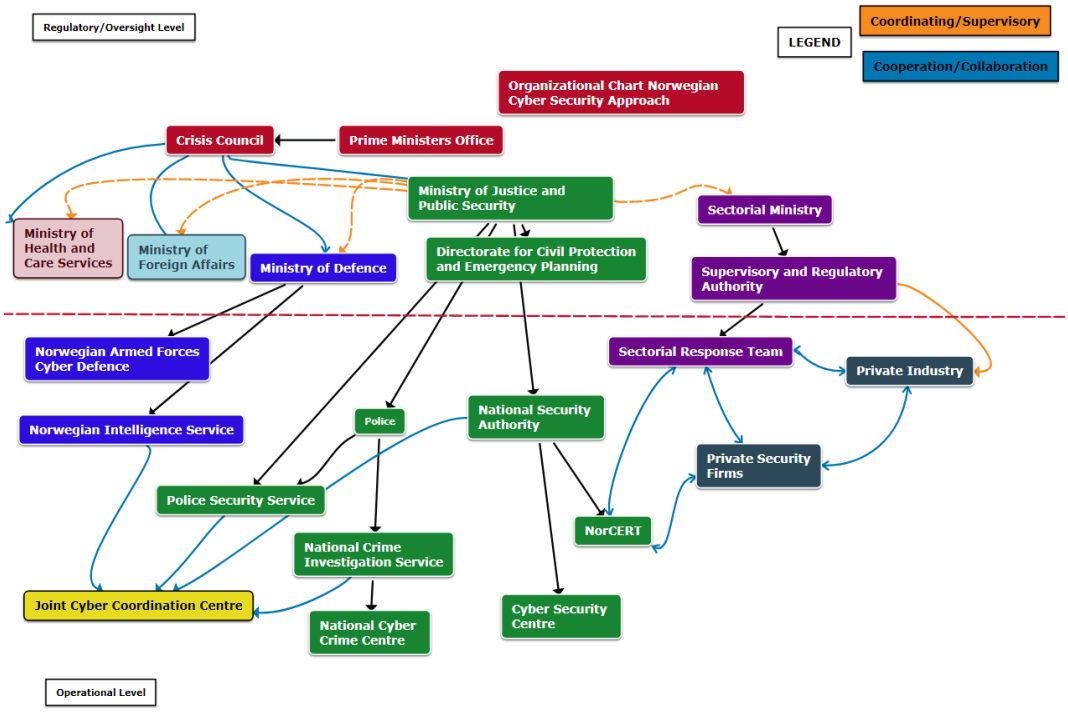
Norway

The architecture of Norwegian societal security is based on four fundamental principles: responsibility, similarity, proximity and cooperation. *Responsibility* indicates that the organization in charge of day-to-day matters should also be responsible in the event of a crisis; *similarity*, that organizing for managing crises should resemble the normal organization; *proximity*, that any crises should be dealt with at the lowest possible level; and finally *cooperation*, that every authority and actor involved in security has the responsibility to ensure the best possible cooperation among and between actors (Meld. St. 10, 2016–2017). In practice this has entailed a structure where each ministry has responsibility for providing security for its specific domains, with some coordinating and overarching responsibilities at the national level.

The Ministry of Justice and Public Security has a cross-ministerial coordinating role on civil security. It is both a coordinating body across the different ministries and public bodies, as well as responsible for formulating national strategies. Supporting the ministry is the *Norwegian Directorate for Civil Protection*, tasked with 'maintaining a complete overview of various risks and vulnerability in general' (DSB 2019). In the event of a large-scale crisis, the *Crisis Council* enters as the coordinating mechanism, convening to ensure collaboration between the ministries involved (Prime Minister's Office 2018). The *Ministry of Defence* is solely responsible for the security of their own systems, placing cyber security firmly within the civilian sector. Defending the military system is the responsibility of the *Norwegian Armed Forces Cyber Defence*; while military resources may be utilized to support civilian sectors, this has not yet been done in connection with a cyber

incident (Norwegian Ministry of Defence 2014). At the operational level, the primary national body is the *National Security Authority (NSM),* tasked with supervising functions under the Security Act. In addition, it informs and advises other actors, and runs the voluntary VDI sensory network. The national CERT, *NorCERT,* is a part of the NSM and is responsible for coordinating the response to digital incidents (Prop 151S, 2015–2016). Further, it serves as the coordinating body of the *Sector Response Teams (SRM),* which act as link between the national authorities and the various companies in the sectors (Norwegian Ministries 2012). These are intended to share information from the national level to the relevant companies, as well as gathering information on incidents in the sector. With the establishment of the new *Cyber Security Centre* this cooperation may undergo changes; however, yet the exact nature of this centre had not been determined at the time of writing (National Security Authority 2018).

Also relevant for the provision of societal security are the *Police*, who are responsible for preventing as well as investigating criminal activity. With the establishment of the new *National Cyber Crime Centre*, police capacity to investigate criminal activity in the digital sphere will be enhanced in the years to come. Further, the *Police Security Service (PST)* is the intelligence and security service tasked with domestic intelligence, transmitting relevant information to actors in annual reports (Police Act, 1995; §17). Annual threat assessments are also published by the *Norwegian Intelligence Service (NIS)*, which is the country's foreign intelligence service. A new law setting the mandate for the NIS is currently under review, with one of the stated goals being greater ability to detect digital threats (Norwegian Government 2018). The intelligence services cooperate with NSM and the *National Criminal Investigation Service* in the *Norwegian Joint Cyber Coordination Centre (FCKS)*, which is to function as a coordination mechanism in the event of serious cyber-attacks (NSM 2019). Finally, the main responsibility for securing critical infrastructures lies with the individual companies that operate the infrastructures: this was underlined with the launch of the new strategy for digital security in 2019 (Norwegian Government 2019).



Norwegian Cyber Security Approach

As the various sectors have important roles to play in providing security, hereunder also cyber security, it is worth examining some of the ways in which the two sectors analysed here differ. For the *energy sector*, ensuring sound management of the resources and companies, hereunder also security, is the responsibility of the *Norwegian Water Resources and Energy Directorate (NVE)*, which undertakes supervision, writes regulations and advises companies in the energy sector. Recently it was decided that NVE is also to function as the SRM for the energy sector (Lovdata 2019: § 3–6). In providing information, analysing incidents and warning companies of emerging cyber risks, NVE cooperates with *KraftCERT*, a private company owned by the major energy operators. KraftCERT serves as both an advisory body and a provider of information to the various companies, specializing in industrial control system (ICS) security, but with a limited operational role and capacity (KraftCERT 2019). For better integration of work on preparedness and security within the energy sector, KraftCERT has been added to the *Energy Supply Preparedness Organization (KBO)*, an organization consisting of all owners of critical energy assets, as well as NVE and KraftCERT (Lovdata 2019).

For the *telecommunications sector*, the body corresponding to NVE is the *Norwegian Communications Authority (NKOM)*, with regulatory and supervisory functions. Unlike the case of the energy sector there is no

CERT owned by the companies themselves: providing information and sharing threat intel is the responsibility of NKOM's operative branch, *EkomCERT*. While EkomCERT is formally a part of NKOM, the two are segregated in practice, to avoid conflicts of interest. EkomCERT further functions as the SRM for the telecommunications sector, facilitating information sharing between national authorities and companies in the sector. Both NKOM and EkomCERT have worked on establishing forums for the exchange of information, with the *EKOM Security Forum* being the most frequently mentioned. This forum aims at improving collaboration and exchange of information between the intelligence services and the major companies in the sector (NKOM 2015). Finally, the telecommunications providers themselves have several advanced cyber security teams and capabilities nationally, as evidenced by Telenors cooperative agreements with the Norwegian Armed Forces Cyber Defence (Telenor 2018).

In recent years there have been several ventures/developments that are now partly concluded, have been concluded while this project was being finalized, or have not yet been implemented. Noteworthy are the potential impacts of the new Security Act (Lovdata 2018), the new cyber security centre (National Security Authority 2018) and the newly established National Cyber Crime Centre (Prime Minister's Office 2019). Moreover, in 2019 the new digital strategy for Norway was issued, along with an action plan and a strategy for improving cyber-security skills (Norwegian Government 2019). Other actions have not yet been implemented, and are at various stages of completion, like the proposed new law regulating the Norwegian Intelligence Services (Norwegian Government 2018) and the recently issued White Paper on national ICT regulation (NOU 2018:14). Finally, the establishment of two new ministries – one for societal security and one for digitalization – is likely to have an impact but is too recent a development to be dealt with in this report.

United Kingdom

The UK approach to cyber security was reworked with the 2016 National Cyber Security Strategy, which reorganized the institutions involved and the general approach. This 2016 Strategy, although identifying several positive gains made since the 2011 version, did not consider the pace of the change as rapid enough to deal with the fast-changing digital threat picture (HM Government 2016). For more agile responses, the government wanted to assume a larger role in pushing for greater cyber security. This was a tacit admission that a market-led approach had proven insufficient as regards cybersecurity, and that private companies

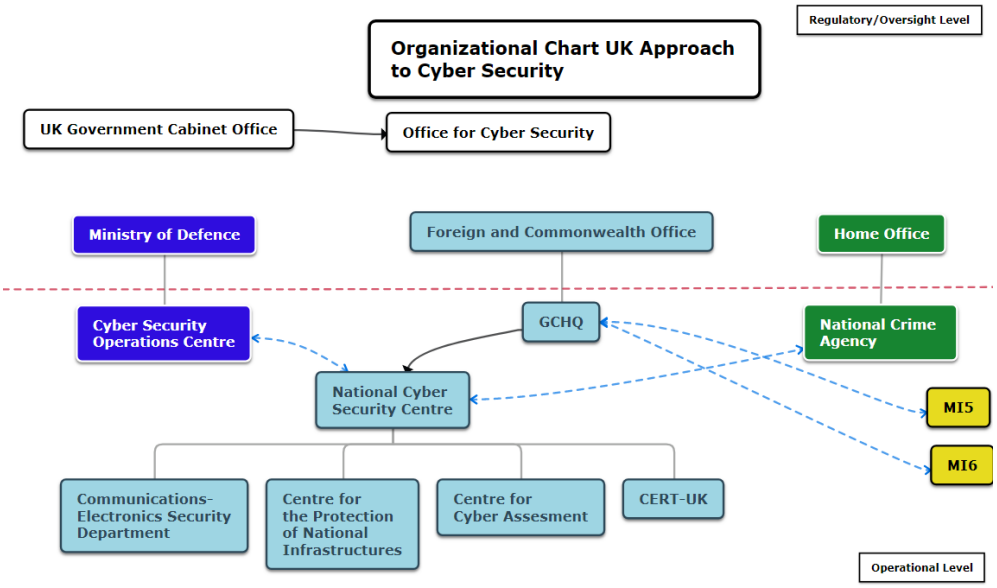
were unwilling or unable to identify and address digital risks properly (ibid: 9). While the 2016 Strategy adopted a forward-leaning rhetoric, the changes have been moderate so far, focused on centralizing and simplifying certain key institutions and organizations, without challenging the underlying reliance on private companies for the provision of societal security[4] (Kriz 2017). Some initiatives have been taken, like the state-led Active Cyber Defence programme, where the state is to take responsibility for mitigating some common digital vulnerabilities, as well as the abovementioned centralizations – but the basic premise and structures of public–private collaboration remain unchallenged (Levy 2018).

The UK approach to cyber security since 2016 is characterized by a fairly centralized and civilian-led approach, with strong involvement from the intelligence services. The overarching responsibility for cyber security resides within the *UK Government Cabinet Office*, which hosts its own *Office for Cyber Security* that sets the main directions and policy initiatives. Thus, the role of oversight and policy development is anchored at the highest level of government. At the operational level, main responsibility lies with the *National Cyber Security Centre (NCSC)* established in 2016, which is to serve as a 'one-stop-shop' for cyber incidents within civilian networks. The NCSC belongs under the *Government Communications Headquarters (GCHQ),* an intelligence body under the *Foreign and Commonwealth Office*. Further, the GCHQ cooperates with both MI5 and MI6 (domestic and foreign intelligence, respectively) in maintaining situational awareness. The police, represented through the *National Crime Agency*, are responsible for dealing with online criminal activity and collaborate closely with the NCSC in classifying and responding to incidents. For the military networks the *Cyber Security Operations Centre* under the *Ministry of Defence* is responsible for cyber security, while also cooperating closely with the NCSC. This ensures a division of responsibilities into a civilian and a military side, with the civilian side spearheaded by the NCSC, which has the greatest responsibility (Dewar 2018).

While various departments and regulators still play a role within their respective domains, and the main responsibility still resides within the owners of critical infrastructures, the broader national institutions have been included in the NCSC. This framework is intended to channel the main body of cyber-security operations through one organization, which thus holds overall responsibility and oversight (HM Government 2016). The result has been a shifting of responsibility for cyber security from

[4] According to interviews

organizations that previously held a more prominent role or merging them with the centre. Interviewees explained that this structure had been chosen as a response to criticisms that previous approaches had been too complicated and chaotic to manage, and that private-sector companies did not know whom to contact if incidents struck. Managing this diverse portfolio has led to the NCSC being further subdivided into four organizations: dealing with intelligence and research (the *Communications-Electronics Security Department*), protecting critical infrastructures (*Centre for the Protection of National Infrastructures*), threat assessments (*Centre for Cyber Assessment*) and emergency support and incident management in the case of major cyber incidents (*CERT-UK*) (National Cyber Security Centre 2018).



UK Approach to Cyber Security

Finland[5]

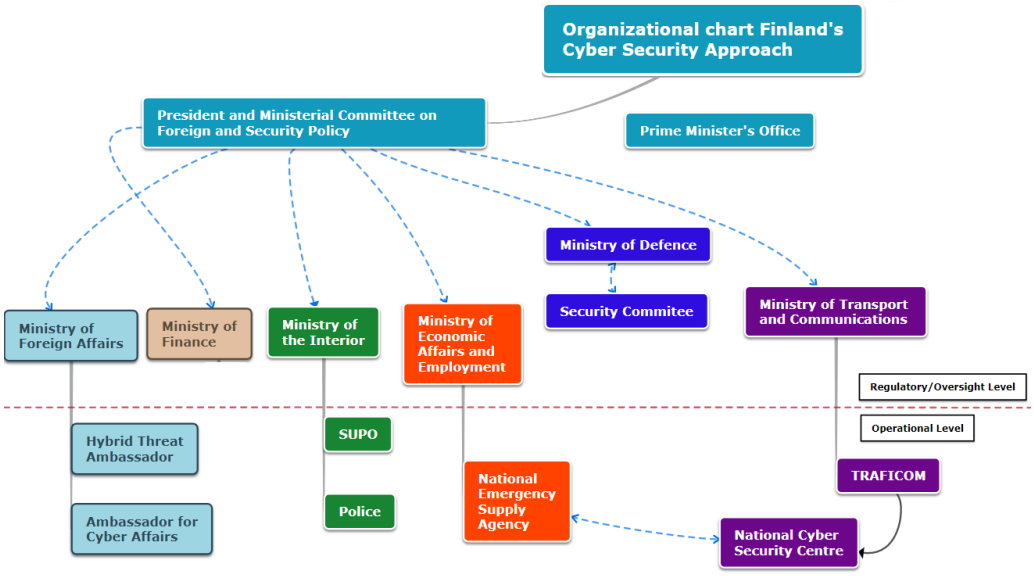
The Finnish approach to cyber security has been primarily defensive, focused on measures of resilience. Building on the existing approach to security, and the history of cooperation between public and private actors, efforts aimed at enhancing resilience have centred around the idea of 'comprehensive security' wherein the whole of society is tasked with contributing to overall security. This entails a close collaboration between various branches of the government, the business community

[5] As a significant share of the publications detailing the security architecture in Finland is written in Finnish, the interviews were used to identify the responsible agencies and institutions.

and even individual citizens (Prime Minister's Office Finland 2011). In the interviews, reasons given were the constraints on available resources, Finland's turbulent history and its exposed geopolitical position. In the development of a cyber-security strategy and approach this 'security on a shoestring' idea was deemed highly relevant, given the high levels of private ownership and involvement. Further, the mechanisms and structures needed to exploit such cooperation were largely in place already. When the strategy was published in 2013, it therefore expanded on a pre-existing structure of comprehensive security, stating that 'In this respect no changes are proposed to the bases of contingency arrangements or to regulations concerning the competences of authorities' (Secretariat of the Security Committee 2013). This further resulted in an ambitious strategy aimed at putting Finland at the vanguard of cyber security by 2016 (ibid).

The structure is based on the ministries having primary responsibility for their respective sectors, with certain cross-sector and national mechanisms in place to coordinate and promote cooperation between different actors. Overseeing the work on comprehensive security is the *Security Committee*, located within the *Ministry of Defence*, which acts as a coordinating body for the various tasks and responsibilities that are delegated and decentralized. Managing crisis responses and facilitating public–private cooperation is the responsibility of the *Emergency Supply Agency*, tasked with protecting and securing the continued functioning of vital societal functions. *The police* have responsibility for dealing with criminal incidents, while the Finnish *Security Intelligence Service (SUPO)* is responsible for intelligence related to national security. *The Ministry of Finance* holds coordinating responsibility for the digitalization and digital security of governmental services, while the *Ministry of Transport and Communications* has an important role due to the telecommunication infrastructures being their responsibility. One of the few cyber-specific bodies to be established is the *Cyber Security Centre (NCSC-FI)*, until recently within the Finnish Communications Regulatory Authority (FICORA), but from 1 January 2019 belonging under the recently established *Finnish Transport and Communications Agency (TRAFICOM)*. Due to its placement within TRAFICOM, the NCSC-FI functions as a centralized hub for collecting information, maintaining situational awareness and responding in the event of a major crisis. *The Ministry of Defence* is tasked with the protection of its own networks but does not have a role in the day-to-day management of cyber security, which in turn ensures that work on cyber security remains in civilian hands. However, in the event of a larger crisis, the *Ministry of Defence* and *the military* may intervene, if invited to do so by the ministry with responsibility for dealing with the incident.

At the time of writing, the Finnish Cyber Security Strategy and approach are under revision. During the interviews, some developments were noted that are likely to influence the ability of Finland to progress in improving its cyber security. The first is the ongoing work on new regulations for the intelligence agencies: the current legislation has been criticized as being too vague, in particular when it comes to the collection and analysis of digital data. Enabling the intelligence agencies to collect and analyse digital information was stressed as important by several interviewees, yet the controversy regarding the trade-off between privacy and security challenged its implementation (YLE 2018). Secondly, the 2013 strategy is currently under revision, yet the publication date of the new strategy is unknown. One of the main issues it is expected that the strategy will address is the lack of a centralized command structure tasked with responding to incidents, resulting in a fragmented approach if a large event was to occur (O'Dwyer 2018). Finally, the thriving private sector for cybersecurity in Finland has shaped the approach to cyber security, relying heavily on the integration of private-sector competencies (Ministry of Transport and Communications 2016).



Finland's Cyber Security Approach

Comparing cyber security

Understanding and comparing different approaches cannot be done solely through organizational charts and lines of responsibility. Equally important are the various cultural factors, interpretations and contexts that affect whether these arrangements will work or not. In the following section, findings from the study are analysed, with a focus on public–private cooperation and international efforts at managing transnational risks.

The challenge of protecting private companies

'Cyber security' is a complex, evolving and multifaceted practice that ranges widely, from nuisance to high-level national security. While protecting critical infrastructures against cyber threats has been a concern for states for well over a decade, it remains a problem, for many reasons. A key factor shaping the various approaches to enhancing the resiliency of critical infrastructures has been the high level of private ownership and involvement in providing security (Herrington & Aldrich 2013). Private companies own a large proportion of what is deemed critical infrastructure – due to the privatization of infrastructures long recognized as critical, such as electricity transmission and water supply, and because of the increased dependence on infrastructures developed primarily by private actors, as with telecommunications (ibid). In the Western world, private companies not only run critical infrastructures: they also possess much of the existing competence and expertise on cyber security (Klimburg 2011). Consequently, there have been frequent calls for basing efforts for achieving cyber security and Internet governance on a combination of public, private and civilian capacities (Harknett & Stever 2009; Sahel 2016).

This is true to varying degrees for different states, but the broad trend is still dependence on the private sector for dealing with the challenges of digitalization (Bossong & Wagner 2016). This has resulted in increased calls for understanding cyber security through the prism of public–private partnerships (PPPs), where the state and various private companies cooperate in providing a public good. The importance of the private sector in providing cyber security is widely acknowledged, but how the cooperation should be organized has been contested, as has the degree of success thus far (Carr 2016; Muller 2016; Bossong & Wagner

2016; Dunn Cavelty & Suter 2009; Christensen & Petersen 2017; Anderson & Moore 2006). The main critique has been that the inherent differences in valuations, goals and ideas between private and public actors remain an obstacle for cooperation (Collier 2018; Muller 2016; Dunn Cavelty & Suter 2009). Others have been more positive, arguing that focusing solely on the conflict between public and private actors disregards other factors that contribute to the relative success of these collaborations (Christensen & Petersen 2016; 2018).

Public–private cooperation: similar issues, different contexts

An important factor is how states and state agencies perceive this threat in their specific contexts. This is true also for the three case countries. In the UK context, the CEO of the National Cyber Security Centre stated: 'I remain in little doubt we will be tested to the full, as a centre, and as a nation, by a major incident in the years ahead, what we would call a Category 1 attack' (NCSC 2018) placing cyber threats on par with international terrorism, geopolitical conflict and major natural disasters (National Security Risk Assessment). The Nordic intelligence agencies also highlight cyber incidents as a major threat, but as the main concerns they emphasize intelligence collection and the possibility of influencing operations, downplaying the potential impacts compared to the UK publications (Fokus 2019; Supo 2018). Official publications in Finland and Norway have been similar in tone, but the Finnish respondents saw the geopolitical concerns as being more pressing.

Even though cyber security is perceived slightly differently in the three states, the broad approaches are similar. All three states and their various organizations used regulation, incentives and cooperation to strengthen critical infrastructures such as energy and telecommunications. There were no clear differences in how representatives of these states judged the importance of public–private partnerships or the general challenges presented by such cooperation. The rhetoric of the 2016 UK strategy seemed to indicate a shift towards a more state-led approach, but actual policies still highlighted cooperation and collaboration, a point that was mirrored in the interviews. While the UK through its Active Cyber Defence and heavy involvement of intelligence agencies is arguably more state-led than Finland or Norway, the divergence was less than expected from published documents and strategies. The most distinct difference between the Nordic states and the UK was not the level of state involvement, but the extent to which it was based on one centralized institution, and the level of involvement of the intelligence agencies.

All three states stressed their continued reliance on private companies for societal cyber security. Similarly, the main issue in establishing successful cooperation was the same: diverging interests and concern between private and public actors. The occasionally misaligned interests and beliefs in private companies and public authorities remain the primary obstacle to any public–private cooperation; this is likely to continue as long as societal security relies on such cooperation.

Although the major trends in the three countries emerged as being similar, the more centralized UK approach diverged from the Nordic states on several key points. One of the major strengths identified in both Finland and Norway was the high level of trust among the various actors in these societies. The cooperative public/private sector tradition was highlighted as one of the reasons for this higher level of trust, as well as the Nordic companies' history of being concerned with societal impact and security. This helped to create a culture conducive to collaboration at the institutional level. Secondly, the relatively small size of Finland and Norway helped to facilitate cooperation at the individual level: in both countries, the communities involved in cyber-security work were small and knew each other. Perhaps the chief effect of this was the greater willingness of civil society to contribute to the provision of security, where the difference noted between the UK and the Nordic countries can be explained by a mix of culture and size (Collier 2016). Coupling such institutional trust with individual relationships also made possible lower barriers as regards information sharing and cooperation. This was the case not only in public–private engagements but across companies as well, with private companies willing to assist each other – to some extent – in dealing with incidents and sharing information.

Expanding on this trust and using small size as an advantage could enable smaller states to pursue different strategies and policies towards improving resilience. On the other hand, small size may also entail specific challenges and difficulties. Smaller size was seen as a barrier to more state-led and intelligence-driven approaches like the one taken by the UK. The relative success of the UK cyber centre was based upon cooperation with the private sector, crossing the classified/non-classified divide, and a foundation of technical expertise. While the first two are replicable in the Nordic context, interviewees from Finland and Norway were sceptical about the ability of the state to build and retain the necessary technical expertise. Lacking the manpower and resources to establish large world-class agencies, smaller states had to innovate, 'building cyber security on a shoestring'. This furthered the view that small Nordic states should expand on their strengths, trust and

familiarity, rather than copying institutions and organizational forms from larger states operating under different contexts.

Transnational issues, regional solutions

A second key feature highlighted in literature and policy documents is the transnational nature of cyber-security threats and incidents (see Kello 2017). This has led to calls for international cooperation on mitigating such insecurities, at the global and regional levels (HM Government 2016; Norwegian Ministry of Foreign Affairs 2017). International cooperation may take place at various levels, using a range of approaches, from multilateral talks on norms and state conduct in cyberspace to exchange of information between technical communities. Perhaps the most clear-cut example of a functioning cooperation that provides real added value is found in the various international forums for computer emergency teams, with the FIRST cooperation the most frequently mentioned. Within these collaborations, security experts can exchange information and assist in interpreting incidents, which greatly enhances the awareness of ongoing threats (Tanczer et al. 2018).

In this report the focus is on European cooperation, mainly at the EU level. In recent years the EU has undertaken a string of initiatives aimed at strengthening the cyber security of its member states. With the General Data Protection Regulation (2016/679) as well as the Directive on Security of Networks and Information Systems (NIS Directive, EU 2016/1148), the EU has provided a baseline regulation for work on cyber security throughout the Union (European Commission 2016). Furthermore, the enhanced mandate of the European Union Agency for Network and Information Security (ENISA), and the pre-existing European Cyber Crime Centre (EC3) provides an organizational platform for the EU to operationalize its increased focus on cyber security. With the conditional agreement on the Cybersecurity Act in December 2018, the EU further strengthened its work, giving ENISA a prolonged mandate and greater (albeit still very limited) resources (European Commission 2018). ENISA was also given a role in upholding the cybersecurity verification scheme, passed in December 2018 and intended to ensure a minimum cybersecurity standard for products and services sold within the EU (ibid). Finally, the developing framework of the Cyber Diplomacy Toolbox aims to give the EU states a common voice when responding to cyber-attacks, to enhance deterrence and stability within the Union (Moret & Pawlak 2017). The EU approach to cyber security should therefore be seen as still under development. Several regulations, organizations and initiatives that are widely considered positive are in

place or underway, although not at the scale or level necessary for significant impact for the three case countries studied here.

The role of the EU in national cyber security

Representatives from all three states were clear on the vital importance of international cooperation for enhanced cyber resilience – in developing norms at the international level and in improving cooperation on incident prevention and response. In addition, several respondents noted concerns over the declining ability of European states to expand their cyber-security sectors, digital systems and services. The growing dependence on Chinese technology, as well as on US firms and intelligence, was viewed unfavourably, albeit this latter concern was mentioned only by a minority of respondents. This decline in the ability of European states, and Europe in general, to keep pace with the growing need for cyber-security firms, technological innovation and specialized competencies was considered a challenge that would require European collaboration to succeed.

There were some differences among the three cases in their approaches to such European collaboration. For Norway the proposed regulation, initiatives and collaborations to strengthening cyber security were viewed positively, but the ability to initiate and strengthen these collaborations was naturally challenged by Norway's not being a full member of the EU. As a result, the EU was accorded a comparatively modest place in Norwegian international engagements for cyber security (Norwegian Ministry of Foreign Affairs 2017). For the UK, the ongoing Brexit negotiations made it highly challenging to obtain clarity on the issue, and there was widespread confusion as to how leaving the EU could affect UK cybersecurity. Here Finland stood out as the most proactive and positively inclined actor as regards European cybersecurity, stressing the potential for European collaboration on several issues (Finnish Ministry for Foreign Affairs 2019). Key among these was expanding the potential market to create competitive cyber-security firms, EU-wide agreements on handling of incidents in the Cyber Diplomacy Toolbox and expanding on collaboration between computer security teams like CSIRTs and CERTs.

None of this was particularly surprising, given the positions of the three states within the European cooperation. However, increased security concerns over digital systems, illustrated most clearly by the Huawei case, are rising on the political agenda and resulting in calls for European collaboration (Politico 2019). If the push for increased overlap between industrial and security policy continues at the European level,

and rhetoric is transformed into action, the position of European non-EU members will become an increasingly relevant question. As the persistent calls for international cooperation to combat the risks from cyber (in)security is being addressed at the EU level, the ability to impact and shape the regulations and developments is likely to become a way for smaller states to get their voices heard and their concerns communicated. EU developments regarding security policy could challenge the relations of non-member states with Brussels and deserves further examination.

Issues, challenges and recommendations

The aim of this project was twofold: first, to map differing approaches and understandings in Finland, Norway and the UK; and secondly, to identify some issues and best practices as regards dealing with these issues. The analysis above has compared approaches in the three countries; the subsequent section will examine the main issues and concerns identified. As the scope of the project had to be scaled down, the main point of departure here is taken in the Norwegian context, using the other two case countries for comparison, to shed light on challenges and possible solutions. The issues identified are not necessarily sector-specific, as there were many similarities in the overarching challenges faced by the two sectors in focus in this report. Where there are sector-specificities to be taken into consideration these will be explicitly mentioned.

Most issues analysed involve difficulties in cooperation between the private and the public sector. To structure the analysis these will be centred around problems that emerge in attempting to prevent security failures and problems in responding to such failures. For the first set of issues, most efforts take place within the various sectors themselves, albeit with national-level regulations and solutions as well. It is in connection with the response-mechanisms, particularly in the event of a politically motivated large-scale and sophisticated attack, that national capacities and responses become especially relevant.

Prevention

Preventing incidents from occurring remains the most efficient way of securing digital systems and critical infrastructures. Although the attention paid to cyber security has risen dramatically in recent years, the fact remains that most incidents and breaches utilize known vulnerabilities and/or human errors (FireEye 2019). The most important work on preventing cyber-security incidents is being done by the companies themselves: 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 in raising awareness in the companies.

How to improve voluntary cooperation?

Private companies undertake most work on cyber security. Both the increased targeting of private companies and the uneven distribution of capacities between the public and private sectors require private involvement in cyber security. This involvement is arguably greater than in the case of other security concerns, making the issue of cooperation more pressing. Why are private companies willing to cooperate? What can be done to promote closer cooperation?

Current situation:

From the interviews, three main mechanisms that improved cooperation were identified: trust, mutual benefit and shared understandings. Trust involved both the interpersonal level and the societal level: whether private companies trusted the government's intentions and institutions, and whether the individuals working in the private and in the public sectors knew and trusted each other. Secondly, the ability of the state to offer valuable services and advice to the private sector was critical. In order to ensure cooperation and goodwill, public institutions had to provide added value that the private sector considered relevant and actionable. The third crucial point was the extent to which private companies were familiar with and able to consider societal security beyond the immediate interest of the company. Thinking and acting in a manner that benefited society at large fostered trust and mutual benefit, as well as making the public services more willing to lean on private actors. Also highlighted was the ability of the public sector to engage constructively with the private sector, taking into account the differing realities and considerations.

Both trust and shared understandings were highlighted as strengths in the Nordic countries. Views on the mutual benefits were more mixed, with some respondents being less optimistic about the value-added provided by public bodies. Providing information, expertise and advice was identified as the main such added-value that public bodies could offer. While interviewees agreed that such information could be useful, they noted that what they received was not always relevant. One problem was the sheer volume of information from various sources, which could be overwhelming even for companies with advanced security teams. Furthermore, the information could at times be overlapping, with the same information coming from numerous sources, even from multiple public bodies. And finally, the limited tradition of sharing intelligence in Norway hampered the ability of intelligence agencies to provide relevant information.

Good practice: Customer feedback

One good practice concerned how certain public bodies took a customer relations approach to PPPs. In Finland, the NCSC-FI gathered feedback from the companies it cooperated with, which in turn allowed it to improve the added value it could provide later and could identify points that needed to be addressed. Similar practices were mentioned in the UK. The public authorities based parts of their approach on the realization that soft measures might be more effective for raising baseline security. This is not to say that feedback mechanisms between private companies and public bodies are non-existent in the Norwegian context – only that expanding on these mechanisms is of importance. Pursuing further initiatives based on this feedback should also be considered.

How can the state improve inadequate practices?

Improving cooperation is an important step for enhancing cyber security. However, what individual private companies deem sufficient might not be enough when broader societal concerns are to be taken into account. As companies have some leeway to interpret regulations as they see fit, this might result in inadequate levels of security. Recognition of the inability of private companies to make sound judgments on risk was in fact a main rationale behind the 2016 UK strategy (HM Government 2016). Mechanisms must be in place for addressing inadequate practices, for instance in supervision and auditing.

Current situation:

A concern raised by a minority of respondents was the lack of supervision on ICT matters by public bodies. The regulations themselves were considered adequate, but companies interpreted these regulations differently, sometimes resulting in poor security practices. This was partly the result of private companies not taking security seriously enough, and partly due to the high level of competency needed to interpret the regulations. Supervision frequently relied on briefings and presentations only and was not equipped to detect such deficiencies. Some respondents called for firmer state intervention to deal with this problem, but none of the case countries appeared to do so in practice.

On the other hand, some respondents argued it was more efficient to use a private company to audit and provide recommendations. As these companies were interested solely in improving security, without the risks of regulations or fines, they were considered more as partners. This

in turn allowed them greater access, which translated into conversations at the level of individual engineers, where issues and practices not addressed during briefings could be identified. Complementing such briefings and reports with 'water-cooler' chat was regarded as indispensable for gathering in-depth information.

Good practice: Benefit of a 'hybrid' structure: KraftCERT

Norwegian interviews highlighted KraftCERT (KC) and their cooperation with NVE as an example of a problem-oriented solution. Being a private actor owned by the companies in the private sector, with detailed information about the various systems in the companies they advised, allowed KC to provide highly useful, tailored information and advice. Having organizations and institutions with detailed knowledge about the various companies and systems was considered a strength in the Norwegian context. This illustrates the value of having SRM and capacities with in-depth knowledge of their specific sectors.

Both KraftCERT and the public authorities in Norway's energy sector were commended for taking a problem-solving approach, drawing on the strengths of one another. The state authorities (NVE) had allocated to KraftCERT clearly defined and formalized responsibilities within the public framework, ensuring that they could reap the benefits of being a representative of the 'state' while maintaining their close ties to companies in the sector. Being integrated into the public framework was considered particularly useful with regard to international organizations and companies, as it gave KraftCERT greater access and authority. KraftCERT was also integrated with Norwegian national authorities like NorCERT, ensuring that their capabilities and knowledge fed into the situational awareness held by the public authorities. Interviewees described this approach to public–private cooperation in preventing incidents as a 'hybrid', and it was widely seen as positive.

Good Practice: Data-driven publications

In the UK the NCSC published several data-driven reports on the efforts of its public bodies and the scale of cyber threats. The rationale behind this practice was to alter the risk assessments of private companies through fact-based publications. Further, the NCSC used social media and public channels in seeking to reach SMCs. Improving baseline security for smaller companies was highlighted as particularly challenging, and practices targeting this segment were recognized as being of crucial importance.

Supply chains as a complex transnational issue

Some issues are difficult or impossible to solve at the level of the individual company or state. One major concern raised in the interviews related to the difficulties in managing global supply chains. Where the manufacturing market was cornered by monopolies or near-monopolies, individual companies had limited ability to address problems arising from supply chains. This issue fell into two categories: concerns with the geopolitical implications of relying on equipment from foreign companies, and concerns with suppliers and manufacturers that failed to deliver equipment that met the required high standards.

Current situation:

The geopolitical implications have been most clearly expressed in the ongoing debate over Huawei in the 5G networks and the unease stemming from possible misuse of this equipment. The increasing criticality of digital equipment has made ownership of suppliers a possible strategic asset, an issue difficult to address within a public–private framework (Lysne 2017; Brekke & Døvik 2019). This is particularly the case for telecommunication providers, but energy sector interviewees also expressed similar concern at being forced to take geopolitical decisions as private companies.

Even when supply chains did not represent a geopolitical challenge, they could pose a security problem. A familiar problem in digital supply chains is the difficulty of holding suppliers responsible for the products they manufacture. Companies buying digital equipment have limited means of securing inherently insecure devices, and the companies producing these devices are not always motivated to improve their security (Anderson & Moore 2006). Several interviewees mentioned instances where suppliers provided security features that were excellent immediately after purchase but deteriorated over time. The serious issue of convincing suppliers to raise their security standards could prove difficult, necessitating other solutions. This problem was nothing new. Respondents in the energy sector noted their reliance on outdated equipment as the most severe vulnerability, forcing them to build security around inherently vulnerable SCADA equipment and other ICSs.

Good Practice: Integrating suppliers in exercises and forums

No state could claim to have 'solved' the issue of supply chain security, and the issue is too complex to be distilled into any single practice. One frequently mentioned challenge concerned the difficulty

in getting suppliers to understand the criticality of their products, and the possible consequences of a failure. An approach taken by the Finnish NESA involved integrating suppliers and private security companies in exercises and forums, to improve awareness and underline their responsibility. This was widely considered as a positive practice. As supply chains and vendor security become a more prominent security issue, raising awareness and improving their security will benefit societal security.

The need for international collaboration

Further, several interviewees called for greater regional cooperation, to enable the pooling of competencies and resources, as well as leveraging the greater combined market power. Although cooperation was viewed favourably by most respondents it was not highlighted as a key component in public strategies: and that may indicate a lacuna in public frameworks.

In responding

While several issues remain, prevention was highlighted as a strong point in the Norwegian approach. However, managing crisis was perceived as far more problematic. As mentioned, the fact that most critical infrastructures are in private hands has led to competencies residing in the private sector as well. Both Finland and Norway have therefore focused on utilizing private competencies in a whole-of-society manner. How this cooperation will work in times of possible crisis and escalating political tensions is a crucial question. Preparing for worst-case scenarios and crisis is an important facet of CNI protection, and an area where public–private cooperation might be tested.

How to detect and classify an incident?

A crucial point in responding – especially considering the rising concern with hybrid warfare[6] and the accumulation of smaller incidents into threats to societal security – is to maintain overarching situational awareness of ongoing incidents. This issue can be further separated into two sub-issues: having insufficient sources of information; and the fragmented approaches to classifying and making sense of that information.

---

[6] See Reichborn Kjennerud & Cullen 2016

The current situation:

Regarding the first issue, concerns were raised regarding the ability of NSM/NorCERT to gather enough information about the state of affairs in Norway. Main inputs informing their situational awareness were public sources, the VDI cooperation, cooperating organizations internationally and nationally, as well as information shared by various companies either directly or through sector capacities. In addition, respondents differed greatly in their perceptions of the utility of involving the police in managing events. With the establishment of the Cyber Crime Centre the police might take a more prominent role, but the extent to which police resources were side-lined in responding to incidents seemed puzzling.

By comparison, the body responsible for maintaining the overall awareness in Finland, the National Cyber Security Centre, had the same sources of information available, and additionally served as the supervisory and regulatory body for the telecommunications sector, hosting various information sharing forums. In the Finnish context, the flow of information towards the public authorities was viewed more favourably, allowing for greater situational awareness. In the UK, the National Cyber Security Centre (NCSC) relied on a range of sources, including independent monitoring systems, private company reporting and intelligence cooperation within the Five Eyes framework. However, the UK NCSC is placed within the GCHQ: and this largely intelligence-driven approach is not necessarily comparable with the Nordic countries.

Regarding the second issue, the Norwegian approach puts considerable emphasis on classifying and responding to events at the level of the company and the SRM (NSM 2018). By placing incident classification at such a low level, a potential problem could be misclassification of events and/or basing the classification on partial information. This was regarded as most serious in events where identifying the wider societal risks was difficult – for instance, if the ramifications extended beyond the companies or sectors themselves. This latter point was mentioned as a particular challenge for telecommunications providers.

Good practice: Information Exchange Points

With a similar approach and structure for responding to digital security, the ability of the Finnish cyber security centre to gather relevant information is roughly comparable to that in Norway. One practice highlighted in Finland concerned the Information Exchange

Points for the different sectors. These forums were hosted in the NCSC and allowed for exchange of information between the sector bodies and the national authorities, helping to ensure that the knowledge and information in industry verticals is more closely integrated with the national authorities. While this work is mainly preventive, it also serves to promote relationships and closer collaboration between individual companies and the national authorities, which was considered advantageous in connection with response. Among the reasons identified for their success was building them on trust and personal relations, as well as hosting them frequently, up to six or seven times a year. A final point of emphasis was engagement at the management level as well as with the dedicated security personnel. With the establishment of the Cyber Centre in Norway similar initiatives might be under development, but at the time of writing this has not been settled.

Good practice: Triage system

The UK NCSC holds the responsibility for classifying any incident reported to or discovered by them in cooperation with the National Crime Agency, providing a uniform system for classification across the UK. Experience from the UK indicates that a coherent national framework for responding to incidents could be advantageous when assisting companies in classifying incidents and determining the appropriate level of response. Several perceived benefits were mentioned in interviews, including greater situational awareness, rapid and accurate responses as well as consistency across incidents. Also mentioned was the ease of cooperating with other states that have similar classification schemes, as perceptions and interpretations did not have to be translated.

How to organize a response?

Another question concerned the crisis-response mechanisms that had been put in place if a larger event was to take place. This question had two distinct sub-components. The first issue raised was the lack of an established centralized institution to take the lead in the event of a crisis, rather than ad-hoc solutions or forums that were convened only when a crisis had occurred. The second sub-component involves the integration of private capacities in national crisis-response mechanisms, in order to leverage as many resources as possible.

The current situation:

The lack of a centralized institution was identified as a key problem in Finland, explicitly mentioned as a matter the revised cyber strategy

was intended to address (O'Dwyer 2018). For Norway, the large number of institutions and organizations involved in providing cyber security was viewed unfavourably by several interviewees, as was the issue of fragmentation and unclear responsibilities. In the UK, placing cyber security within one organization was considered advantageous, as it pooled available resources and simplified their roles in the event of a crisis.

As noted, the UK struggled to a greater extent in integrating civil society in providing societal security yet regarded its cooperation with the private sector to be largely satisfactory (Collier 2016). In this regard the Nordic states had an advantage in the more cooperative spirit and willingness to collaborate on a voluntary basis, a point frequently mentioned as a source of strength in both countries. However, Norwegian respondents in the private sector were critical to this wider approach, arguing that the response mechanisms were inadequate, ad-hoc and that they were not prepared.

Good practice

Finnish respondents expressed greater confidence in the cooperation, which indicates that Finland has come further in this endeavour. Various rationales were given for this, including the more exposed geopolitical situation of the Finnish state, as well as its non-membership in NATO. Whatever the cause, the implication remains: the tradition of societal security is more entrenched in Finland, and that the integration of private companies in providing cyber security has progressed further. Formally integrating private competencies into the national framework, as well as having exercises and shared understandings, was proposed as a means of better integrating these resources. Although not distilled into any clear policy or best practice, the ability to utilize private companies in the provision of cyber security is clearly of great importance to smaller states.

Who ensures that response capacities are adequate?

A further difficulty that can limit the ability to respond to incidents is the lack of national capacity. Such lack of relevant competencies and resources was noted in all three countries, but the limitations in responding to this issue were more severely felt in Finland and Norway. This points towards a main problem facing small, highly digitalized countries: the capacity to build sufficiently large, specialized work forces to meet the challenges of cyber security. States with a low resource base may struggle to cover all niches of cyber security. Ensuring that the available competencies cover the spectrum of digital challenges and also

have in-depth knowledge of every issue was considered impossible. This is particularly acute when the existing competencies are fragmented and located across a multitude of organizations, perhaps resulting in overlapping instead of complementary skill-sets.

The current situation:

A case from the protection of Industrial Control Systems in Norway can illustrate the challenge: While politically motivated attacks on industrial systems remain rare, they do occur as illustrated in the Trisis case. In this sense having the ability to manage security incidents in industrial systems is not just a company responsibility: it could be a matter of national security. KC remains the leading ICS resource in Norway, but it is scaled to the level of information sharing and advice, with only a handful of employees. This makes sense as KC is run as a private business, but at the societal level the lack of an operational resource able to assist in the event of a serious attack on ICS is a real concern. Barring incentives from the public authorities, private companies will continue to scale their operations to protect their systems within a reasonable acceptance of risk. For business-as-usual this is probably enough, but questions should be asked about its adequacy in crisis situations.

The responsibility for answering questions such as what capacities are sufficient, who should be tasked with holding those capabilities – and, not least, who pays for ensuring that CNI can be kept functioning in times of crisis – remains unclear. The same can be said for the fundamental question of what capabilities a small state like Norway can realistically maintain on its own, and how to deal with such issues where national capacities are inadequate.

The need for regional collaboration

The interviews did not result in any clear-cut best practices for addressing the problem, but Nordic cooperation was the most frequently mentioned suggestion. Almost all respondents considered it advantageous to pool the resources among similar and like-minded states. As the Nordic states are all small, highly dependent on digital services and faced with the same challenge of developing sufficient workforces, greater cooperation should be pursued in order to foster niche communities in cyber security. There are numerous existing initiatives on a Nordic level, the NordBER cooperation for the energy sector being a prominent example, but respondents argued that there remained underutilized potential for closer collaboration (NVE 2019)

Conclusions

This report has examined the approaches to, and organization of, cyber security in the UK, Finland and Norway, using the energy and telecommunications sectors as cases. The initiatives and approaches taken in all three states underline the crucial importance and the difficulties of providing cyber security as regards critical infrastructure. Broadly speaking, the three states have been similar in their approaches: all three have involved private companies and resources; all three face possible transnational threats that necessitate international efforts; and all three highlighted the complicated and evolving nature of cyber threats. The main dividing line runs between the UK and the two Nordic countries. The difference here lies not in the level of state involvement, but in the contrast between the intelligence-led centralized approach of the UK, and the whole-of-society approach of the two Nordic states.

The primary finding of this report is the importance of accounting for national differences and peculiarities when providing cyber security. Arguing that any given state has 'better' cyber security than others is a futile exercise. Rather, all states should realize the benefits and pitfalls of their national approaches, and tailor policies and initiatives to expand on strengths and mitigate the most pressing shortfalls. A clear distinction in this regard concerns the consequences of smaller size and high levels of trust: respondents in Norway and Finland highlighted how smaller size and institutional trust resulted in less friction in the collaboration between public authorities, private companies and the civil sector. Leveraging the small-state tradition of greater trust and cooperation is a competitive advantage that should be pursued. Some ways to expand trust and cooperation include structuring cooperation through formalized agreements and meetings, as well as allowing for greater sharing of threat assessments and intelligence.

However, smaller size puts also emplaces clear restrictions on the ability of the state to intervene, provide relevant guidance and deal with incidents. This challenge is particularly pressing as regards the many 'niches' of cyber security, like industrial control systems. This points towards another topic examined in this report: regional and European cooperation. While initiatives are being implemented at the European level, they are generally too recent or to limited to have had significant impact. All the same, cooperation and collaboration are essential for smaller states, and the trend is towards closer and more extensive

European collaboration on these issues. Until such European efforts are in place, however, calls for greater Nordic collaboration will definitely remain relevant.

Regarding Norway, there were noticeable differences between preventing and responding to incidents. Among our respondents, perceptions of the former were uneven, but broadly favourable. Trust and widespread mutual understanding were highlighted as strong points but providing mutual benefits for private-sector companies was seen as more challenging. This does not necessarily mean costly state interventions; it could involve simple practices such as filtering information and intelligence down to actionable and relevant inputs. In sum, work on preventing incidents was viewed far more positively than the ability to respond. There were widespread concerns that incidents would fly below the radar, and that possible responses would be fragmented and insufficient. Proving or disproving such claims is exceptionally difficult, but the number of concerns indicate that the problem should be taken seriously. Numerous initiatives are either underway or under development and might address these shortcomings. This report can offer little more than a snapshot of the current situation. Putting efforts into tackling cyber insecurity in a broader context is likely to remain useful. As all three states analysed had developed novel and innovative solutions to what were frequently similar issues, continued learning and exchange of experiences remains a fruitful exercise.

References

Anderson, R. & Tyler Moore (2006): 'The economics of information security', Science, 314 (5799): 610–613

Bing, Chris (2018): 'Trisis has the security world spooked, stumped and searching for answers', Cyber Scoop 16.01.2018. https://www.cyberscoop.com/trisis-ics-malware-saudi-arabia/, accessed 05.03. 19

Bossong, Raphael & Ben Wagner (2016): 'A typology of cybersecurity and public–private partnerships in the context of the EU', Crime, Law and Social Change, 67 (3): 10-14

Carr, Madeline (2016): 'Public–private partnerships in national cyber-security strategies', International Affairs, 92 (1): 43–62

Christensen, Kristoffer Kjærgaard & Karen Lund Petersen (2016): 'Samarbejde bygget på forskellighed: Anbefalinger til offentlig–privat samarbejde om IKT-sikkerhed', University of Copenhagen Report https://polsci.ku.dk/ansatte/vip/?pure=da%2Fpublications%2Fsamarbejde-bygget-paa-forskellighed(a2d04447-27da-43b1-8823-fdac54bb52dd).html

Christensen, Kristoffer Kjærgaard & Karen Lund Petersen (2017): 'Public–private partnerships on cyber security: a practice of loyalty', International Affairs, 93 (6): 1435–1452

Demchak, Chris (2012): «Cybered Conflict, Cyber Power, and Security Resilience as Strategy', in Derek S. Reveron (ed), Cyberspace and National Security. Washington DC: Georgetown University Press

Dewar, Robert S. (2018): 'National Cyberdefence Policy Snapshot – United Kingdom', in Robert S. Dewar (ed), National Cybersecurity and Cyberdefence Policy Snapshots, Zurich: http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports_National_Cybersecurity_and_Cyberdefense_Policy_Snapshots_Collection_1.pdf

Direktoratet for samfunnssikkerhet og beredskap (DSB) (2019): Analyser av Krisescenarioer 2019, https://www.dsb.no/rapporter-og-evalueringer/analyser-av-krisescenarioer-2019/, accessed 05.03. 19

Direktoratet for samfunnssikkerhet og beredskap (DSB) (2019): 'About DSB', DBS.no. https://www.dsb.no/menyartikler/om-dsb/about-dsb/, accessed 12.03. 19

Dragos (2017): Trisis Malware – Analysis of Safety System Targeted Malware, https://dragos.com/wp-content/uploads/TRISIS-01.pdf accessed 05.03.19

Dragos (2018): Xenotime, https://dragos.com/resource/xenotime/, accessed 05.03. 19

Dunn Cavelty, Myriam & Manuel Suter (2009): 'Public–Private Partnerships are no silver bullet: an expanded governance model for Critical Infrastructure Protection', International Journal of Critical Infrastructure Protection 4 (2): 179-187

E24 (2017): 'Nytt senter mot cyberangrep', 29.03.2017. https://e24.no/digital/norge/nytt-senter-mot-cyberangrep/23961486, accessed 05.03. 19

Electronic Communications Resilience & Response Group (EC-RRG) (2011): 'Telecommunication Networks – a vital part of the Critical National Infrastructure', https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61335/telecommunications_sector_intro.pdf

Eder, Florian, Andrew Gray & Stephen Brown (2019): 'German CDU chief: Europe must adapt to survive', Politico.eu, 08.02.2019, https://www.politico.eu/article/german-conservative-cdu-leader-annegret-kramp-karrenbauer-europe-must-adapt-to-survive-christian-democratic-union/, accessed 05.03. 19

Egloff, Florian (2017): 'Cybersecurity and the Age of Privateering' in George Perkovich & Ariel E. Levite (eds), Understanding Cyber Conflict: Fourteen Analogies: 231–247, Washington DC, Georgetown University Press

Energy Authority Finland (2018): 'National Report 2018 to the Agency for the Cooperation of Energy
Regulators and to the European Commission', https://www.energiavirasto.fi/documents/10191/0/National+Report+2018+Finland+1411-480-2018_20180726.pdf/10b8e538-2eef-4e97-8629-aafd4ad9ee02

European Commission (2016): Directive 2016/1148 on security of network and information systems (NIS Directive), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC accessed 05.03. 19

European Commission (2016): Regulation 2016/679 (General Data Protection Regulation), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

European Commission (2018): Cybersecurity Act, 11.12.2018. https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en, accessed 05.03. 19

Fingrid (2019): 'Electricity Systems of Finland', available at: https://web.archive.org/web/20190321132406/https://www.fingrid.fi/en/grid/electricity-system-of-finland/

Finnish Ministry of Foreign Affairs (2019): 'Cyber security and the cyber domain', at https://um.fi/cyber-security-and-the-cyber-domain, accessed 06.03.19

FireEye (2017): Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure, https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html, accessed 05.03.19

FireEye (2018a): 'Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure', 14.01.2017. https://www.fireeye.com/blog/threat-research/2017/12/attackers-deploy-new-ics-attack-framework-triton.html, accessed 04.03.19

FireEye (2018b): TRITON Attribution: Russian Government-Owned Lab Most Likely Built Custom Intrusion Tools for TRITON Attackers, https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html, accessed 05.03. 19

Greenberg, Andy (2018): 'The Untold Story of Notpetya, The Most Devastating Cyberattack in History', Wired, 08.22.2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/, accessed 04.03.19

The Grugq (2017): Internet of Wilderness of Mirrors – Why is WannaCry? https://medium.com/@thegrugq/internet-of-wilderness-of-mirrors-9eaa24bd99d8, accessed 05.0.19

The Guardian (2017): 'What is WannaCry ransomware and why is it attacking global computers?', 12.05.2017. https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20, accessed 05.03.19

Harknett, Richard J. & James A. Stever (2009): 'The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen', Journal of Homeland Security and Emergency Management, 6 (1): article 79

Haugli, Mina, Hilde Nilsson Ridola, Hanne Bjørdal Roald & Arne Kristian Gansmo (2019): 'Avinor: Dataproblemene er løst', NRK.no, 08.02.2019. https://www.nrk.no/ostlandssendingen/avinor_-dataproblemene-er-lost-1.14420969, accessed 02.03.19

Herrington, Lewis & Richard Aldrich (2013): 'The Future of Cyber-Resilience in an Age of Global Complexity', Politics, 33 (4): 299–310

HM Government (2015): 'National Emergency plan for the Telecommunications Sector', https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/61807/emergency-plan-telecomms-sector.pdf

HM Government (2016): National Cyber Security Strategy 2016–2021 https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

HM Government (2017): Energy Statistics 2017, https://web.archive.org/web/20190321131853/https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/736151/Ch1.pdf

International Energy Agency (IEA) (2017): 'Norway 2017 Review', https://www.iea.org/publications/freepublications/publication/EnergyPoliciesofIEACountriesNorway2017.pdf

International Energy Agency (IEA) (2018): 'Finland 2018 Review', https://webstore.iea.org/download/summary/2372

Kaspersky (2016): 'Threat Intelligence Report for the Telecommunications Industry', https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07185213/Kaspersky_Telecom_Threats_2016.pdf

Kello, Lucas (2017): The Virtual Weapon and International Order, New Haven, CT: Yale University Press

Klimburg, Alexander (2011): 'Mobilising Cyber Power', Survival, 53 (1): 41–60

Klimburg, Alexander (2017): The Darkening Web – The War for Cyberspace, New York, Penguin Press

Krebs, Brian (2018): 'Posts tagged: Mirai Botnet', https://krebsonsecurity.com/tag/mirai-botnet/

Kriz. Danielle (2017): 'A Global Model: UKs 'National Cyber Security Strategy', SecurityRoundtable.org, https://www.securityroundtable.org/global-model-uks-national-cyber-security-strategy/

Libicki, Martin C. (2009): Cyberdeterrence and Cyberwar, Santa Monica, CA: RAND Corporation

Lovdata (2018): 'Lov om nasjonal sikkerhet (Sikkerhetsloven)', https://lovdata.no/dokument/NL/lov/2018-06-01-24

Lovdata (2019): 'Forskrift om sikkerhet og beredskap i kraftforsyningen (kraftberedskapsforskriften)', https://lovdata.no/dokument/SF/forskrift/2012-12-07-1157

Levy, Ian (2018): Active Cyber Defence – One Year On, 05.02.2018 https://www.ncsc.gov.uk/blog-post/active-cyber-defence-one-year

Moret, Erica & Patryk Pawlak (2017): 'The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?', Policy Brief. Paris: European Union Institute for Security Studies

Muller, Lilly Pijnenburg (2016): 'Makt og avmakt i cyberspace: hvordan styre det digitale rom? ', Internasjonal Politikk, 74 (4): 1-23

Nasjonal Kommunikasjonsmyndighet (NKOM) (2015): 'Årsrapport 2015'. https://www.nkom.no/aktuelt/rapporter/_attachment/22915?_ts=1537ee974f3

Nasjonal Kommunikasjonsmyndighet (NKOM) (2017): 'Robuste og sikre nasjonale transportnett – målbilder og sårbarhetsredusernde tiltak', 07.04.2017. https://www.nkom.no/teknisk/sikkerhet-og-beredskap/ekomsikkerhet/nkom-foresl%C3%A5r-omfattende-tiltak-for-mer-robuste-fiberveier-i-og-ut-av-norge/_attachment/28565?_ts=15ba9c519ef

National Cyber Security Centre (NCSC) (2018): Annual Review 2018 – Making the UK the safest place to live and work online https://www.ncsc.gov.uk/404

National Security Authority (2018): 'NSM etablerer nasjonalt cybersikkerhetssenter', 13.08.2018, https://nsm.stat.no/aktuelt/nsm-etablerer-nasjonalt-cybersikkerhetssenter/

National Security Authority (2019): 'Felles cyberkoordineringssenter (FCKS)', https://web.archive.org/save/https://www.nsm.stat.no/NCSS/ncss-om/felles-cyberkoordineringssenter-fcks/

National Security Risk Assessment UK 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62484/Factsheet2-National-Security-Risk-Assessment.pdf

NATO Cooperative Cyber Defence Centre of Excellence (2017): Tallinn Manual 2.0. On The International Law Applicable to Cyber Operations, second edition, New York: Cambridge University Press

NorSIS (2019): 'Politiets Nasjonale cyberkrimsenter er åpnet', 28.01.2019. https://norsis.no/politiets-nasjonale-cyberkrimsenter-nc3-er-apnet/, accessed 05.03.2019

Norwegian Government (2012): 'Cyber Security Strategy for Norway', https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/cyber_security_strategy_norway.pdf

Norwegian Government (2018): 'Høring – Forslag til ny lov om Etterretningstjenesten, 12.11.2018. https://www.regjeringen.no/no/dokumenter/horing---forslag-til-ny-lov-om-etterretningstjenesten/id2618620/

Norwegian Government (2019): 'Nasjonal strategi for digital sikkerhet', 30.01.2019. https://www.regjeringen.no/no/dokumenter/nasjonal-strategi-for-digital-sikkerhet/id2627177/

Norwegian Ministry of Defence (2014): 'Forsvarsdepartementets retningslinjer for informasjonssikkerhet og cyberoperasjoner i forsvarssektoren', https://www.regjeringen.no/globalassets/upload/fd/dokumenter/fdsretningslinjercyberoperasjoner.pdf

Norwegian Ministry of Foreign Affairs (2017): 'International cyber strategy for Norway', https://www.regjeringen.no/globalassets/departementene/ud/dokumenter/sikpol/cyberstrategy_2017.pdf

Norwegian National Intelligence Service (NIS) (2019): Fokus 2019, https://forsvaret.no/fokus

NOU 2015: 13 'Digital sårbarhet – sikkert samfunn' (Lysne 1), https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/pdfs/nou201520150013000dddpdfs.pdf

NOU 2018: 14 (2018): 'IKT-sikkerhetsutvalget', https://www.regjeringen.no/no/dokumenter/nou-2018-14/id2621037/

NSM (2018): Rammeverk for håndtering av IKT-sikkerhetshendelser. : https://web.archive.org/web/20190307142818/https://nsm.stat.no/globalassets/dokumenter/vedlegg-til-rammeverk-for-handtering-av-ikt-hendelser/rammeverk-for-handtering-av-ikt-sikkerhetshendelser.pdf

NVE (2016): Network Regulation, : https://web.archive.org/web/20190321131629/https://www.nve.no/energy-market-and-regulation/network-regulation/

NVE (2018): Informasjonssikkerhetstilstanden i energiforsyningen, https://web.archive.org/web/20190321125753/http://publikasjoner.nve.no/rapport/2017/rapport2017_90.pdf

NVE (2019): Beredskapssamarbeid, https://www.nve.no/damsikkerhet-og-kraftforsyningsberedskap/kraftforsyningsberedskap/organisering-av-kraftforsyningsberedskap/beredskapssamarbeid/

Nye, Joseph S. (2017): 'Deterrence and Dissuasion in Cyberspace' International Security, 41 (3): 44–71

OFGEM (2019): 'Electricity', https://web.archive.org/save/https://www.ofgem.gov.uk/electricity

Police Act (1995). https://lovdata.no/dokument/NL/lov/1995-08-04-53

Prime Minister's Office (2018): 'Hovedprinsipper i beredskapsarbeidet', for regjeringen.no, 28.09.2018. https://www.regjeringen.no/no/tema/samfunnssikkerhet-og-beredskap/innsikt/hovedprinsipper-i-beredskapsarbeidet/id2339996/ accessed 12.03.2019

Prop. 151S (2015–2016): 'Kampkraft og bærekraft – Langtidsplan for forsvarssektoren' https://www.regjeringen.no/contentassets/a712fb233b2542af8df07e2628b3386d/no/pdfs/prp201520160151000dddpdfs.pdf

Rid, Thomas (2013): Cyber War Will Not Take Place, New York: Oxford University Press

Rid, Thomas & Ben Buchanan (2014): 'Attributing Cyber Attacks', Journal of Strategic Studies, 38 (1–2): 4–37

Sahel, Jean-Jacques (2016): 'Multi-stakeholder governance: a necessity and a challenge for global governance in the twenty-first century', Journal of Cyber Policy, 1(2): 157-175

Sanger, David E. (2018): The Perfect Weapon, New York: Crown Publishers

Schneier, Bruce (2017): 'WannaCry and Vulnerabilities', Schneier on Security, 02.06.2017. https://www.schneier.com/blog/archives/2017/06/wannacry_and_vu.html, accessed 05.03.19

Secretariat of the Security Committee (2013): Finland's Cyber security Strategy. https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

Singer, P. W. & Allan Friedman (2014): Cybersecurity and Cyberwar – What Everyone Needs to Know, New York: Oxford University Press

Slowik, Joseph (2018): 'Evolution of ICS Attacks and the Prospects for Future Disruptive Events', Dragos.com. https://web.archive.org/web/20190321130133/https://dragos.com/wp-content/uploads/Evolution-of-ICS-Attacks-and-the-Prospects-for-Future-Disruptive-Events-Joseph-Slowik-1.pdf

Smith, Don C (2018): 'Enhancing cybersecurity in the energy sector: a critical priority', Journal of Energy & Natural Resources Law, 36 (4): 373–380

Statnett (2019): About us, https://web.archive.org/web/20190321131504/https://www.statnett.no/en/About-Statnett/

Supo (2018): National Security Review 2018, https://www.supo.fi/www.supo.fi/brochures/1/1/supo_s_national_security_review_2018_76778

Symantec (2017): WannaCry: Ransomware attacks show strong links to Lazarus group, https://www.symantec.com/connect/blogs/wannacry-ransomware-attacks-show-strong-links-lazarus-group, accessed 05.03. 19

Tanczer, Leonie Maria, Irina Brass & Madeline Carr (2018): 'CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy', Global Policy, 9 (3): 60-66

Telenor (2018): 'Digitale trusler krever mer enn dugnadsinnsats', https://www.telenor.no/om/digital-sikkerhet/digitale-trusler-krever-mer-enn-dugnadsinnsats.jsp

Traficom (2019): 'E-Service Statistics Database', https://www.traficom.fi/en/statistics-and-publications/statistics

UK National Audit Office (2017): Investigation: WannaCry cyber attack and the NHS, https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf

United States Department of Justice (2018): U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations, 04.10.2018. https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and-disinformation-efforts

Von Solms, Rossouw & Johan van Niekerk (2013): 'From information security to cybersecurity', Computers & Security 38: 97–102

Wiedeman, Reeves (2018): 'Gray Hat', Nymag.com 19.02.2018. http://nymag.com/intelligencer/2018/03/marcus-hutchins-hacker.html, accessed 04.03.2019

Zetter, Kim (2014): Countdown to Zero Day, New York: Crown Publishers

Zetter, Kim (2015): 'A cyberattack has caused confirmed physical damage for the second time ever', for Wired, 01.08.2015. https://web.archive.org/web/20190312145415/https://www.wired.com/2015/01/german-steel-mill-hack-destruction/

Norwegian Institute of International Affairs

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from short-term applied research to more long-term basic research.

About the author:

Lars Gjesvik is a research assistant in the Research group for Security and Defence, working mainly on cybersecurity.
He is a master student in political science at the University of Oslo, and has studied international studies and history. His research interests are cybersecurity and cyber warfare.

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PB 7024 St. Olavs Plass, 0130 OSLO
www.nupi.no | post@nupi.no