Organizational aspects of ICT security policy in Norway:

Challenges of specialization and coordination

Mikael Østhus Schärer

Master's thesis in political science

Department of political science,

University of Oslo

Spring 2019

Words: 34617

Organizational aspects of ICT security policy in Norway:

Challenges of specialization and coordination

2019

Organizational aspects of ICT security policy in Norway:
Challenges of specialization and coordination

Mikael Østhus Schärer

https://www.duo.uio.no/

Print: Reprosentralen, Universitetet i Oslo

Summary

This thesis is an analysis of the Norwegian government's ICT security policy since the 1990s until 2018. ICT security is viewed as a subfield within the larger public security field. The study therefore emphasizes aspects within the civil sector. The thesis is based on the following research question: *What are the major organizational trends in the central government's ICT security policy since 1990s until 2018? How can instrumental, cultural-institutional and neo-institutional theory explain these trends?* The methodical approach is theoretical interpretative case-study. The data-collection and analysis are founded upon content analysis of public documents. The primarily sources are Official Norwegian Reports, Auditor General reports, government white papers, royal resolutions, and information security strategies.

The study finds four major trends: 1) The central government has been organized according to two contradictory principles since mid-1990s. 2) Coordination of ICT security policy at ministry level was enforced by two actors from 1997 until 2013. 3) The key ICT security agency (NSM) uniquely operates in the interface of the military and civil sector. 4) ICT security policy is characterized by slow developments, but the policy field has gradually developed in direction of stronger lead organizations (MoJ and NSM).

The instrumental expectations are to a large degree confirmed as organizational solutions offer more horizontal coordination in response to the problem of fragmentation. However, the analysis indicate that the problem of ICT security is too complex to manage without turning to complex and hybrid organizational solutions that are filled with tensions. Ministerial responsibility as the primary organizational principle of the central government promote conflict of interest and cultural resistance against strong coordination policies centered at Ministry of Justice (MoJ). It has led to weak horizontal coordination mechanisms since the 1990s. However, with the increased coordination authority in 2017, the institutional balance between ministerial responsibility and cross-sectoral coordination substantially shifted towards a more hierarchical model. The development of MoJ as lead ministry must be considered as a gradual transformation and in line with Joined-up government reform strategies. Also, the myths of coordination and of MoJ as lead ministry have been reoccurring themes. The re-design of National Security Authority (NSM) in the early 2000s seems to follow instrumental thinking as it concentrated capabilities into one civil-military hybrid which promote holistic approach to ICT security across military, civil government and private sectors. The further development of NSM seems to follow the institutional framework put in place in the early 2000s.

Preface

First and foremost, I want to thank my supervisor Tom Christensen for your thoughtful input and feedback. However, your help extends our meetings and email correspondence. Your enormous amount of research publications has also been an important source of guidance to my work with this thesis.

I also want to thank all the lectures and fellow students throughout the years in Trondheim and Oslo for making the university to such a great place. And, to SAIH for all the friendships and for putting politics and organization into real-life experiences.

My mother and father deserve their thanks for all the support over the years, and in particular these last few months.

To write the thesis in English has proved more difficult than I first imagined. The choice was made in the spirit of making information and knowledge available across national and language borders. And, to improve my own skills. I want thank Lars Vingelsgård for the help with grammar these final weeks.

I take full responsibility for the content and any faults or errors.

Mikael Østhus Schärer

Tynset, May 15, 2019

Abbreviations

* Norwegian name in parenthesis

CCIS – Coordination committee for information security (Koordineringsutvalget for informasjonssikkerhet)

DSB – Directorate for Civil Protection (Direktoratet for Samfunnssikkerhet og Beredskap)

MoD – Ministry of Defense (Forsvarsdepartementet)

MoI&T – Ministry of Industry and Trade (Nærings- og handelsdepartementet)

MoJ – Ministry of Justice and Public Security, before 2011: Ministry of Justice and Police (Justis- og beredskapsdepartementet / Justis- og politidepartementet)

MoR&A – Ministry of Renewal and Administration (Fornyings- og administrasjonsdepartementet)

MoT&C – Ministry of Transportation and Communication (Samferdselsdepartementet)

Nkom – Norwegian Communications Authority, former Post and Telecommuncations Authority – PTT (Nasjonal kommunikasjonsmyndighet / Post- og teletilsynet)

NSM – National Security Authority (Nasjonal sikkerhetsmyndighet)

Table of contents

Figures and tables

1. Introduction

1.1 Topic

In recent years have 'ICT security' been given more attention by and become a more evident subfield within public security policy in Norway. The 2015 Norwegian Official Report on digital vulnerabilities and the following white paper on ICT security in 2017 are hallmarks of this development. ICT security most been seen in relation to the radical development of digital information and communication technologies (ICTs) like computer systems, internet and telecommunications, and its comprehensive diffusion into Norwegian society. As the 2017 white paper puts it, it is easier to be in contact with each other, access information, and society's value creation and growth is fundamentally dependent on digital technologies (St. Meld., nr 38 (2016-2017), p. 11).

This development has also transformed society's vulnerabilities. Only within the last year we have seen unwanted digital occurrences at several County governor offices (NRK, 2018), Health South-East, Norway's largest regional health administration (NRK, 2019) and AVINOR, stopping all flights nationally for several hours (ABC Nyheter, 2019). Internationally, the 2017 Wannacry worm that among others hit the National Health Service in the UK and led to more than 19000 cancelled appointments (The Telegraph, 2018), are an illuminating example of how digital technology have transformed the vulnerabilities of modern society.

ICT security policy, like most of public security policy, deals with issues that are often characterized as wicked problems. Wicked problems are associated with multiple stakeholders, organizational complexity, ambiguity, and scientific uncertainty (Head, 2008; Head & Alford, 2015; Rittel & Webber, 1973). These problems are of transboundary nature because they go across organizational entities, sectors and possibly even national borders. Welfare and environmental policies are examples of other policy fields that deals with wicked problems. By definition, wicked problems do not have perfect solutions. However, coordination and collaboration are viewed as key components to address these complex issues (Head & Alford, 2015). Since government capacity, organizational solutions, coordination and collaboration are at center when facing wicked problems, the research tradition of public administration and management are an appropriate analytical approach to policy field of ICT security.

Public security policy has received increased attention during the last ten years by the research community of public administration and management. Prominent works are Fimreite, Lango, Lægreid and Rykkja's (2014) *Organisering, samfunnssikkerhet og krisehåndtering*,

Lægreid and Rykkja's (2018) *Societal security and crisis management*, together with a range of articles (f. ex. Christensen, Lægreid & Rykkja (2018) on the police reform, Christensen, Lægreid & Rykkja (2018) on the national police emergence response center, and Lægreid & Rykkja (2015) on coordination arrangements). *Organisering, samfunnssikkerhet og krisehåndtering* highlighted the problems of fragmentation, pulverization of responsibility and weak coordination mechanisms in public security. The authors argued that these problems illustrate a fundamental challenge with the Norwegian central government. It is difficult to establish strong coordination functions across government sectors. This was labelled "the eternal coordination problem" (Fimreite, Lango, Lægreid, & Rykkja, 2014, pp. 73-74). However, the subfield of ICT security policy and its organizational solutions, have not been a prominent part of these analysis. The ambition of this thesis is therefore to contribute to this research tradition and shed light on the organizational trends in Norwegian ICT security policy. Have the coordination problems of ICT security been similar to those of public security policy, and are these problems still manifest as of 2018?

From a public administration and management perspective the case of ICT security is especially interesting for two reasons. Firstly, ICT security highlights some different key organizations and arrangements that have not been much studied by previous public security research. For example, neither organizations within the police sector nor the Directorate for civil protection (DBS), with its many responsibilities for public security, are heavily involved. Secondly, ICT security was a new issue that the government had to handle during the 1990s and onwards. By contrast, other issues within the definition of public security are not particularly new (St. Meld., nr. 17 (2001-2002), p. 4). It is rather that issues like protection from natural disasters like floods, forest fires and pandemics, or intended threats like sabotage and terrorism were brought together in the concept of public security that was new. Therefore, this case offers insight to how the Norwegian government have responded in face of a new problem within public security.

1.2 Research question and clarifications

The thesis asks the following questions:

- *What are the major organizational trends in the central government's ICT security policy since 1990s until 2018?*
- *How can instrumental, cultural-institutional and neo-institutional theory explain these trends?*

The term 'ICT-security' is used in this analysis because it is the term the government itself uses (St. Meld., nr 38 (2016-2017)). It is understood within the frame of public security because it is related to protection of critical infrastructure and functions within the civil sector. The term has overlapping qualities with concepts like information security and cyber security. 'Information security' usually refers to ensuring information or data's confidentiality, integrity and availability (NOU, 2006: 6), and can therefore be viewed as broader than my emphasis on critical infrastructures and functions. 'Cyber-security' is also a broader term, which is defined by the US Department of Defense as: "A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (Crowther, 2017, p. 63). Cyberspace was in 2016 included as a fourth domain by NATO along with the traditional land, air and sea (NATO, 2016). Hence, cyber security is more related to a military understanding of digital vulnerabilities, threats and risks.

In order to figure out what the major organizational trends are, I will direct my analysis towards the most prominent organizational features, arrangements policy changes by the central government to prevent intended or unintended breakdowns of critical digital infrastructure and functions. The central government includes both ministerial and agency level. The analysis will not only describe and explain each major feature and arrangement, these will be viewed in relation to each other, together with the development over time. By doing to, my aim is that I will be able to describe and explain these major trends. The analytic timeframe is set to 1990s until December 2018. The start of the timeframe is set to the 1990s so that the analysis can shed light on the introduction of the important coordination efforts and their culminating effects.

1.3 Theoretical approach

The organizational trends of the central governments ICT security policy is analyzed and explained based on theories of public management and administration. I have chosen the theoretical approach of public management and administration because of its ability to analyze administrative policies, organizational features and solutions. The main theories of public management and administration are instrumental and institutional theory, which is a separation that will be used in this analysis. Research on public management and administration have found several waves of different organizational thinking. These categorizations or paradigms assist the analysis of the major organizational trends in ICT security policy.

Instrumental theory is characterized by its emphasis on formal structure as the main

explanatory factor (Egeberg, 2012). Key components are hierarchy, division of labor and rules, regulations and procedures. These structures give organizational capacity and shape decision-making behavior. Instrumental theory views public organizations as problem-solvers based on a rational logic of consequence. Therefore, formal organizational solutions are used as instrumental tools or solutions to reduce problems (Christensen, Lægreid, Roness, & Røvik, 2009). Since ICT security policy are characterized as a wicked issue, a central instrumental expectation is that organizational measures will promote more collaboration and coordination to reduce this problem. Since the aim of this thesis is to describe and explain a number of organizational features and solutions to ICT security, the structural dimensions of vertical and horizontal specialization and coordination are essential to the analysis (Gulick, 1937; Egeberg, 2012). Based on these insights, central organizational settings and solutions is described assisted by organizational charts. The structural dimensions are also central in explaining direction of complexity and hybrid organizational features (Christensen & Lægreid, 2011).

Institutional theories are the second theoretical approach. Informal norms and the logic of appropriateness, path-dependency theory, gradual transformative change, and neo-institutional insights are the central elements to my institutional approach. Institutionalists do not dismiss that organizations are shaped by formal structures and rational thinking, but they highlight that organizations operate within a social and cultural context. Thus, are normative and cultural-cognitive elements also important explanatory factors (Scott, 2014).

Through a process of institutionalization are actors infused with values, attitudes and norms that influence their behavior (Selznick, 1957). Therefore, organizational solutions to ICT security are expected to be chosen based on what is considered culturally appropriate (March & Olsen, 1989; Olsen, 2007). Path-dependency theory stresses the enduring feature of institutional arrangements (Mahoney, 2000). This theory argues that the foundational years have long lasting impact because they create institutional paths which will be reproduced and difficult to change unless a critical juncture arises. For example, institutional arrangements created early in the analytical timeframe will be expected to have lasting impact. Streeck and Thelen's (2005) theory about gradual transformative change is used to contrast path-dependency's expectations that institutional change only either occur within the larger institutional path or through divergence to new paths because of critical junctures.

The neo-institutionalists are characterized by their constructivist view of the world, where social reality is not given, but a result of perception through symbolic interaction and sense-making. Therefore, organizations and actors are heavily influenced by the external framework and in search of legitimacy (Scott, 2014, pp. 66-69; Meyer & Rowan, 1977). This

theory basic assumption is that the institutionalized external environment holds cultural norms about what is legitimate ways of organizing. These norms are called *myths* (Christensen, Lægreid, Roness, & Røvik, 2009). Policymakers are expected to imitate other organizational solutions and prescriptions in search of legitimacy (DiMaggio & Powell, 1983). Since more coordination and collaboration are considered the best way to reduce the problems of wicked issues (Head 2008, Head & Alford 2013), I will expect organizational solutions to ICT security will be centered around myths about coordination and collaboration. Based on Brunsson (2006), more talk about coordination and collaboration (myths) are greater than actual implementation.

Lastly, I will use four conceptualizations about public management and administration paradigms to assist the analysis of the organizational trends of ICT security policy. I will bring attention to the Old Public Administration (OPA), New Public Management (NPM), Joined-up government (JUG) and New Public Governance (NPG).

1.4 Method and empirical material

The research design strategy is founded on theoretical interpretative case-study (Andersen, 2013). The theories described above will guide the description and explanation of the organizational trends in the central government's ICT security policy. Case-study method is a useful strategy when researching processes, and explanations about how things occur are at center. Gerring (2007) stresses that a case belongs to a larger unit or population of cases. The most closely related larger unit this case belongs to is public security policy, since ICT security is viewed as a subfield within public security. However, sometimes are policies about ICT security and public security interlinked, which makes the separation ambiguous. This case also belongs to the larger unit of how governments responds to wicked problems, since ICT security policy can be defined within the frames of wicked problems. Lastly, I argue that this is also a case about organizational trends of the Norwegian central government overall.

My methodical approach is based on qualitative content analysis of public documents. It entails searching for underlying themes in the material being analyzed (Bryman, 2012, p. 557; Brattberg, 2014). The qualitative content analysis is based on reports and public documents about ICT security or public security policy documents that contain elements of ICT security. The documents sources are Auditor General reports, Norwegian Official Reports, government white papers, royal resolutions, information security strategies and laws. See chapter three for full overview.

The empirical material is organized according to the chronological order of the most central organizational solutions and changes. First, the process behind and further development

of the 1994 establishment of a coordination function at Ministry of Justice (MoJ) described. This section follows the development of this organizational solution up until the 2011 terrorist attacks. Secondly, the re-design of National Security Authority (NSM) around the turn of the millennia and the delegation of new tasks are described. Thirdly, the lead ICT and ICT security ministry model and its supporting organizational tool are described, which was a ministry level coordination solution lasting from 1997 to 2013. This section also highlights the model's relation to other central ICT security organizations. The fourth section begins with post-July 22 policies, then turns to the end of the ICT and ICT security ministry model and the transition of ICT security policy to MoJ's public security portfolio in 2013. The fifth section describe the most recent organizational developments on coordination policies, both in terms of increased coordination authority and through creations of several horizontal coordination bodies.

1.5 Outline of the thesis

The thesis is structured into six chapters. The second chapter describes the theoretical framework in which the analysis is based upon. The instrumental and institutional theories are explained and how they will be used are accounted for. Also, theoretical expectations or hypotheses are derived to make it easier to consider explanatory force. Lastly, the four paradigms of public administration are presented. Chapter three describes the methodological approach. The case-study approach and qualitative document analysis is accounted for. How the theoretical variables are operationalized is described and presented in a table. Furthermore, the validity and reliability of the thesis is discussed.

Chapter four presents the empirical data. The most important events, organizational features and solutions are presented in a chronological manner. At the end, a summary of key empirical data are presented and four major trends are highlighted. In chapter five are the empirical material discussed based on the theoretical framework presented in chapter two. The four major trends are analyzed separately within each of the theoretical approaches. At the end, in chapter six, an overview of the study, summary of the empirical material and conclusions are presented. Implications of the study is also discussed. Lastly, the study's strengths and weaknesses are considered and possible further research on ICT and public security policy are discussed.

2. Theory

2.1 Introduction

In this chapter the theories used in explaining the major organizational trends in the central government's ICT security policy are accounted for. In short, instrumental theory is characterized by its emphasis on structural factors and views public organizations as rational problem-solvers based on the logic of consequence. The institutional theories emphasize cultural aspects influence on actors and government decisions. In order to assess the power of the individual theories, I will derive concrete hypotheses and expectations.

The theories are not used in a competing fashion, but rather as complementary theories. Scott (2014) argues that institutionalized organizations consist of regulatory, normative and cultural-cognitive elements. The instrumental, cultural-institutional and neo-institutional theories coincide with these three elements. Therefore, to ensure the strongest possible explanatory force, the theories must be viewed together. Sometimes only one of the theories will be able to explain a process or outcome. However, often, two or more theoretical approaches are needed to understand and explain processes or outcomes. Towards the end of this chapter, I will describe four conceptualizations of public management and administration paradigms. These will be used to assist the analysis of the major trends of ICT security policy in the Norwegian central government.

2.2 Instrumental theory

2.2.1 Main features

Instrumental theory emphasize hierarchy, division of labor and rules, regulations and procedures. This line of thinking can be traced back to Max Weber's theory on bureaucracy. Organizations and how they operate are believed to be rational, impersonal, and are managed from the top as in a commando structure (Christensen, Lægreid, Roness, & Røvik, 2009). In this perspective are organizations thought of as tools or instruments to solve problems or achieve goals, for example raising quality of education or security. A central theme in instrumental theory is the role of formal structure first highlighted in organizational studies by Gulick (1937). However, his contributions and emphasis on formal structure were for a long while considered irrelevant due to Simon's (1946) criticism and influence of organizational studies. In recent decades, Gulick and his focus on structure have regained credibility and explanatory force (Hammond, 1990; Egeberg, 1999; Egeberg, 2012), most notably with conceptualization of structural specialization principles.

With an instrumental approach to organizations, is a build-in understanding or logic of

consequence. This follows the aforementioned view that organizations serve as tools to achieve something. A problem refers to the distance between actual and wanted reality, and the solution tries to reduce or eliminate that distance. When government employees look at alternative problem-solving measures, they consider expected *consequences* of these alternatives and choose accordingly (Christensen, Lægreid, Roness, & Røvik, 2009, p. 35). Organizations are thus rational and purpose-oriented problem-solvers based on a logic of consequence. Since ICT security policy are characterized as a wicked issue, a central instrumental expectation is that organizational solutions will promote more collaboration and coordination to reduce this problem.

The instrumental perspective is characterized by two main variants (Christensen, Lægreid, Roness, & Røvik, 2009). The hierarchical variant emphasizes the hierarchical commando structure of organizations, which limits decision-making to top political-administrative leaders. This variant expects strong relationship between problem-definitions, goal, solutions and implementation, and has a homogenic view of government organizations (ibid: 34, 42-43). The negotiation variant, on the other hand, takes into account that public organizations often are more heterogenic and pluralistic than the hierarchical variant acknowledges both internally and inter-organizationally. Decision-making processes therefore reflects conflicts of interests, which leads to bargaining, compromises and ambiguous results (ibid: 34, 43-44).

2.2.2 Formal structures – Specialization and coordination

The theory about formal organizational structures lays out the architecture of organizations and its division of labor. These structures consist of rules and regulations about who are supposed to do what, and how (Scott 1981, in Christensen et. al. 2009). Therefore, structures give a broad sense of direction, with stated purposes, goals and interests to the designated roles. What information is gathered, or alternatives seem relevant to a decision-maker, is inherently biased by his or her structural surroundings. Since complete information only is a theoretical notion, structures help solve the necessity of reducing complexities and information overload on the one hand, and give filter and decision premises on the other (Egeberg, 2012).

Why are the formal structures expected to be so influential and followed by the people within organizations? Formal structures must be understood as formalized norms (Egeberg, 2012, p. 3). Therefore, people may feel morally obliged to follow formal organizational norms. Modern organizational life is heavily dominated by rational codes of conduct and impersonal relationships that assists employees to separate private interests. Secondly, in many cases it will

be in the self-interest to operate within the given rules and roles because of build-in incentive mechanisms with rewards and punishments. For example, individuals at the lower levels knows that following organizational norms are prerequisite to advancing their careers. And thirdly, Egeberg, highlights social control and peer review by colleagues as a normative force that reduce deviant behavior (ibid).

Dimensions of specialization

Fundamentally, all organizations have vertical and horizontal structures. They say something about how labor and authority are specialized and coordinated. The latter will be addressed in the next subsection. Specialization indicate division of labor and principles on how an organization's work is specialized according to the vertical and horizontal dimensions.

Vertical specialization refers to division of labor on the vertical structure. It indicates how labor and decision-authority are specialized and divided between different hierarchical levels, either within or between organizations (Egeberg, 2012, p. 4). Government organizations are basically hierarchies with a vertical line of command, from the top and downwards. That entails that those with superior authority can command and/or instruct subordinate individuals or organizations. Vertical specialization can also contain *collegial* elements, which tend to reduce the degree of hierarchical commando authority. Collegiality usually refers to decision-making processes that are a result of arguing, bargaining or voting (Egeberg 2012: 4). The cabinet meetings, with all ministers of government, are a prime example of a collegial body. Collegial bodies are usually found as task forces, committees, councils, boards, project groups or similar forms. These structures can be permanent or temporary to solve a passing problem, and are often a complementary or secondary structure to the usual hierarchical line (Egeberg, 1999; Egeberg, 2012; Christensen, Lægreid, Roness, & Røvik, 2009, p. 39). With supplementary collegial bodies being added to the traditional bureaucratic organization results in more vertical and horizontal connections and increased complexity. And a more *network*-oriented style of governing. In ICT security policy I will therefore look at how the vertical specializations are organized. Which ministry is on top, inter-organizational lines of command and degrees of hierarchical instruction power versus collegial elements are central questions.

The second dimension is *horizontal specialization*. It indicates how issues or policy areas are separated or linked, that are on the same hierarchical level (Egeberg, 2012, p. 3). How organizational boundaries are set up are expected to affect information flows and coordination processes. Conceptually, it is common to separate between four different principles of horizontal specialization, which was first promoted by Gulick (1937).

The *sector principle* is organizing according to purpose, where decision-makers seek solutions and standards to sectoral concerns or problems (Egeberg, 1999). The Norwegian central government is heavily organized according to this principle due to the ministerial rule system, with designated ministries for health, education, transportation and so on. Security is, as this thesis will describe and discuss much more later, not as clear-cut as many other policy fields. But there is an evident distinction between national security and sovereignty that are the Ministry of Defense's responsible on the one hand, and Ministry of Justice's responsibility for criminality and civil security on the other. The *process principle* relates to organizing according to how the work is done and professional knowledge (Egeberg, 1999, p. 158). A ministry can for example be divided into units for handling planning, budgets, personnel and judicial cases. In relation to ICT security, technical skills and professional knowledge about digital technology are of special interest. With the *Clientele principle* units are organized according specific groups of the population (ibid). If, for example, one ICT security organization is addressing small businesses and another is addressing large companies, indicate specialization according to the clientele principle. The final principle of horizontal specialization is the *territory principle*. With this type of specialization issues across sectors can be considered comprehensively according to the needs within a given geographical area (Egeberg, 2012). This principle is common within most sectors, first with a sectoral ministry and directorates on central level, and then with geographical units below – which is often divided into a regional and local level.

When I use horizontal specialization analytically, I am mostly concerned with how inter-organizational horizontal specializations are set up at the ministry and agency level.

Coordination

The size of governments and degree of specialization make them inherently multi-dimensional (Bouckaert, Peters, & Verhoerst, 2010, pp. 13-14). This brings forth the issue of coordination. Coordination can be defined as "both the process through which decisions are brought together and an outcome of that process" (ibid: p. 15). My focus is on coordination as a process because I am more interested in how coordination is brought about through organizational solutions rather than the policy results themselves. In security policy, where responsibility is decentralized to all sectors and organizations, and at the same time are supposed to be led by a few central actors, make coordination an essential feature. Next, I will describe key distinctions of coordination that will be used in the analysis.

Coordination is tightly linked to specialization and follows the same horizontal and vertical structures as mentioned above. Whether coordination is vertical or horizontal depends

on the direction of the coordinative initiatives. *Vertical coordination* is forms of coordination between different levels of government. It usually refers to coordination by a high-level organization/unit of lower level's actions. (Bouckaert, Peters, & Verhoerst, 2010, p. 24). The ministerial rule system primarily follows this type of coordination. While *horizontal coordination* is forms of coordination between organizations or units on the same hierarchical level (ibid), for example between ministries or between directorates. A combination of these two dimensions are also possible. Most ministries have several agency level organizations under its vertical authority. Then, the parent ministry needs to enforce coordination between these agencies. Thus, the vertical coordination is between a ministry and its agency level organizations, and the horizontal coordination is between the different agencies. It can also entail, as we will see later in the empirical chapter, horizontal coordination at ministerial level and vertical coordination to one agency level organization.

It is a dynamic relationship between specialization and coordination. Strong degree of specialization brings forth increased pressure on coordination. Gulick (1937) emphasized what type of coordination problems that are more intrusive depends on whether government organizations are specialized according to purpose, process, clientele, or territory. If the government is based on purpose, then the coordination problem will between the structurally differentiated sectors. While a process-based organization principle will bring forth coordination problems between different professional groups, and so on (Egeberg, 2012). Since the ministry level is heavily based upon the purpose/sector principle coordination problems across these sectors will be expected, and measures to reduce the sectoral coordination problem.

A minimalistic version of coordination is what Frizt Scharpf (1994) calls negative coordination. It only requires that a new policy does not harm existing policies and the interests of other government subunits. This type of coordination holds low aspiration of coordination and can be viewed as minimum condition for governing (Scharpf, 1994, pp. 38-39; Bouckaert, Peters, & Verhoerst, 2010, p. 20). Positive coordination, on the other hand, is associated with much higher aspirations, where the government's overall performance is taken into account. Positive coordination seeks to maximize a policy's efficiency and efficacy by brining together several ministerial portfolios through joint strategies and action. These two extremes, not interfering versus build coherence, result in two very different modes of coordination as well. When I analyze coordination arrangements in ICT security policy, I will find positive coordination if arrangement promotes multilateral negotiations within and/or between ministerial boundaries, where policy options by all participating units are considered (Scharpf 1994). Bouckaert, Peters and Verhoerst argues that actors may be required to give up some

policy goal in order to achieve greater overall performance (2010, p. 20). If, by contrast, coordination efforts operate in a bilateral fashion with a 'clearance' mechanism by potentially affected units, it will indicate negative coordination.

Coordination through network offers a different approach to coordination than the hierarchical one. Network entails establishment of contact with a variety of actors. They are often interdependent actors which are all part of the same overall service-delivery (Klijn & Koppenjan, 2012). Network approaches to coordination also open up the possibility for government organizations to coordinate with important private sector actors. A major feature of networks is the horizontal character (ibid). However, a complete flat structure of equal partners is seldom the case. Network constellations often entail power inequalities, where participants do not have an equal voice (Osborne, 2010, p. 9). This is can be referred to as networks' "shadow of hierarchy" (Christensen, Lægreid, & Rykkja, 2016, p. 893) Collegial supplementary bodies, touched upon above, often operates in a network-oriented fashion. Management through networks will operate differently due to the weak hierarchical elements. Negotiating skills, binding actors together and ability to forge new solutions are central to successful management and coordination through network (Klijn & Koppenjan, 2012, p. 593).

A key organizational arrangement to promote coordination in public security policy is the 'lead agency model'. The model entails to concentrate policy capabilities on a transboundary issue to one or a limited number of organizations (Boin, Busuioc, & Groenleer, 2014, pp. 11-12). Thus, the model is a mixture of a traditional hierarchy and a network approach. The model has been popularized in the US, where the Department of Homeland Security became responsible for inter-agency oversight after the 9/11 terrorist attacks. The lead agency often chairs an inter-agency working group to coordinate policy, ensures cohesion among involved organizations and is responsible for implementing decisions (Christensen, Danielsen, Lægreid, & Rykkja, 2014, p. 8). Thus, the network elements relate to the lead agency's multiple connections to other relevant organizations. While, the hierarchical elements are associated to its function to impose control on other organizations within the network (Christensen, Lægreid, & Rykkja, 2016, p. 893). The term lead agency model might indicate that this model only appears on agency-level, but the model is also highly relevant on ministry-level as we will see in the empirical chapter. Of special interest to the analysis is the degree of hierarchical and network elements in the lead organizations of ICT security policy.

2.2.3 Structural complexity and hybridity

Modern public organizations are becoming increasingly complex and hybrid as they try to attend to many goals, ideas, considerations, demands and structures, which also can be in conflict to each other (Christensen & Lægreid, 2011, p. 407). An explanation is that public sector organizations have gone through several waves of administrative policies and reforms, and that these reforms have been layered on top of each other (Streek & Thelen, 2005). This have created complex systems with embedded inconsistencies. Public security policy, management and administration is no exception. A prime example of this kind of inconsistency, which will be described and discussed more later, is the notion of cross-sectoral responsibility at one ministry while at the same time have sectoral responsibility on each ministry. This thesis uses Christensen and Lægreid's (2011) conceptualization of complexity and hybridity to describe and explain the major organizational features and trends of ICT-security policy. Although these concepts contain both structural and cultural element, this section will emphasize the structural features.

When complexity is viewed as a structural variable it takes us back to Egeberg (2012) and Gulick's (1937) dimensions of vertical and horizontal specialization, expressed either intra or inter-organizationally. By looking at all these dimensions it is possible to get a picture of how structurally complex a policy field like ICT security is. On one extreme, there is strong vertical and horizontal specializations. This is typical for New Public Management (NPM) reforms. While low degree of specialization is more common with old public administration (PA), and the newer post-NPM reform regime (Christensen & Lægreid, 2011, p. 409). Although, it is difficult to measure exact structural complexity, this analytical tool makes it possible to determine the direction complexity in ICT security is going.

Complexity and hybridity are often used interchangeably, but Christensen and Lægreid carefully distinguished the two by making complexity a precondition for hybridity (Christensen & Lægreid, 2011, p. 410). Thus, complex organizational arrangements don't have to be hybrid. But when complex organizational arrangements lead to lasting tensions and inconsistencies, the result is hybridity. Examples of hybrid organizations are quasi-governmental entities that operating in the grey areas of public and private sector. Mixtures of hierarchy, networks and/or market solutions also lead to hybridity because each of these solutions pull in different directions. Hybrid organizations are often multifunctional that combine different tasks, values and organizational forms, with partly inconsistent considerations that result in trade-offs and lasting tensions (ibid). Highly relevant to this analysis is the border between civil and military sector which is supposed to be clear-cut and not mixed. But in security policy this border can

be challenged or produce grey areas, making organizations or arrangements operating in the interface of civil and military sector prone to hybridity. Hybridity is not inherently negative and something that needs to be cured. It is rather a systemic feature of modern public organizations that has the advantage of flexibility (Christensen & Lægreid, 2011, p. 420). Why public organizations develop in an increasingly complex and hybrid manner is however contested. One argument is that organizational design is a result of negotiation by several different driving forces. And that the involved actors are constrained by their contextual features.

2.2.4 Instrumental expectations

I will use instrumental theory to describe and explain how formal structures and instrumental logic have shaped the development of the ICT security policy field. In the descriptive part will formal structure with its dimensions of specialization and coordination be central in mapping the key organizations and organizational arrangements – and later to explain behavior and results. These dimensions will also be used analytically to describe and explain complexity, its direction, and hybridity.

- The overall expectation is that the policy-makers will be influenced by an instrumental logic and use organizations or arrangements as tools to solve problems in a rational fashion.
- Because security in general and ICT security in particular are characterized as wicked problems, solutions are expected to promote more collaboration and coordination.
- Coordination pressures/problems are expected to occur in relation to horizontal specialization principle, and coordinative solutions to will be adopted counter these issues.
- The structural organization of the ICT security policy field will shape behavior and performance.
- If the hierarchical variant of instrumental theory dominates the organizational solutions to ICT security policy, I expect strong vertical lines of command and relationship between problem-definition, solutions and implementation, and little ambiguity.
- Based on the negotiation variant I expect to see heterogenic decision-making processes with conflict of interests that results in compromises with ambiguity.

2.3 Institutional theory

2.3.1 Main features

Institutionalists do not dismiss that organizations are shaped by formal structure, laws and regulations. But institutionalists argue that there are more to organizations than formalities and that their actions cannot be purely impersonal and based on rational calculation. Scott (2014, p. 56) define institutions as consisting of "regulative, normative and cultural-cognitive elements, that together with associated activities and resources, provide stability and meaning to social life". The institutional approach emphasizes that organizations operate within a social and cultural context, and thus centers around the normative and cultural-cognitive pillars in Scott's definition.

"Traditional" institutionalists draw attention to the informal norms and cultures within an organization or between organizational arrangements, and are therefore mostly concerned with the normative pillar. The bulk of this section are this kind of cultural-institutional theories. At the end I will turn to neo-institutional theories which are more concerned with the cultural-cognitive pillar. These theories hold a constructivist approach to social reality and stresses how the external environment affect interpretations and actions in organizations.

2.3.2 Institutionalization, logic of appropriateness and cultural complexity

Compared to the instrumental perspective on organizations, the cultural-institutional approach highlights enduring features and solidity to social systems across time and space, which can be transmitted across generations, maintained and reproduced (Scott, 2014, p. 57). Central to this aspect is the process of institutionalization:

> It is something that happens to an organization over time, reflecting the organization's own distinctive history, the people who have been in it, the groups it embodies and the vested interests they have created, and the way it has adapted to its environment. […] In what is perhaps its most significant meaning, "to institutionalize" is to *infuse with value* beyond the technical requirements of the task at hand (Selznick, 1957, pp. 16-17).

As a result, organizations are thought of as carrying distinct identities and intrinsic value. The process of institutionalization and development of cultural features are predominantly understood as evolutional, natural processes, due to gradual adaptation to internal and close external environment (Christensen, Lægreid, Roness, & Røvik, 2009, p. 59). When organizations become increasingly institutionalized their history are reflected in the present. This is firstly because actors are operating in an institutional context. Secondly, possible actions are constrained by available institutional capabilities and these are a result of choices made at

an earlier point in time (Krasner, 1988, pp. 71-72).

A popular way to conceptualize how organizational culture shape actions are that actors are following a logic of appropriateness (March & Olsen, 1989), rather than of consequence as in instrumental theory. This entails that actions follow what is thought of as acceptable, fitting and reasonable in relation to the given norms, values, identities and roles (Scott, 2014, pp. 64-66; Olsen, 2007, p. 3). It can be described as a matching process, where situations are coupled with identities which in turn leads to appropriate actions (Christensen, Lægreid, Roness, & Røvik, 2009, p. 54). Therefore, I am interested in identifying the major norms and cultural attitudes towards the organization of (ICT) security in the central government. Are reform efforts in line with what is thought of as appropriate or are they threatening these norms? If the latter is the case, we are likely to witness cultural resistance from central actors. However, since informal norms are evolutionary and adaptable to pressure can initial resistance to inappropriate solutions change over time.

In relation to the concepts of complexity and hybridity, strong cultural complexity means a variety of informal norms and values either intra- or inter-organizationally (Christensen & Lægreid, 2011, pp. 409-410). Even though government organizations do share some common cultural features, they also contain sub-cultures. Cultural complexity can enhance overall hybridity when sub-cultures' values and norms that are not easily compatible or with competing views on what is culturally appropriate (ibid: 412). Since (ICT) security is often in the interface of military and civil sector, am I especially interested organizational solutions that are across these sector, which might indicate cultural complexity and hybridity.

2.3.3 Critical junctures and path-dependency

At the basis, path-dependency argues that decisions made in the formative years of an institutional arrangement is highly relevant to unfolding events (Mahoney, 2000, p. 510). Thus, cultural norms and values at the organizational genesis are transmitted to later generations. This is often described as "birth marks". For example, organizations created in a period of decentralization or democratic values will have different formal structures and informal norms compared to organizations created in a period of hierarchy and centralization (Christensen, Lægreid, Roness, & Røvik, 2009, p. 62). Mahoney distinguishes between self-reinforcing sequences and reactive sequences as two separate ways of understanding path-dependency (2000, pp. 508-509). I will limit the analysis to the former, due to the latter's complexity and dubious relevance to the empirical material.

Self-reinforcing sequences centers around increasing returns of institutional

arrangements (Pierson, 2000). Institutions are prone to increasing returns because they make it increasingly costly and unattractive to change course over time. Within an institutional framework, actors (both individuals or organizations) are encouraged to specialize, deepen relationships to other actors and develop particular identities. These actions increase the attractiveness of the existing institutional system relative to other hypothetical ones (ibid: 259). Thus, institutions and institutional arrangements promote stability and inertia, where paths are locked-in and reinforced by its own institutional setting. However, institutions may vary in their ability to create rapid and decisive self-reinforcing mechanisms after its creation. If they do, a lock-in situation is successfully achieved. But, if these self-reinforcing mechanisms are generated more gradually, an institution may not be able to capitalize on its early advantage and can be overcome by alternative solutions (Mahoney, 2000, p. 515). The literature is not unified on how the self-reinforcing mechanism do work. Arguments vary from rational cost-benefit assessments through power-explanations to what is considered just or appropriate.

Change in this conceptual framework is mostly understood as small adjustments within the path. While more substantial change demands external shock to the system that create a new critical juncture and divergence to a new path (Mahoney, 2000). Critical junctures are points in time when an institutional arrangement is adopted from usually two or more alternatives. However, prior to the critical juncture it can be difficult to predict which alternative will be chosen. It is thought of as critical because after the arrangement is chosen it is increasingly difficult to go back to a situation with multiple alternative solutions (Mahoney, 2000, p. 513). This theory of change is by many described as punctuated equilibrium.

When I use path-dependency on the empirical material, I will bring attention to institutional genesis' and their self-reproducing mechanisms in the formative years. Institutional arrangements are expected to continue unless new critical junctures arise. Of particular interest is situations where institutional arrangements are struggling to self-reproduce, which might explain why competing and/or conflicting arrangements also appear.

2.3.4 Gradual transformative change

The institutional theory about path-dependency and critical junctures is not without criticism, perhaps in particular by other institutionalists. The key issue derives from their inability to explain substantial changes to institutional arrangements (Thelen, 1999; Streek & Thelen, 2005). Streeck and Thelen argues that "real" change in the path-dependency literature, that is change that result in discontinuity, only is possible through an abrupt process which give rise to a new path (Streek & Thelen, 2005, p. 8). In their typology, this type of change is categorized

in the lower right cell. Incremental change, on the other hand, by the path-dependency literature is predominantly understood as reactive and adaptive, and serve to continue the exiting path (upper left cell). Contrary to the path-dependency literature, Streeck and Thelen argue that incremental change with transformative results (upper left cell) is not only possible, but frequent. Therefore, gradual transformative change should be of more interests to institutionalists in social and political sciences (Streek & Thelen, 2005, p. 9).

		Result of change	
		Continuity	Discontinuity
Process of change	Incremental	Reproduction by adaptation	Gradual transformation
	Abrupt	Survival and return	Breakdown and replacement

Table 1: Streeck and Thelen's (2005) typology of change

Throughout the empirical timeframe we will see several reform and re-organization attempts. This typology will be used analytically to describe these policies in terms of their process and result. If reproduction and adaptation or breakdown and replacement types of change are evident will indicate that path-dependency are highly relevant. While, if discontinuity have come about incrementally will indicate a gradual transformation stressed by Streeck and Thelen. They offer five different modes of gradual and transformative change. These are displacement, layering, drift, conversion and exhaustion. I will attempt to distinguish between these modes un cases where gradual transformation are evident.

Displacement is the gradual process of which new models surface and discredit existing and traditional arrangements. Change can origin internally through rediscovery or activation of previously suppressed or suspended possibilities. It can also origin externally through importation and cultivation of international institutions and practices. *Layering* is a type of change when a new system is put on top of an existing one, so that two or more systems coexists. Layering often occurs as amendments, additions or revisions to an existing institutional arrangement. The reform-wave of New Public Management was in many cases layered on top of the existing arrangements of Norwegian public administration. *Drift* can occur due to lack of reproduction and maintenance of an institution. With gradual changes in its attending surroundings, and without sufficient adaptation, an institution can experience decay or erosion as an incremental discontinuity. *Conversion* occurs when institutions are redirected to new goals, functions or purposes. These redirections can origin from new environmental and

external factors, as for example technological developments and vulnerabilities. Changes in power relations is also a possible source of conversion, as actors not originally involved in the institutional design rise to power. *Exhaustion*, lastly, does not strictly speaking lead to transformational change, but rather institutional breakdown. The process, however, is gradual and therefore constitutes transformation until the breaking down (Streek & Thelen, 2005, pp. 19-29).

2.3.5 Cultural-institutional expectations

I will use cultural-institutional theory to describe and explain how informal norms and cultural factors have shaped the development of ICT security policy and organization. In the empirical chapter will informal norms on how (ICT) security should be organized be identified, and if reforms or re-organization attempts are in line with these norms. These changes will also be described in the empirical chapter with Streeck and Thelen's (2005) typology in mind, so that these changes can be explained later in the analysis.

- The overall expectation is that policy-makers will be influenced by the informal norms on how ICT security in the central government ought to be organized.
- Because of institutionalized informal norms policy changes and new organizational solution will be based on a logic of appropriateness. Changes that threaten dominating norms are meet with cultural resistance.
- Over time norms can evolve and cultural resistance against coordination measures will be reduced.
- I expect that organizational arrangements will self-reproduce and be resistant to "real" change, unless new critical junctures create new paths.
- In contradiction to the latter, I expect that changes will be of gradual transformative character.

2.3.6 Neo-institutional theory

Neo-institutional theories break from instrumental and institutional theories on several basic premises. They hold a social constructivist view on the world, where our social reality is not given, but a result of perception through symbolic interaction and sense-making. Interpretative processes are largely shaped by external frameworks, because the outside world offers belief systems and cultural frames that mediate with or are imposed on individual actors and organizations (Scott, 2014, pp. 66-69; Meyer & Rowan, 1977). These external cultural systems operate on multiple levels and are fluid rather than sealed. They range from shared local

understanding, through common frames in an organization or logics in a policy field, to shared assumptions and ideologies about political and economic preferences on national and transnational level (Scott, 2014, p. 68).

Since organizations operate in an institutionalized environment, they are continuously confronted with how they ought to act and be organized. These external cultural norms are what is called *myths* (Christensen, Lægreid, Roness, & Røvik, 2009, p. 75). Neo-institutionalism therefore place adaptation to the institutionalized environment and its expectation at center. Myths can come to light in administrative policy-making, reform and re-organization processes because policy-makers use myths and symbols to demonstrate that they are acting on what is collectively valued and to generate legitimacy. In search of legitimacy can leaders also use the strategy of hypocrisy or "double-talk" as coined by Brunsson (2006). Speeches or policy-documents can contain talk about change with fitting symbols and myth, while actually have low degree of implementation. Central questions based on this theoretical approach, are particular symbols used repeatedly by certain actors? Is the organizational thinking realistic or are they over-selling it?

Perhaps the most central organizational myth is modern society's belief in rational authority. This was already conceptualized by Weber in his analysis of the emergence of rational-legal authority. Meyer and Rowan (1977) re-popularized this idea and showed how these beliefs are embedded in laws, educational processes and public opinion. Organizational myths are usually created, popularized and spread through natural development processes. Central actors in these processes are for example international organizations like the UN or OECD, consultant companies, higher education sector, media or publishing houses, or large multinational corporations (Christensen, Lægreid, Roness, & Røvik, 2009, pp. 82-86).

When I analyze the empirical material of ICT security policy based on neo-institutional insights, I will bring particularly interest towards myths and symbols about coordination and collaborations since they are commonly thought of as reducing transboundary problems like ICT security. And, maybe, we will also see more talk about coordination than action?

Neo-institutionalist argue that organizations become increasingly homogenic due to the influence of rationalized myths (Christensen, Lægreid, Roness, & Røvik, 2009, p. 75). The most common concept to describe the homogenization process is isomorphism. It entails a constraining process that forces a unit to resemble other units which face a same set of environmental conditions (DiMaggio & Powell, 1983, p. 149). DiMaggio and Powell (1983) distinguish between three mechanisms for institutional change through isomorphism: coercive isomorphism, normative pressure, and mimic adoption.

With *coercive isomorphism* organizations are pressured by other organizations they are dependent on. Through laws and regulation, they can be formally imposed certain prescriptions, leaving them with little or no choice. But, organizational change can also be a result of more subtle processes like cultural pressure that forces a certain way to organize (DiMaggio & Powell, 1983, pp. 150-151). *Mimic isomorphism* is a mechanism for adoption of myths that is largely related to uncertainty. Uncertainty can be that technologies are poorly understood, goals are ambiguous, or the environment creates symbolic uncertainty. When facing uncertainties, organizations look at successful or legitimate organizations and imitate their solutions (DiMaggio & Powell, 1983, pp. 151-152). This mechanism of isomorphism seem highly relevant to this case since ICT security policy is dealing with a new technology with large uncertainties. *Normative isomorphism* largely rests on professionalization of public organizations. Through education and training, different groups of professionals internalize cognitive bases and norms on legitimate ways of organizing. Since only certain educational and professional demographics are employed in specialized organizations, adoption of myths and change can be derived from what is thought as appropriate by its dominating type of professional staff (DiMaggio & Powell, 1983, pp. 152-154; Christensen, Lægreid, Roness, & Røvik, 2009, pp. 90-91). Therefore, I will be looking for references to solutions or measures used by other countries. If, for example, the government propose an organizational solution already operating in several allied countries is a strong indication of neo-institutional myths.

2.3.7 Neo-institutional expectations

I will use the neo-institutional theories to describe and explain how the institutionalized external environment have influenced the development of ICT security policy and organization. With this approach it will be central to identify the use of symbols and rationalized myths, if there is distance between talk and action, and cases of isomorphism.

- I expect that the government will seek legitimacy through symbols and myths about coordination and collaboration.
- I expect that there will be a distance between talk about coordination and collaboration and actual implementation.
- I expect that the government will mimic organizational solutions to ICT security that are already adopted by central allied countries.

2.4 Public administration paradigms

2.4.1 Introduction

I am researching organizational trends in ICT security policy since the 1990s. That is almost three decades of government policy, organizational thinking and solutions to a policy field that needs explaining. Therefore, it is useful to get a picture of the major trends characterized administrative thinking, policy and reforms of the state apparatus over the last several decades to assist the analysis. I differentiate between four main types of paradigms or ways public administration researchers usually categorizes administrative policy trends. These paradigms have implications for all the three theoretical approaches described above. They have structural implications which relevant to the instrumental analysis. In particular the first paradigm has normative implications because it has been institutionalized over many decades. They also have mythical features as they represent some sort of external norms.

2.4.2 Old Public Administration

Old Public administration (OPA) have characterized the development of the state apparatus since late 19th and early 20th century and must be considered foundational to modern public administration. OPA was the dominating way of thinking about the organization of state apparatus in the post-World War Two era, until New Public Management-reforms was introduced in the late 1970s (Hood, 1991). The importance of rule of law where administering is based on guidelines, rules and laws, i.e. input control, are key features of OPA. Professional public servants in public administration are central to development and implementation of policies (Osborne, 2010, pp. 2-3). OPA is therefore closely related to Max Weber's research and theories on the rule-based bureaucracy.

Organizationally, OPA is characterized by an integrated and strong central government, however the integration primarily is on the vertical dimension (Osborne, 2010, p. 8). This is due to the departmental organization of central governments. In the Norwegian context, the central government has been separated into ministries on the horizontal dimension since Norway's foundation in 1814 and onwards (Christensen, Egeberg, Larsen, Lægreid, & Roness, 2007, pp. 29-34). This has formed the *ministerial rule system*, where authority over agency level organizations and policy sectors is founded upon vertical coordination of horizontally specialized ministries. Thus, OPA's departmental structure has fostered problems of horizontal integration of central government (Kavanagh & Richards, 2001). Therefore, I expect that both structural and cultural features of OPA, its departmental structure and ministerial rule system influence central actors in my case in ways that inhibits horizontal integration efforts.

2.4.3 New Public Management

The discourse of public policy and administration changed from late 1970s onwards. Insights from the private sector were emphasized and converted to public organizations to ensure better governing, control and efficiency. This led to a wave of reforms commonly labelled New Public Management (NPM) (Hood, 1991). The most prominent elements were A) increased specialization both vertically and horizontally, with the intention of creating more 'single purpose organizations' and less organizational overlap. B) More professionalized managers with more autonomy. C) Introduction of performance management on top of the rule-based mechanisms from OPA. With new attention towards goals and results, and accompanying reporting, implied that government administration was under both input and output control mechanisms. D) Increased attention to user-friendliness and service. E) Stronger belief in market allocation, which resulted in more outsourcing of services and partial or full privatization (Christensen, Egeberg, Larsen, Lægreid, & Roness, 2007, pp. 98-99).

NPM cannot be characterized as an unified reform wave, but rather a basket of reform elements inspired by the business world. The Anglo-Saxon countries of Great Britain, USA, Australia and New Zealand adopted NPM in a strong degree. While Continental Europe like Germany and France and the Nordic countries have been more reluctant reformers (Christensen & Lægreid, 2007). This has resulted in a public administration funded upon a combination of old, Weberian thinking and new elements of NPM (Pollitt & Bouckaert, 2004, pp. 99-100).

The most relevant NPM elements to my case and research question relate to point A about increased vertical and horizontal specialization. If NPM thinking influence decision-makers new organizational solutions are expected to be highly specialized on both horizontal and vertical dimensions, and follow 'single purpose' mentality. Point E about privatization also is relevant to this case, in relation to service-delivery of electronic information and communication technology.

2.4.4 Joined-up government

In 1997 the Tony Blair government in UK first introduced the concept Joined-up government (JUG). Policies and reforms within the label of JUG typically promoted coordination initiatives aimed at wicked issues that falls between organizational boundaries, administrative level or policy sectors (Christensen & Lægreid, 2007, pp. 1059-1060). Similar efforts in New Zealand and Australia around the turn of the millennia have been labeled Whole-of-Government (WG). These reforms are seen as responses to the structural devolution and fragmentation promoted by NPM because they offered a more holistic approach and sought integration strategies.

Therefore, Post-NPM also has been a way to categorize these reform initiatives (ibid).

In relation to my case, I am interested to see if new measures entail strengthening the political-administrative center, more integration and stronger coordination measures. Typical JUG or Post-NPM features also relate to collaborative inter-ministerial or interagency units, task forces, or other types of network-oriented approaches to coordination (Christensen & Lægreid, 2007). These network elements are however at the core of NPG, which I will turn to now.

2.4.5 New Public Governance

New public governance (NPG) is a conceptualization of public sector and service-delivery that are based in institutional and network theory (Osborne, 2010). NPG stresses the plural and pluralist elements of the modern state. It is plural in the sense that multiple interdependent actors contribute to the delivery of public services. The state is pluralist in the sense that multiple processes inform policy-making processes (Osborne 2010: 9). Due to the complexities of the state and its policy and service implementation the central resource allocation mechanism is interorganizational networks. OPA, by contrast, holds a unitary view of the state and hierarchy as the main resource-allocation mechanism. While NPM are more based on competition, price and contractual mechanisms. Post-NPM reforms are characterized by their re-emphasis on hierarchy.

Osborne's conceptualization of NPG is grounded in empirical evidence from the UK. He argues that the complex, plural and fragmented nature of government implementation and service delivery are becoming increasingly apparent. If NPG are of relevance to this case about ICT security policy, I expect to see complex, plural and fragmented features and that they are solved by governance through network-mechanisms to be increasingly prominent.

3. Methods

3.1 Introduction

The purpose of this thesis is to describe, interpret and explain the major organizational solutions and trends in the central government's ICT security policy since the 1990s until 2018. To do so in a social scientific way, the investigation needs to be anchored in its methodical approach and the choice of method must be suitable to the research question asked. The most fundamental divide in social science research is between quantitative and qualitative methods. The quantitative method entails collection of numerical data, statistical analysis, champions positivism and mimics natural science approach (Bryman, 2012, p. 160). The qualitative method is more concerned with words and epistemologically characterized by an interpretative approach (ibid: 380).

As the research question is concerned with government policies and organizational solutions, the qualitative approach is considered to be the most appropriate. I have also chosen case-study as research design based on document analysis to generate data. In this chapter I will account for the case-study design as methodical approach. Then, I will account for the data collection process and document analysis approach, before turning to the process of operationalization. The chapter will end with reflections on the validity and reliability of the investigation.

3.2 Case study design

The case-study is a research design and method that entail the detailed and intensive analysis of a single phenomenon (Bryman, 2012, p. 66). A case is a "spatially delimited phenomenon (a unit) observed at a single point in time or over some period of time [...] The type of phenomenon that an inference attempts to explain" (Gerring, 2007, p. 19). Case-studies are therefore well suited to investigate complex phenomenons with many variables.

The case and unit of analysis in this thesis is the Norwegian central government's organizational solutions to ICT security policy. Gerring (2007) stresses that a case belongs to a defined universe. That is, a case is understood as a part of a larger unit or population of cases. The most obvious larger unit my case is part of is public security policy, because I understand ICT security as a subfield within the larger policy field of public security. However, there are situations where this divide becomes blurry because ICT security is very tightly connected to the overall public security field. Some policies, f. ex. about Ministry of Justice's coordination authority, affects ICT security policy and the larger realm of public security simultaneously. I will also argue that this case belongs to the larger universe of wicked problems, or rather how

governments (organizationally) handle wicked problems since ICT security can be defined within the wicked problem-concept. Lastly, this analysis is also arguably a case of the organizational trends in the central government overall.

The aim of this analysis is to generate knowledge about the government's ICT security policy through mapping and categorizing the data, and explain these processes and outcomes based on instrumental and institutional theories. This aim and case-study method has consequences for the relationship between data and theory. My research design is a theoretical interpretative study (Andersen, 2013). That entails the use existing theories and concepts to structure and categorize the empirical material.

To lend the concepts quantitative research, my research design and approach is as following: The dependent variable (Y) is *the major organizational solutions and trends in the central government's ICT security policy since 1990s until 2018*. This outcome is explained by independent structural-instrumental variables (X1), cultural-institutional variables (X2) and neo-institutional variables (X3). In the theoretical chapter I have accounted for what these variables are and what to expect if these variables have explanatory force. I will turn to the operationalization of these variables shortly.

3.3 Document analysis and data collection process

The qualitative case-study method makes several ways of data collection and analysis possible. Interviews, observations and documents are the most common ways of generating data (Tjora, 2010). I have only chosen data collection and analysis of public documents since it is an efficient method when large number of material is needed, and because public document provide documents of relatively high authenticity (Bryman, 2012, pp. 549-550).

My approach to document analysis is qualitative content analysis. It entails searching for underlying themes in the material being analyzed (Bryman, 2012, p. 557). Broadly speaking, it is a systematic study of political messages. More refined, it can be defined as qualitative analysis of the presence of ideas in text, where interpretation is an essential part of the analysis (Brattberg, 2014, p. 57). Therefore, this approach offers a way to map out the strictly observable content and to interpret that content. Since this is a theoretical interpretative study, as mentioned above, the theories will guide my interpretations. To exemplify how this approach is used. My systematic analysis show that Ministry of Foreign Affairs (MoFA) have not been formally involved in any ICT security coordination bodies until 2017. This is strictly observable content. An interpretation of that content may point towards that involvement of MoFA is a deliberate organizational tool in response to the increased importance of international policies to national

ICT security policies.

The qualitative document analysis is based on public documents about ICT security or public security policy documents that contain elements of ICT security. I have collected and analyzed a range of documents. The main documents are: **Auditor General reports** (Riksrevisjonen, 2005: dokument nr. 3:4; Riksrevisjonen, 2010: dokument nr. 1), **Norwegian Official reports** (NOU, 2000: 24; NOU, 2006: 6; NOU, 2012: 14; NOU, 2015: 13; NOU, 2018: 14), **Government white papers** (St. Meld., nr. 48 (1993-1994); St. Meld., nr. 48 (1993-1994); St. Meld., nr. 47 (2000-2001); St. Meld, nr. 39 (2003-2004); St. Meld., nr. 17 (2006-2007); St. Meld., nr. 22 (2007-2008); St. Meld., nr. 29 (2011-2012); St. Meld., nr. 10 (2016-2017); St. Meld., nr 38 (2016-2017)), **Royal resolutions** (Kgl.res., 16.09.1994; Kgl. res, 20.12.1996; Kgl.res., 19.12.1997; Kgl.res., 03.11.2000; Kgl.res., 29.08.2003; Kgl.res., 01.10.2004; Kgl.res., 11.11.2011; Kgl.res., 15.06.2012; Kgl.res., 22.03.2013; Kgl.res., 10.03.2017), **information security strategies** (Forsvarsdepartementet, Nærings- og handelsdepartementet & Justis- og politidepartementet, 2003; Forynings- og administrasjonsdepartementet, Justis- og politidepartementet, Forsvarsdepartementet & Samferdelsdepartementet, 2007; Justis- og beredskapsdepartementet, Forsvarsdepartementet, Samferdelsdepartementet & Fornyings- & administrasjonsdepartementet, 2012), and **laws** (Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), 1998; Lov om elektronisk kommunikasjon (Ekomloven), 2003).

In the beginning of the data collection process, as I was searching for the relevant documents and starting to get familiar with them, I realized the need to gather raw data to filter the relevant information from the irrelevant, before continuing the analysis and writing the empirical chapter. Therefore, a raw data document was created where each document got a headline organized chronologically. From each document analyzed, I copy-pasted ICT security-related paragraphs or sentences, and/or wrote key information from them. In that way I was able to get overview over all the important policies, problem definitions and organizational solutions, which was very helpful in writing the empirical chapter and analysis.

When I turned to writing the empirical chapter and later analysis, I used a combination of chronological order and categorical separation. For examples, since the 1994 establishment of a coordination function at Ministry of Justice (MoJ) occurred first, I will describe that first. But instead of immediately turning to other topics that happened just a few years after, I will continue to describe the development of MoJ's coordination function. When the topic of MoJ's coordination function is finished, I will turn to a new topic and describe the chronological development of that policy/organizational solution. In this way, I'm combining the principles of chronology and category.

3.4 Operationalization

A central part of scientific research is the linkage between concepts and observations. This linkage raise key questions about measurement validity, i.e. does "observations meaningfully capture the ideas contained in the concepts" (Adcock & Collier, 2001, p. 529). To achieve coherence between observation and idea Adcock and Collier a four-level measurement process is needed (2001). A table of how operationalization through this four-level process to my study is provided below. But first a description of Adcock and Collier's process.

On the most abstract level are background concepts (level 1). In my thesis these are the instrumental and institutional theories. Elements of these theories need to be specific formulations of systemized concepts (level 2) through a process of conceptualization. Decision-makers use organizations as tools to solve problems, are an example of a systemized concept from instrumental theory. Furthermore, one or more indicators (level 3) need to be drawn from these systemized concepts through a process of operationalization. I separate between indicators about actors and decision-making processes on one side and organizational solutions on the other. That is because the different theories provide key insights into both how actors operate and decision-making processes work, and how actual implemented organizations will look like. The final step is scoring indicators (level 4). I have chosen "yes/no" scores, although in several situations, since some processes and solutions contain many smaller policies, both yes and no can be the case, which indicate mixed scores. Adcock and Collier stresses that measurement is valid when scores derived from an indicator can meaningfully be interpreted within its systemized concept (Adcock & Collier, 2001, p. 531). In the table below I have tried to do so as coherently as possible.

In the theoretical chapter I have given indication of what observations are expected the theoretical descriptions and through concrete hypotheses. However, the derived hypotheses operate in the interface of Adcock and Collier's (2001) systemized concepts and actual indicators. In the table below, to show how the hypotheses fit in Adcock and Colliers schema, the hypotheses are placed between systemized concepts and indicators.

	The process of operationalization					
Main theories	**Systemized concepts**	**Theretical expectations**	**Indicators about processes and actors**	**Scores**	**Indicator about organizational solutions**	**Score**
Instrumental theory	Decision-makers follow a logic of consequence, purpose-oriented rationality and use organizations as tools to solve problems.	The overall expectation is that the policy-makers will be influenced by an instrumental logic and use organizations or arrangements as tools to solve problems in a rational fashion. Because security in general and ICT security in particular are characterized as wicked problems, solutions are expected to promote more collaboration and coordination.	Central actors will ensure processes that define problems and solutions ICT security, typically through NOU's or other official reports.	Yes/no	New tasks and organizations are created to solve problems of ICT security. New organizational solutions promote coordination and collaboration across organizational and sectorial boundries.	Yes/no Yes/no
	It is a dynamic relationship between specialization and coordination.	Coordination pressures/problems are expected to occur in relation to horizontal specialization principle, and coordinative solutions will be adopted to counter these issues.	The way the central government is horizontally specialized coincides with observable coordination problems.	Yes/no	New solutions promote more coordination to counter horizontal specialization principle.	Yes/no
	The set of formal structures will shape behavior and ability/performance.	The structural organization of the ICT security policy field will shape behavior and performance.	It is obserable that central actors' vertical and horizontal linkages and authority enhance and limit their behavior	Yes/no		
	Public sector organizations are characterized by its hierarchical organization and commando structure.	If the hierarchical variant of instrumental theory dominates ICT security policy, I expect strong vertical lines of command and relationship between problem-definitions, solutions and implementation, and little ambiguity.	Few actors are clearly in charge of ICT security policy Actors have common interests	Yes/no Yes/no	Solutions are closely linked to problem-definitions. Clear separations of responsibility.	Yes/no Yes/no
	Public sector organizations are characterized by a plurality of actors and negotiation.	Based on the negotiation variant I expect to see heterogenic decision-making processes with conflict of interests that results in compromises with ambiguity.	Multiple actors are involved in decision-making processes. Actors have competing interests and bargain.	Yes/no Yes/no	Solutions are result of negotiations and ambiguous about responsibility.	Yes/no

Table 2: Operationalization

Cultural-institutional theory	The social and cultural nature of organizations shape decision-making.	The overall expectation is that policy-makers will be influenced by the informal norms on how ICT security in the central government ought to be organized.	The most dominating norms of Norwegian central government, like ministerial rule, influence key actors and processes.	Yes/no	Solutions ICT security will be in line with key norms like ministerial like.	Yes/no
	Decision-makers primarily follow what is considered culturally appropriate.	New organizational solution will be based on a logic of appropriateness. Changes that threaten dominating norms are meet with resistance.	Central government actors look to solutions in according with norms like ministerial rule and responsibility principle. Solutions that oppose these norms are met with resistance.	Yes/no Yes/no	New organizational solutions corresponds with norms and attitudes about organization of the central government. Solutions that oppose dominating norms will be implemented in a weak fashion.	Yes/no Yes/no
	Culture and informal norms and not static but evolves over time in relation to its close environment.	Over time norms can evolve and cultural resistance against coordination reduce.	Problems of coordination are a reoccuring theme within the central government and its close environment. Resistance against coordination gradually reduces.	Yes/no Yes/no	Coordination policies gradually is implemented stronger.	Yes/no
	Formative years of institutional arrangements create self-reproducing patterns which promote stability, unless external shocks occur.	I expect that organizational arrangements will self-reproduce and be resistant to "real" change, unless new critical junctures create new paths.	Decisons made about coordination arrangements has lasting impact. Shocks will promote decison-making processes where institutionalized patterns are of lesser importance.	Yes/no Yes/no	New solutions are of minor character and only serve to continue existing system of responsibility. Shocks to security policy at large or ICT security will lead to drastic organizational changes.	Yes/no Yes/no
	Institutions gradually transforms with discontinuing effects.	In contradiction to the latter, I expect that changes will be of gradual transformative character.	Key actors promote many small solutions that promote coordination.	Yes/no	Many small coordination policies at put on top of existing coordination system. As more coordination measures are implemented, the coordination system is transformed.	Yes/no
Neo-institutional theory	Organizations operate in an intitutionalized environment and have to show they are acting on what is collectivly valued.	I expect that the government are sensitive to external views and seek legitimacy through symbols and myths about coordination and collaboration.	Central actors are sensitive to external views on (ICT) security policy and organization of central governments. Words like "coordination" and "collaboration" are often used in policy documents.	Yes/no Yes/no	Solutions, at least on to the outside world, promote coordination and collaboration.	Yes/no
	A legitimacy strategy is double-talk or hypocricy.	I expect that there will be a distance between talk about coordination and collaboration and actual implementation.	Same as above: Words like "coordination" and "collaboration" are often used in policy documents.		Implementation of coordination and collaboration measures are significantly weaker than .	Yes/no
	Organizations tend to resemble other units which face a same set of environmental conditions	I expect that the government will mimic organizational solutions to ICT security that are already adopted by central allied countries.	Decison-making processes focus on how other countries, in particular allied countries have organized, and give them high status.	Yes/no	Organizational solutions to ICT security mimics solutions in allied countries.	Yes/no

3.5 Validity and reliability

Validity

Internal validity in qualitative research is whether, or to which degree, research approach and empirical data reflects the purpose of the study and represents reality (Johannessen, Tufte, & Christoffersen, 2016, p. 232). It is therefore a question of internal consistency and the credibility or trustworthiness (Tjora, 2010). The most important effort to strengthen internal validity has been through collection of relevant documents about the Norwegian government's ICT security policy. The field of ICT and public security policy is highly complex, I therefore risk missing important organizational solutions or events. However, key documents refer to the same key measures or organizations repeatedly, which strengthens validity. Another issue, security policy is by nature secretive which sometimes make information scarce. This is especially the case on a more operational, crisis management level. The empirical material therefore is a bit biased in direction of preventive measures and organizational solutions where information is more open.

Triangulation or mixed methods increase probability of credible results (Johannessen, Tufte, & Christoffersen, 2016, p. 232). Ideally, interviews would have supplemented the document analysis, but for several reasons this was not applied. The scope of the analysis and number of documents studied already were a massive endeavor. For supplementary interviews to be applied rigorously at all major stages of the empirical timeframe, the number of interviews needed would have surpassed twenty. Therefore, to conduct interviews in a rigorous way would have been too time-consuming. The data loses some depth without interviews, but I still consider internal validity good due to the high number of documents and the quality of them.

Single case-studies are not suited for far-reaching generalization (Bryman, 2012, pp. 69-70). External validity in qualitative research rather centers on the generality of the study (Johannessen, Tufte, & Christoffersen, 2016, p. 233). Thus, it is a question of whether the generated knowledge is transferable to other related phenomena. As argued above, I find this case to be within the larger universe of public security, most clearly, but also within how governments handle wicked problems and of organizational trends in the central government overall. The generality or transferability is not very strong, but the generated knowledge can have implications for these larger phenomena which is discussed in the final chapter.

Reliability

Reliability brings attention to the data, data-collection processes and how reliable they are. Sound reliability is a question of whether myself or other researchers will get the same measures/results using the same methods and procedures (King, Keohane, & Verba, 1994, p.

25). Reliability is closely related to replicability, which all research should attempt to achieve (ibid). My use of only public documents gives possibility of complete replicability. The data-collection method describes above ensures transparency of the study. Therefore, I consider the reliability to be strong.

4. Empirical data

4.1 Introduction

This chapter presents the major organizational features, solutions and trends concerning the central governments ICT security policy. The next three sections describe the development of the three major organizational arrangements in the central governments ICT security policy since the 1990s until 2013. Section 4.2 describes the development of the Ministry of Justice and Police (MoJ) as lead and cross-sectoral coordination ministry for public security, which implicates responsibility for ICT security policy. Section 4.3 describes the development of National Security Authority (NSM), an agency level organization specialized on ICT security which operates in the interface of the military and civil sector. Section 4.4 relates to the lead ICT and ICT security ministry model, which was a cross-sectoral coordination model on ICT security policy at ministry level. The section also describes the (complex) relations this model had with other organizations and sectors.

Section 4.5 describes the 2013 dissolvement of the ICT and ICT security model and the ICT security responsibility's transition to MoJ. However, the section begins with the aftermath of the 2011 terrorist attacks, as it sets the stage for a second wave of changes to the field of ICT and public security policy. Section 4.6 focuses on the recent efforts to strengthen coordination capacity at both ministry and agency level. These coordination efforts have both entailed stronger coordination authority and new horizontal coordination bodies. The final section summarizes the most important organizational solutions and features. At the end, it provides a description of the major organizational trends of ICT security policy, which the analysis will be founded upon.

4.2 Organizing for public security

4.2.1 Managing principles

Public security policy is defined by four managing principles which have organizational implications. The responsibility, proximity and similarity principles were formulated in 2002 (St. Meld., nr. 17 (2001-2002)), but these principles have a long tradition in Norwegian government. In 2012 a fourth principle about collaboration was introduced as well (St. Meld., nr. 29 (2011-2012)).

The responsibility principle states that what organizations are responsible for in a normal situation also make them responsible for its security. The telecom company Telenor, for example, normally is responsible for producing telecommunication services to its customers. Because of this principle, it makes them also responsible for the safety and security

of these services. The responsibility principle is also related to overarching ministerial responsibility. For example, on top of a hospital's responsibility for the security and preparedness locally the Ministry of Health has an overall sectoral responsibility for security in the health sector.

The similarity principle states that an organization should operate similarly in a crisis as it does on a regular basis. *The proximity principle* holds that a crisis shall be handled at the lowest level organizationally. These principles are coherent in the sense that they build a foundation for a bottom-up approach to security. *The collaboration principle* gives each organization responsibility for ensure best possible collaboration with other relevant organizations in its preventive security measures and emergency response plans. The principle does not change existing lines of responsibility, but rather highlight interdependencies across organizational boundaries and sectoral borders (St. Meld., nr. 17 (2001-2002); St. Meld., nr. 29 (2011-2012)).

4.2.2 Ministry of Justice as lead ministry

The responsibility principle was in reality an old managing principle in the Norwegian government, which have formed a decentralized organization of security in the civil sector, as well as overarching responsibility placed on each ministry for its sector. A newer and contradictory trend was the emergence of stronger central managing of security in the civil sector. MoJ was made 'lead ministry' for security in civil sector already eight years prior to the first white paper on public security.

Norwegian civil security organization break with the fragmented and decentralized organizational arrangements began in the early 1990s. The policy shift was induced by the 1992 Buvik-report and its conclusion that stronger coordination through a coordinative ministry was needed to ensure a more goal-oriented and effective civil security and emergency response. MoJ, Ministry of Defense (MoD) and the Ministry of Industry were the three main candidates. The report recommended that MoJ should take this role, mainly because it already had highly relevant actors within its sector, most notably the Directorate for Civil Protection, Search and Rescue services and police authorities (NOU, 2006: 6, p. 52). Two years later, the government followed the Buvik reports recommendation, and established a coordination responsibility and function on the MoJ in all civil protection and security matters (St. Meld., nr. 48 (1993-1994); Kgl.res., 16.09.1994).

The 1994 establishment of cross-sectoral responsibility is arguably a turning point in the organization of security policy in the civil sector. However, each ministry would still have

an overarching responsibility for security in its sector (NOU, 2006: 6, p. 52). Thus, the policy did not break from the responsibility principle. The idea behind the lead ministry model was that MoJ would have an additional, secondary responsibility for all governmental sectors. These two principles are contradictorily and inconsistent because each ministry cannot have responsibility for its sector alone at the same time as MoJ has cross-sectoral responsibility. The inconsistency and rather vague formulations in the royal resolution resulted in a lack of shared understanding about what constituted MoJ's cross-sectoral coordination responsibility and function for preventive civil security.

A process to sort out MoJ's responsibility centered around improving internal control and auditing mechanisms in the following years (St. Meld. , nr. 25 (1997-1998)), which eventually led to second royal resolution on internal control and auditing (Kgl.res., 03.11.2000). The ministry was strengthened vertically with the establishment of National Security Authority, which I will elaborate more on later, and the fusion of Directorate for Civil Protection and Directorate for Fire and Electronic security into DSB. These two agencies were put to perform security-related auditing across governmental sectors, and report to MoJ (see figure 1) (Kgl.res., 29.08.2003). A sensitive question was, however, what powers would MoJ have if weaknesses in a given sector was found in the inspections. For example, the Ministry of Transportation and Telecommunication (MoT&T) showed resistance. In the input to the 2000 royal resolution on internal control and auditing argued MoT&T that voluntary counseling was sufficient cross-sectoral involved by MoJ. The result was limited to counseling and recommendations initiated by MoJ, which must still be considered a rather mild horizontal power by the lead ministry (Fimreite, Lango, Lægreid, & Rykkja, 2014).

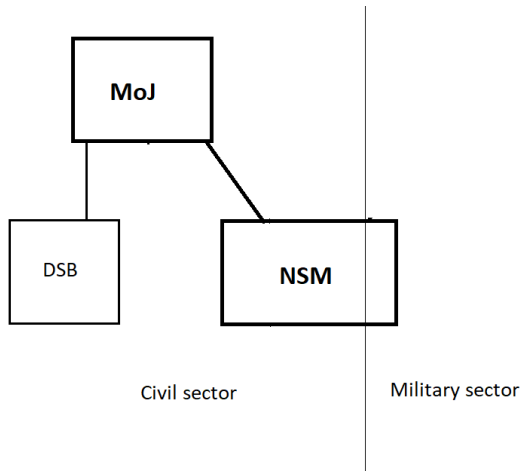

Figure 1: Map of MoJ and key overlying agencies

The uncertainties surrounding MoJ's cross-sectoral responsibility, the institutional defense of the sector-principle and the government emphasis on primarily auditing during the first years after 1994, showed an inability to reinforce and lock-in a pervasive, policy-oriented institutional arrangement. This context must be viewed in relation to the 1997 establishment of the lead ICT and ICT-security ministry model, which will be described later in 4.4.

In an effort to bring more attention to civil security and preparedness policy, MoJ was able to put down a Norwegian Official Report to look more broadly at vulnerabilities of and security threats against Norwegian society. The culminating Vulnerability report (NOU, 2000: 24) highlighted modern society's increasingly complex nature mainly due to globalization and growth of ICTs, and that these trends would only continue and make society more vulnerable. Combined with the reduced military threats and risk of war, civil protection and public security must be highly prioritized in the years to come, the report argued. The report also proposed several changes to the organization of the security sector. Among the proposals was the creation of a designated ministry of security. The proposal also entailed a stronger hierarchical model of organization, and therefore a move from the existing decentralized and network-oriented model (Lægreid og Segristad 2006). The re-organizing attempt led to a lot of institutional defense, especially by the military sector, which were able to stop the 'security ministry' idea from ever being proposed to the parliament (ibid). While the report's re-organizing attempts was rather unsuccessful, the emphasis on ICT did make a lasting impact.

Two years after the report followed the first white paper that used the term "public security". Public security was defined as the ability to maintain societal functions, and protect citizens' life, health and basic needs. The concept ranged from smaller natural emergencies, through crisis' that represent dangers to life, health, environment and material values, to larger security threats against national existence and sovereignty (St. Meld., nr. 17 (2001-2002), p. 4). The white paper recognized not only that ICT was an important societal function in itself, but also that other societal functions were highly interdependent on ICTs. Furthermore, the white paper had ICTs as the first subsection on vulnerability reducing measures which symbolized its importance in the new public security policy. Organizationally, instead of placing overarching responsibilities to a new security ministry, MoJ's position as lead ministry with cross-sectoral responsibilities was reinforced, and its role was to be further developed and strengthened. Interestingly, ICT-security policy was used to exemplify MoJ's cross-sectoral responsibility for public security: "[MoJ's coordination role] can entail coordinated considerations of which measures should be implemented in case of serious ICT failures, especially related to critical societal functions" (ibid: 102). The white paper clearly defined ICT security within the domain

of public security and thus part of MoJ's role as lead ministry. This trend becomes even more evident with the establishment of the National Security Authority and its linkage with MoJ, as I will be turning to shortly in section 4.3. However, at that time was the ICT and ICT security ministry model already operative, which is largely inconsistent with and contradictory to these public security policies. This will be more thorough described in section 4.4.

The nature of MoJ's cross-sectoral responsibilities have been contested, not only related to ICTs, but also in public security policy in general since the beginning in 1994. The 2002 white paper did not resolve these issues, but rather promised to further develop and strengthen MoJ's lead and coordination responsibility. A recurring theme in public security policy after 2002 have been strengthening MoJ. The ministry has gradually been strengthened vertically by the delegation of auditing and inspections of other sectors work on security to NSM and DSB. This have given MoJ important cross-sectoral overview. To enhance the horizontal coordination, the government introduced the ministerial coordination council for public security (St. Meld., nr. 22 (2007-2008)). It is a supplementary collegial body where all ministries are represented to bring up and discuss experiences about cross-sectoral public security. But this measure did not change the balance between sectoral responsibility at each ministry and MoJ's cross-sectoral coordination responsibility and authority. Coordination in public security policy have therefore been characterized by negative coordination rather than positive. The issue of MoJ's weak coordination powers has been labelled "the eternal coordination problem" of public security policy (Lango, Lægreid & Rykkja 2014: 73-74).

4.3 National Security Authority - A civil-military hybrid

4.3.1 Introduction

This section centers around the establishment, tasks, organization and early developments of the National Security Authority – the principal organization on agency level in ICT security policy. The section begins with a description of NSM's delegated tasks and projects, and how it operated as a coordinative ICT security agency. Then, I will turn to the topic of NSM's organizational re-design, ministerial connections and the resulting complexity and hybridity.

4.3.2 Main tasks and projects

The origin of the National Security Authority (NSM) we know today leads back to the new security law passed in 1998, which was put into force as of 2001 (Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), 1998). It contained four main regulations regarding personnel security, information security, security administration and procurements of classified material. A fifth regulation on object security was added to the law a few years later. Most

importantly, the new law gave the national security authority several tasks within civil sector as well as military. Specifically, the security authority was given tasks to coordinate preventive security measures and investigate military and civil government administration through inspections, technical investigations, monitor information systems and test possible intrusions, and perform personnel control. NSM was also given the authority to certificate crypto equipment, approve information systems, and to check and clear private firms when procurements of classified material is needed. In sum, the security law paved the way for a complex and multifunctional organization with many different tasks. Most notably concerning preventive ICT security were the tasks related to inspections and auditing on the one hand, and certification and approval of digital equipment and systems on the other. But NSM were also given ICT security tasks outside the new security law, which I will now turn to.

NSM's central role as the Norwegian government's ICT experts was already integrated in the organization before prior to the security law. In late 1990s a pilot project named Alert system for digital infrastructure (VDI) was established as a collaborative measure by the intelligence, surveillance and security services. The secretariat function was from the beginning placed at NSM. The new project placed sensors on the most critical digital infrastructures, both privately and publicly owned. If one of the digital systems was attacked, the VDI secretariat would receive information about what the attack/threat is. Then, they would be able to inform and coordinate with other operators of critical digital infrastructure so that vulnerability reducing measures can be implemented (St. Meld, nr. 39 (2003-2004), pp. 45-46; St. Meld, nr. 17 (2006-2007), pp. 161-162).

This role was further developed with establishment of CERT (Computer Emergency Response Team) in early 2000s. It was a response to a growing concern about Norway's capabilities to handle coordinated cyber-attacks on critical infrastructure and functionalities (St. Meld, nr. 39 (2003-2004), p. 45). In countries like Finland, Germany, Netherlands, Belgium, England, France and the U.S. a unit with this kind of capabilities had been established. The government argued that creating a CERT-unit would connect Norwegian authorities to a growing professional community internationally, and strengthen the national crisis management capacity against cyberattacks. However, the CERT-unit would not reduce the existing responsibility on owners of ICT systems, but rather be a supplement and ensure better coordination (ibid: 46). A stated goal for VDI and CERT was that they would include and be accessible to many important organizations in both private and public sector. However, by mid-2000s only a limited number of external participants were included in these projects (Riksrevisjonen, 2005: dokument nr. 3:4, p. 9). The CERT-unit was established and organized

in connection to VDI. The national CERT-unit has later been named NorCERT, to fit into the international CERT-community. More recently have sectoral CERTs also emerged under the CERT umbrella, like HealthCERT and FinanceCERT.

4.3.3 Organizational design

Historically, the national security authority had been organized within the military organization, specifically in the supreme command and security staff. But with all the new tasks delegated to the security authority, the question of re-organizing was brought to attention. The vulnerability report (NOU 2000: 24) recommended that this authority should be organized as a directorate organizationally underneath their proposed Ministry of Security. The Ministry of Defense (MoD) had the question of organizationally placing national security authority examined by two additional reports. Both these reports concluded – similar to the vulnerability report – that the national security authority ought to be removed from the top hierarchy of the military organization and rather be organized as a directorate because of the number of tasks and amount of responsibility within the civil sector. However, these reports recommended that the security authority was kept under MoD. Finding the organizational solution to NSM to an institutional battle between MoD and justice sector (Lægreid & Serigstad, 2006), which this thesis will not go into detail about. What more interesting is the result, see figure 2 below.

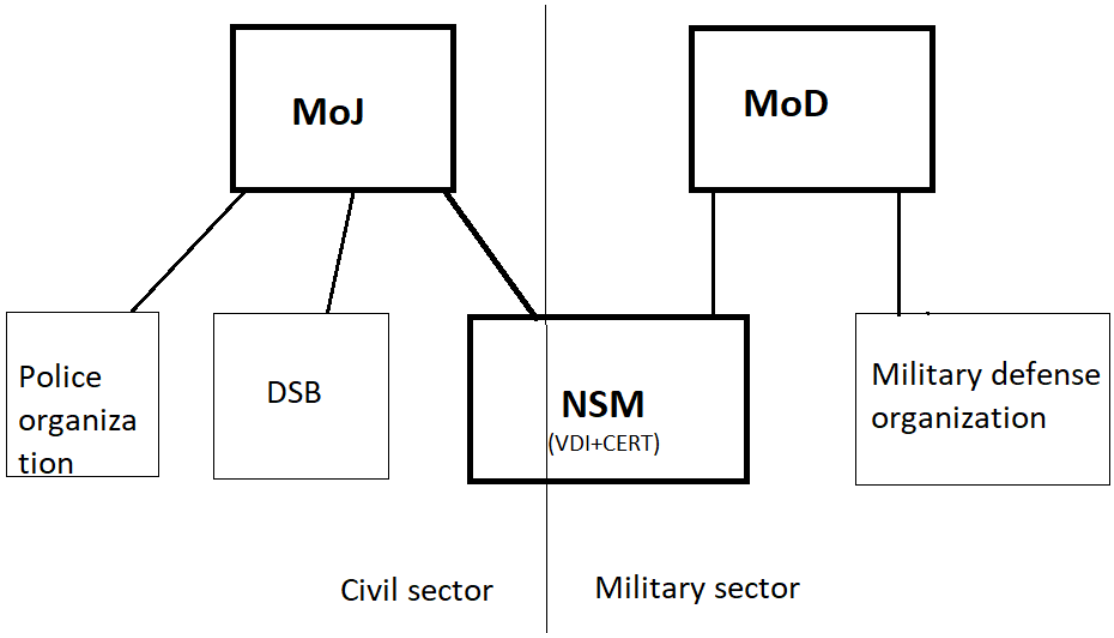

Figure 2: Map of NSM and its parent ministry organization

The result was that the National Security Authority was established as a separate agency in 2002. This brings us to the vertical and horizontal dimensions of specialization. The creation of NSM meant that it was vertically specialized as a directorate under MoJ and MoD, with

delegated authority and tasks mentioned above. It also entailed a horizontal specialization and inter-organizational separation away from the military defense organization. Thus, the organizational thinking was that NSM needed to become more autonomous from the military organization. Much of NSM's tasks were related to technical skills (especially with ICTs) which demands certain professional knowledge. This seem to indicate relevance of the process principle. Additionally, it seems like the clientele principle also was a factor because NSM was specialized in relation to owners and operators of critical and digital infrastructure. While Center for information security (CIS), which will be described in 4.4.2 was an agency level organization specialized to help municipalities, small private business' and private citizens in ICT security matters.

Although NSM is highly complex in itself, the organizational design of its ministerial management and steering only increased the complexity. As we have seen is NSM's horizontal specialization across the military and civil sector, making it an inherently civil-military hybrid. Therefore, it is a build-in tension internally in NSM concerning its priorities on military versus civil tasks and objectives. The organizational design on ministry level furthers that complexity and hybridity since MoD is only hierarchically steering NSM in military tasks and objectives, and MoJ in civil sector matters. With steering signals and policy demands divided on those same lines makes the agency arguable prone to being pulled in different directions. A more holistic approach to NSM's cross-sectoral duties might have been encourage with steering by only one ministry. That was the Vulnerability report's proposed idea, with NSM being vertically managed by their proposed security ministry (NOU, 2000: 24). Even though a Ministry of Security would have been a complex civil-military hybrid in itself, it would have entailed reduced complexity in NSM's vertical line of command. The two vertical lines to NSM are not only a unique case in Norwegian security organization. No similar solution is seen elsewhere in Norwegian state apparatus, nor internationally. The process leading to NSM's organizational design of parent ministry shows signs of competition and compromise between the military and justice sector.

The organizational design also has cultural ramification since NSM has a history as an integrated department within the military defense organization. The design also demands coordination between MoD and MoJ to ensure sound hierarchical steering of NSM and agreed upon definitions of civil and military tasks. The military and justice sectors have shown difficulties in this respect, as for example in the aftermath of the Vulnerabilities report's organizational proposals. Lack of shared understanding on what are appropriate military and

civil tasks has also been visible in the matter of object security (Riksrevisjonen, 2018: dokument nr. 3:11).

4.4 The lead ICT and ICT security ministry model (1997-2013)

4.4.1 Introduction

In this section I describe how the ICT and ICT security model unfolded. I begin with a description of the two ministries that have served this function, i.e. the Ministry of Industry and Trade (MoI&T) and the Ministry of Renewal and Administration (MoR&A), and their vertical advantages in having that role. I then turn to the vertical disadvantages of not being in neither the civil security sector nor in the telecom sector, and the resulting complexity and hybridity. Then follows a description of the Coordination committee for information security (CCIS), a secondary structure that gathers the different ICT security stakeholders. Finally, I give a summary of key trends and the organizational situation prior the 2013 dissolvement of the ICT and ICT security ministry model.

4.4.2 The two lead ministries

The institutional genesis of the ICT and ICT security ministry model dates back to December 1997 as the new Bondevik 1 government gave the Ministry of Industry and Trade this role. Previously, under the Jagland government, it was the Ministry of Planning and Coordination that had the responsibility for cross-sectoral ICT-policy, but that responsibility had not included security aspects (Kgl. res, 20.12.1996). The 1997 policy gave the Ministry of Industry and Trade (MoI&T) responsibility to identify and follow up ICT issues across sectors, and initiate and coordinate measures of transboundary character, including work on preventive IT security measures (Kgl.res., 19.12.1997). MoI&T's capacity was strengthened in 2000 with a designated department for ICT-policy within the ministry (Royal resolution June 28th 2000). On political level, an IT policy group of state secretaries from different ministries was created and led by the state secretary from MoI&T.

The responsibility principle in civil security policy makes those responsible for an organization, policy or sector also responsible for its security aspects. Thus, the new design with linkage between cross-sectoral ICT policy and ICT security policy clearly shows that the responsibility principle dominated the organizational thinking. What was new with this implementation of the responsibility principle was that it never had been used on cross-sectoral policy domains before. The establishment of the ICT and ICT-security ministry model directly contradicted the cross-sectoral coordination responsibility MoJ had been given for security in the civil sector, as described in section 4.2.2. However, the early years of MoJ's cross-sectoral

coordination responsibility were characterized by uncertainties surrounding MoJ's role. The primary focus on building MoJ's cross-sectoral role centered around auditing and control mechanism during the 1990s, and was not developed to be a more policy-oriented role until the 2002 white paper on public security. This context paved the way for the lead ICT and ICT security ministry model in 1997.

However, Ministry of Industry and Trade (MoI&T) role as lead ministry only lasted until late 2004, when the Bondevik 2 government moved the ICT and ICT security responsibility to Ministry of Modernization (MoM) – a ministry with primarily an administrative portfolio (Kgl.res., 01.10.2004). The new Stoltenberg government in late 2005 renamed the ministry to Ministry of Renewal and Administration (MoR&A), which became lead ministry until 2013 when the model was abolished.

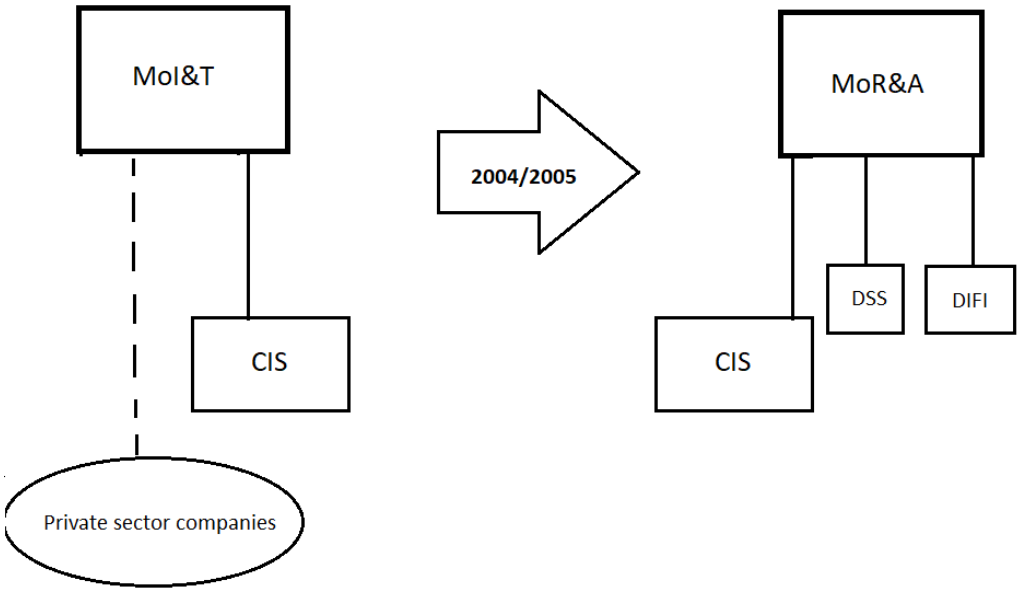

Figure 3: Map of the two lead ICT security ministries

The Ministry of Industry and Trade's only vertically connected organization working with ICT-security was the Center for Information Security (NorCIS). It was established in 2002, and was a direct follow-up from the 2000 vulnerability report (White Paper nr. 17 (2001-2002)). The center for information security's role was primarily to promote awareness, knowledge and "safety culture" in society about ICT threats and vulnerabilities through information work and counseling. Their target groups were (and still are) small business, municipalities and private citizens (White Paper nr. 17 (2006-2007): 162). Thus, CIS was horizontally specialized not only

according to the purpose principle (ICT security), but also according to clientele. While NSM clientele was owners and operators of critical and digital infrastructure. The center was administratively placed under Ministry of Industry and Trade, but it was organized with extensive autonomy from the ministry level. Hence, the long vertical line in figure 3. In 2010 it was organized as a foundation to further enhance the center's autonomy. As MoR&A became lead ministry, they also took over administrative responsibility for CIS.

The two ministries that have filled the role of lead ministry for ICT and ICT-security were characterized by different vertical advantages, while sharing a key vertical disadvantage. In short, the lead ministry's task to digitalize both public and private sector, and take care of the security aspect of this development. MoI&T's vertical advantages was its preexisting sectoral responsibility for private sector policy, and had therefore extensive relations to major companies that was driving the ICT transformation. Highly relevant example of that was that MoI&T managed the state's shares in Telenor, Norway's largest telecom company. MoR&A, on the other hand, had vertical advantages in their sectoral responsibility for government administration. With underlying agencies like Government Service Organization (now Government Security and Service Organization - DSS) and Agency for Public Management and eGovernment (DIFI) gave MoR&A tools to push an ICT and security agenda across government.

However, the transition from MoI&T to Ministry of Modernization (later MoR&A) as lead ICT and ICT-security ministry was not flawless, especially regarding contact and dialog with private sector enterprises (Riksrevisjonen, 2005: dokument nr. 3:4). Within the MoI&T was a designated section to follow up ICT in the private sector. At the same time, Ministry of Modernization was supposed to push measures from a new information security strategy which included measures targeted private sector actors. But, according to the Auditor General neither ministry had been in contact the private sector organizations during the investigative period (ibid). The uncertainties about which ministry was responsible for private sector dialog were likely due to the institutionalized relation between MoI&T and the private sector, while the more government administration-oriented Ministry of Modernization had little or no preexisting relation private sector relations.

4.4.3 Relation to other organizations and sectors

The designated ICT-security ministry solution arguably followed Gullick's purpose/sector principle. But, normally are ministries that are horizontally specialized on a certain policy field also vertically connected to its most relevant agency-level organizations. However, a shared

structural feature for MoI&T and MoR&A was that neither were vertically connected to the civil security sector nor the telecom sector. These sectors were instead led by their own ministries. I will begin with the relation the civil security sector, before going into the telecom-sector, and then summarize the resulting complexity.

As already described, MoJ was the lead ministry for the civil security sector and was vertically linked to NSM, the key ICT-security agency, together with MoD. This was already a complex and hybrid arrangement. With MoI&T/MoR&A as lead ministry for ICT-security, the government had created an even more complex arrangement where the lead ICT-security ministry lacked direct vertical connection to the specialized agency-level, but was still supposed to push policies horizontally across government sectors. This arrangement did not only put MoI&T/MoR&A in a weak position to be lead ministry, but also made MoJ's overarching public security responsibility uncertain regarding ICT.

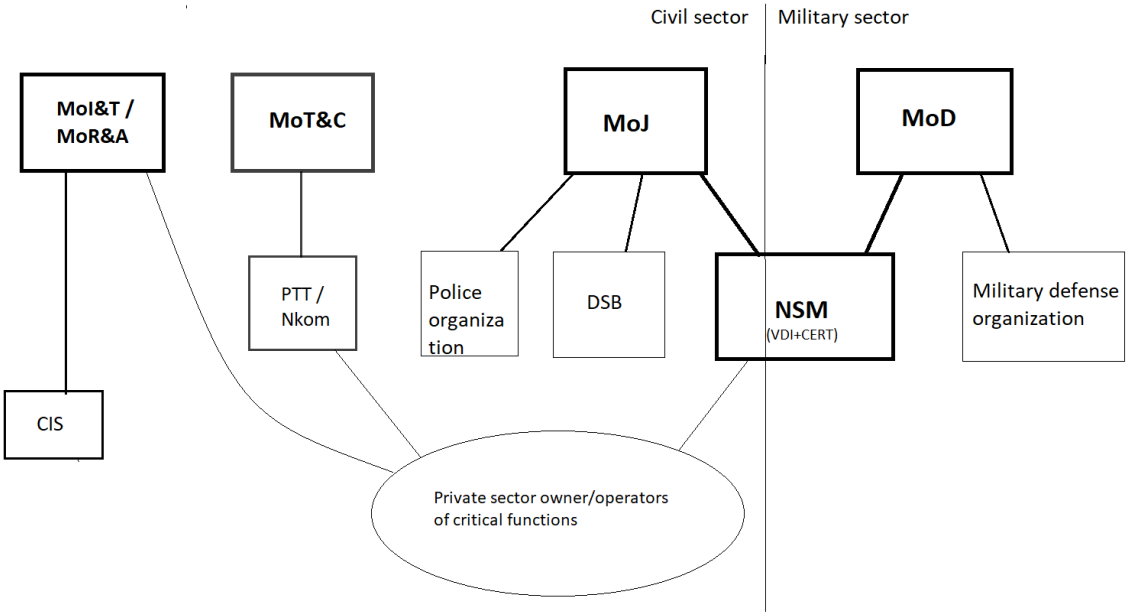

Figure 4: Map of key ICT security actors

ICT-security is also closely related to the telecom policy which is a horizontally separated policy field that is led by its own ministry. The Ministry of Transportation and Communications (MoT&C) had (and still have) sectoral responsibilities for electronic communications (telecommunications and internet). With the privatization of telecom market in the 1990s followed policies and regulation to ensure functionality and security. With policies like 2001 white paper on telecom-security and preparedness and the 2003 law on electronic communications, made the underlying Post and Telecommunication Authority (PTT) – now National Communications Authority (Nkom) – the main regulative body (St. Meld., nr. 47

(2000-2001); Lov om elektronisk kommunikasjon (Ekomloven), 2003). This included security aspects in the (private) communications sector.

4.4.4 Coordination committee for information security (CCIS)

The most notable organizational solution to support the lead ICT and ICT security model was the Coordination committee for information security (CCIS). It was developed by MoI&T, MoJ and MoD when they worked on the 2003 strategy for information security (Forsvarsdepartementet, Nærings- og handelsdepartementet & Justis- og politidepartementet, 2003). The Coordination committee for information security (CCIS) consisted of representatives from the ministries of defense, justice, transportation and telecommunication, and industry and trade. Agency level actors like Directorate for Civil protection (DSB), NSM, Post and Telecommunications Authority (PTT) and Data Protection Authority was also included. The main tasks for the committee was coordination of auditing functions, ensure coherent development of policies, laws and regulations, and to be an advisory body on how to secure critical infrastructures. MoI&T led the committee, with MoJ as deputy leader (St. Meld, nr. 17 (2006-2007)). Ministry of Modernization, and later MoR&A, took over the leadership of the committee as the ICT responsibility was moved. This coordination arrangement lasted until 2013, i.e. as long as the ICT and ICT-ministry model lasted.

The establishment of the CCIS indicates that the ministries behind the information security strategy realized that the lead ICT and ICT security model lacked vertical connections to relevant actors. The organizational solution, then, was a secondary governmental structure which gathered relevant stakeholders from across sectors and administrative levels. With the lead ICT and ICT-security ministry as chair of the CCIS, MoI&T (and later MoR&A) gained some vertical coordination powers over the ICT-security sector. However, it was in a collegial way. This complex and network-oriented organizational design seem also heavily based on positive horizontal coordination. An example on how lead ICT and ICT security ministry model through the CCIS was able to lead the policy field through positive coordination was the 2006 white paper on ICT and digitalization policy (St. Meld., nr. 17 (2006-2007)). It contained subsection about ICT-security policy that described responsibilities of NSM, CERT, VDI and PTT, in which neither was under MoR&A authority in the traditional hierarchical sense.

4.4.5 Summary of organizational set up

The complex organizational design of ICT security at ministry level did receive public concerns and skepticism. Most prominent were the reports by The Office of the Auditor General (Riksrevisjonen, 2005: dokument nr. 3:4) and Official Norwegian Report *The infrastructure*

report (NOU, 2006: 6). Both reports had quite similar remarks about the organizational solutions. One element was the many actors involved in ICT security, another was the lack of clear responsibilities and overlapping duties. Especially was the number of overarching ministries emphasized as a source of confusion by actors involved. The internet serves as a prime example of the existing confusion, complexity and hybridity in the organization of ICT-security policy-field. MoJ had an overarching responsibility for all critical infrastructure and functions, while MoI&T/MoR&A had overarching responsibility for ICT security, and Ministry of Transportation and Communications (MoT&C) had sectoral responsibility to govern the law of electronic communications in which the internet was subjected (Riksrevisjonen, 2005: dokument nr. 3:4).

The government's response to the concerns raised by the Auditor General and Infrastructure report led to little organizational changes. The responsibilities of the agency level organization were attempted to be clarified, but without any major changes (St. Meld, nr. 17 (2006-2007)). The lead ICT and ICT security ministry model continued with MoR&A in the role, and in charge of CCIS, until 2013. And the 2008 white paper on public security promoted more coordination between the existing organizational design instead of re-organization (St. Meld., nr. 22 (2007-2008)).

4.5 Responsibility for ICT security transitions to Ministry of Justice

4.5.1 Post July 22nd 2011 policies

The terrorist attacks on July 22rd 2011 in Oslo and Utøya was a national tragedy which killed 77 people and left many more injured. It was also an external shock to the public security policy field. The following Inquiry Commission did not bring attention to lack of capacities or structural aspects. Rather, the Inquiry Commission argued leadership, culture and attitudes towards recognizing risk, implement existing plans, coordination and collaboration and willingness to clarify responsibilities were the main problems (NOU, 2012: 14).

At first, the name of Ministry of Justice and Police was changed to Ministry of Justice and Public Security to emphasize the ministry's responsibility for public security (Kgl.res., 11.11.2011). It was also stated that the Ministry's responsibility for public security would be increased. The ministry would be, on default, lead ministry in crisis situations, and its role in promoting security measures in government organizations would be strengthened. This was followed up half a year later with a new white paper and royal resolution (St. Meld., nr. 29 (2011-2012); Kgl.res., 15.06.2012). The royal resolution of 2012 merged the royal resolution from 1994 (about JD's coordination function) and royal resolution from 2000 (about internal

control and auditing). The policy documents highlighted MoJ role in ensuring that public security measures and emergency response was coordinated and unified across sectors. It entailed promoting security work across ministries and be the driving force in identifying issues where more collaboration is needed or grey areas where responsibilities need clarification. Furthermore, a fourth managing principle introduced called the coordination principle.

However, the constitutional responsibilities of the sectoral ministries were re-emphasized, thus preserving the major institutional balance between ministerial sector responsibility and cross-sectoral coordination. It seems, therefore, that the policies on ministerial level in the aftermath of terrorist attacks were dominated by symbols with the renaming of MoJ, its role as "driving force" and the introduction of the collaboration principle as the most notable examples. Attention to security culture and cross-sectoral collaboration culture also was significant (St. Meld., nr. 29 (2011-2012); Justis- og Beredskapsdepartementet, 2013).

4.5.2 Ministry of Justice gets ICT security responsibility

In the years following July 22rd 2011 brought a lot of attention to public security policy and MoJ's responsibilities, but much was related to countering terrorism, emergency police and object security – and leadership, attitudes and culture. However, regarding ICT-security, a crucial change was announced in the new national strategy for information security introduced in December 2012. It said that "*the Ministry of Justice and Public Security will take over and further develop the responsibility for ICT-security in society*" (Justis- og beredskapsdepartementet, Forsvarsdepartementet, Samferdelsdepartementet & Fornyings- & administrasjonsdepartementet, 2012). This was followed up a few months later with a designated royal resolution (Kgl.res., 22.03.2013). I will come back to what this change constituted, but first let's look closer at the contextual drivers behind this change, which can be characterized by two forces. One is the long institutional path of ICT security with accompanying feedback and reproduction mechanisms. The other is related to the shock induced by the 2011 terror. I will begin with the former.

As previously described was concerns related to the complex organization of ICT security expressed already in 2005 and 2006 (Riksrevisjonen, 2005: dokument nr. 3:4; NOU, 2006: 6). But at that time was the government able to reproduce and reinforce the organizational arrangement through minor adaption. However, more concerns and criticism followed, especially by the Auditor General. The yearly report of 2009 revealed shortcomings in several government ministries sectoral responsibility for information security (Riksrevisjonen, 2010:

dokument nr. 1). This included MoR&A, who additionally was criticized for its cross-sectoral work. The MoR&A's lack of overview and plans over prioritized cross-sectoral ICT security measures was highlighted by the Auditor General's report. Furthermore, the report found that several ministries were unfamiliar with CCIS work with common standards, methods and tools for information security (ibid: 128). Additionally, NSM reported the following year that the state of ICT security was insufficient (Nasjonal sikkerhetsmyndighet, 2011). These long-term feedbacks were increasingly negative, and played right into the process of developing a new ICT security strategy which started prior to the terrorist attacks.

Then the terrorist attacks happened, which led to examinations and scrutiny into the civil security sector. MoR&A coordination abilities was heavily questioned, although not in ICT-related matters. MoJ was under similar pressure. ICT security was, however, included in the internal Bleikelia report appointed by MoJ. The report looked broadly into the responsibilities for public security and preparedness, and among the recommendations was clarification about ICT security (Fimreite, Lango, Lægreid, & Rykkja, 2014, p. 70).

MoJ's new ICT-security responsibility constituted design of national policies and regulations for ICT security in both public and private sector, as well as national strategies and action plans (Kgl.res., 22.03.2013). MoJ received budgetary responsibility of Center for information security (CIS). Dialog with private sector organizations and their NGOs, and participation in ICT security-related international fora was also MoJ's new responsibility. The royal resolution also emphasized NSM's role in supporting the ministry. The change meant that MoR&A was organizationally out of ICT-security picture. CCIS was also abolished. However, MoR&A kept several its ICT responsibilities and pushed digitalization policy across public sector, but without ICT security policy as its overarching responsibility. With Gulick's (1937) specialization principles in mind, does this change indicate horizontal de-specialization as ICT security was integrated into MoJ's public security portfolio. Figure 5 below illustrate the key empirical events of cross-sectoral responsibility for ICT security at ministry level.

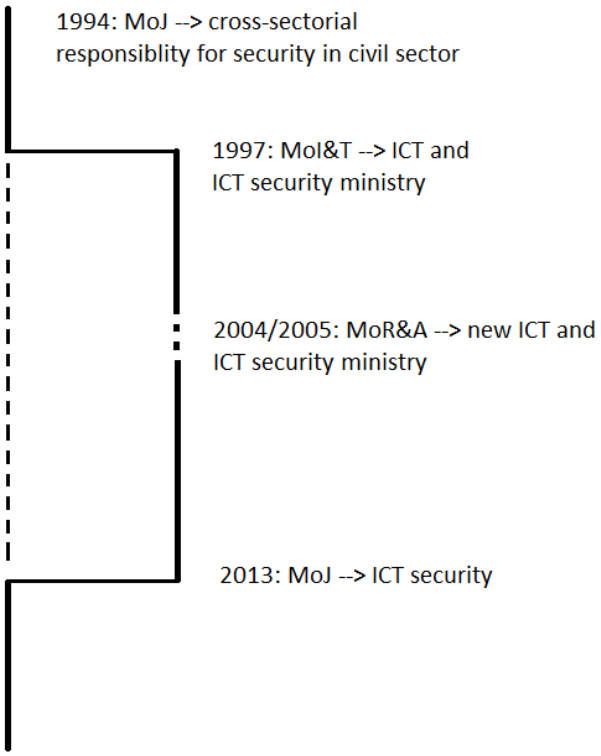

Figure 5: Timeline of cross-sectoral responsibility for ICT security

4.6 Stronger coordination measures

4.6.1 Strengthened coordination authority

One of the first measures was internally in MoJ where an ICT-security section within the department of public security was established in 2015. More importantly, the ministry ordered an Official Norwegian Report on digital vulnerabilities (NOU, 2015: 13), which would turn out to be highly influential. The report's foremost concern was technical, which emphasized that almost all critical societal functions are dependent on Telenor's core net. The report also emphasized the transboundary character of digital value chains and vulnerabilities, and the need for transboundary measures. They observed that the different sectors have been struggling to concur on implementing these kinds of measures, and argued for a stronger MoJ with abilities to push through cross-sectoral measures. The report also argued for strengthening ICT competence in sectoral auditing bodies, improved public-private collaboration and adoption of international ICT-security standards.

The NOU's (2015: 13) desire for stronger cross-sectoral abilities was nothing new. It rather followed a trend started by the Buvik report in 1992 and continued by the Vulnerability report (NOU, 2000: 24) and the Infrastructure report (NOU, 2006: 6). However, the latest

measure to address MoJ's coordination problem stands out from any of the previous efforts. MoJ was given authority, within the civil sector, to determine requirements to the ministries work on public security and national standards on ICT-security (Kgl.res., 10.03.2017). The policy also brought MoJ's responsibility for ICT-security together with its responsibility for public security. Hence, it formalized the horizontal de-specialization of ICT security and integration of ICT security to the overall public policy that was introduced in 2013. But most importantly, it gave MoJ for the first time the ability to instruct other ministries in public security policy. As previously mentioned, MoJ's horizontal coordination powers was limited to counseling and recommendations. Hence, this policy represents a shift in institutional balance between ministerial sector responsibility and cross-sectoral coordination. Analytically, as figure X shows, gave the new policy a hierarchical dimension with "hard tools" for MoJ to employ in its ministry level coordination effort. However, the ministries sectoral responsibilities are still emphasized in the 2017 royal resolution. I will continue with describing the two organizational tools MoJ established to execute its enhanced role as lead ministry, and then turn to three networks centered around NSM on agency level.

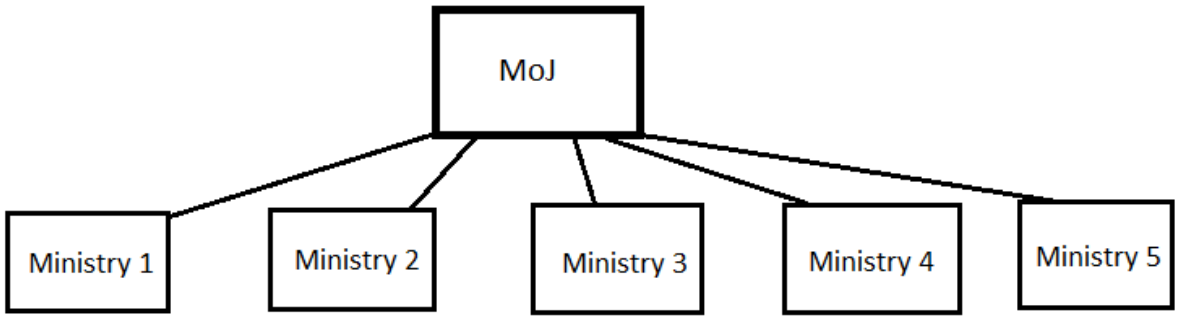

Figure 6: Map of MoJ's increased authority across ministry level

4.6.2 New organizational arrangements

Ministry level

When MoJ received ICT-security responsibility in 2013 was not any new horizontal structures on ministry level immediately established. However, after the 2017 royal resolution about MoJ's coordination powers two organizational bodies was established. First was the *Network for national ICT security*. The body is led by MoJ and all ministries are represented. The network's function to ensure that strategically important ICT-security issues can be discussed and coordinated by the central government. But it also an arena where Ministry of Defense can bring important questions related to civil-military cooperation, and for Ministry of Foreign Affairs to coordinate Norwegian positions in international cyber politics (NOU, 2018: 14). The

network bears many of the same features as the broader public security network established in 2007. The second organizational body is the *Forum for national ICT-security.* In this body MoJ gathers the ministries of Defense, Fisheries and Trade, and Foreign Affairs, together with major private sector companies, industry sector NGOs and academia. The forum serves as an arena for public-private dialog where strategic questions related to digital threats and ICT-security policy can be discussed (Ibid). Civil-military, public-private and international collaboration have been three goals and dimensions of coordination in public security policy since early 2000s (St. Meld, nr. 39 (2003-2004)). The *forum* seems designed with all of these dimensions in mind.

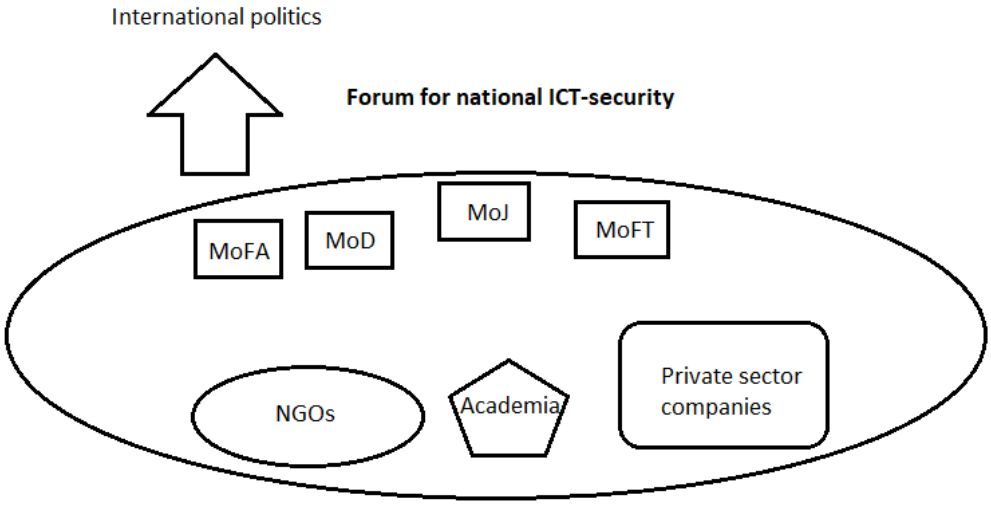

Figure 7: Map of Forum for national ICT security

Agency level

On agency level three coordination bodies are initiated in recent years to improve preventive ICT-security capacity. First, the *National cyber-security center* was initiated and led by NSM. This new body established during the fall of 2018 gathers a wide range of actors to discuss, council, and develop measures to protect critical national functions, public administration and private sector from digital threats. The center involves police and intelligence service, and collaborate with digital security experts from the most relevant private actors in the power, finance, health, and telecom sectors, as well as sector authorities, academia and international partners (Nasjonal sikkerhetsmyndighet, 2018). This is a supplementary body with little hierarchical power. Its primary function seems to be oriented towards building down sectoral barriers and create common understanding and collaboration across government and private sectors. It has resemblance with MoJ's forum, but goes even further in its outreach, and shows a tendency from ICT-security actors to use more network-oriented approach. Internationally have similar centers been established in Denmark, Netherlands and Great Britain.

The second coordination effort is within the police and security agencies. A few years back a body was created to bring NSM, the intelligence service and the police security service (PST) together to collect and provide essential information about threats and vulnerabilities in cyberspace. This information is intended for to serve both operational and strategic leadership in decision-making. This organizational body was named Cyber coordination group, and was led by NSM. In 2016 the body's mandate was broadened, and changed name to Common cyber coordination center. and the national criminal investigation service (Kripos) was permanently included (St. Meld., nr. 10 (2016-2017), pp. 67-68). The purpose includes sharing information and coordinate resources in case of major cyber-attacks where the perpetrator has, or is believed to have, connection to foreign states (NOU, 2018: 14, p. 30). Information about this coordination efforts is very scarce due to its secrecy, but it shows a trend with increased focus on supplementary horizontal organizational solutions to ICT-security threats, and that NSM are at the center of these measures.

The third and final horizontal coordination effort in recent years is the related to auditing and the 2017 update of the security law. It included that sectoral auditing authorities will get responsibility to audit security measures in its sector. To ensure strengthened ICT-security competence and common methods in the sector authorities, MoJ ordered NSM to establish a coordination arena with these auditing authorities. The Holte-report argued for inspiration by the government's previous success with a unified health, environment and security regulation which was orchestrated by the labor authority (NOU, 2018: 14, p. 91)

These organizational arrangements show how the ICT security sector are developing in an increasingly network-oriented fashion. They are also heavily rooted in NSM which shows how the organization is further developing its multifunctional and hybrid character.

4.7 Summary of empirical data and major organizational trends

This chapter been directed to answer the first research question:

- *What are the major organizational trends in the central government's ICT security policy since 1990s until 2018?*

In order to figure out what the major organizational trends of ICT security have been, I have described the most prominent organizational features and solutions of the policy field in chronological order. Firstly, a table with all the central policies, reports and changes are provided, before turning to a summary of these organizational features and solutions. Secondly, four major trends are described which is the starting point for the analysis in the next chapter.

Policy documents					WP nr 47 2000-2001	WP nr 17 2001-2002	WP nr 37 2003-2004		WP nr 37 2006-2007	WP nr 22 2007-2008		Info-security strategy 2012			WP nr 10 2016-2017	WP nr 38 2016-2017	
		RR 1994	Security law 1998		RR 2000		Info-security strategy 2003			Info-security strategy 2007		RR 2011 + 2012	RR 2013		revisioned Security law RR 2017		
Reports	Buvik 1992				Vulnerability 2000		Auditor General	2005	Infrastructure 2006	Auditor General	2010			Digital vulnerabilities 2015			Holte 2018
NSM				VDI 1999	Re-design 2001		CERT 2003							CCG 2015		Coordination arena (audit) 2017	Nat. cyber sec center 2018
Lead ICT & ICT security ministry			Creation at MoI&T 1997				CCIS 2003	MoM--> 2004	MoR&A 2005				END				
MoJ		Coordination function 1994			Internal control 2000					Coordination council 2007			ICT security transitions 2013			Network+forum More authority 2017	
Timescale	1990				2000						2010						2018

Abbreviations
WP = White paper
RR = royal resolution

Table 3: Central policies, reports and changes

Summary of prominent organizational features and solutions

The empirical data has shown that the 1994 establishment of a cross-sectoral coordination function at MoJ represents the initial break from the original decentralized system of public security (Kgl.res., 16.09.1994). However, the cross-sectoral responsibly was an addition to the existing system ministerial rule and responsibility principle. Thus, it created a complex arrangement with build-in uncertainty and tensions, in particular about the balance between the ministries' sectoral responsibility on one side, and the level of cross-sectoral authority at MoJ on the other. MoJ gradually strengthen its position as lead ministry of public security with 2000 royal resolution (Kgl.res., 03.11.2000), improved agency level support from DSB and NSM, and a more clearly defined lead ministry responsibility in 2002 white paper (St. Meld., nr. 17 (2001-2002)). However, the cross-sectoral coordination authority was limited to counseling and recommendations, and therefore relatively weak.

The 2002 white paper for the first time defined the concept 'public security, and, highly important to this study, critical functions and infrastructure were included in the definition. Since many critical functions and infrastructure were (and increasingly are) digital, MoJ's lead ministry function became intertwined with ICT security. However, another cross-sectoral coordination function was established at ministry level between MoJ's initial coordination function in 1994 and its broadened mandate in the early 2000s. The 1997 establishment of the lead ICT and ICT security ministry model connected cross-sectoral ICT policy with security aspects (Kgl.res., 19.12.1997). MoI&T was the initial ministry to hold that role, until MoR&A took over in mid-2000s (Kgl.res., 01.10.2004). The model lasted until 2013 (Kgl.res., 22.03.2013). In that period, the government operated with a complex and inconsistent double cross-sectoral coordination system at ministry level in ICT security matters. The central feature of both MoI&T and MoR&A was their lack of structural connection to the security sector and its auditing agencies. The complexity at ministry level was reduced when the ICT and ICT security model was abolished, and ICT security policy was transferred to MoJ's public security portfolio in 2013.

At agency level became National Security Authority (NSM) the key organization. The 1998 security law delegated a wide range of security task to NSM, which went across the military and civil sectors, and across public and private sectors (Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), 1998). Many of these tasks were ICT security related. NSM was also delegated ICT security tasks outside of the security law, like administrating Norway's Computer Emergency Response Team (CERT) (St. Meld, nr. 39 (2003-2004)). This was also a secondary coordination structure on top of the existing decentralized responsibility

system. NSM's civil-military nature resulted in a unique dual parent ministry model, shared between Ministry of Defense (MoD) and MoJ. Although NSM is characterized by its highly complex and hybrid design, its advantages are also prominent. Since NSM operate in the interface of the military and civil sector they are the ICT security organization independent of an incident or threat should be considered within the category of public security (civil) or state security (military).

During the last few years of the empirical time-frame have the field of ICT security seen an increasing use of network-oriented coordination measures centered around MoJ at ministry level and NSM at agency level (St. Meld., nr. 10 (2016-2017); NOU, 2018: 14). Some of these arrangements are directed towards coordination across government, while others are gathering actors from private sector and civil society. Another significant development in recent years is that MoJ has received increased coordination authority. The 2017 policy gave MoJ authority to determine requirements and national ICT standards (Kgl.res., 10.03.2017). This marks a substantial shift in the institutional balance between the ministries' sectoral responsibility, and the cross-sectoral authority at MoJ.

The major trends

Many patterns and trends in the empirical material could be highlighted. I will bring attention to four major organizational trends in the central governments ICT security policy. These trends are:

1. *The central government has been organized according to two contradictory principles since mid-1990s*.
2. *Coordination of ICT security policy at ministry level was enforced by two actors from 1997 until 2013.*
3. *The key ICT security agency (NSM) uniquely operates in the interface of the military and civil sector*.
4. *ICT security policy is characterized by slow developments, but the policy field has gradually developed in direction of stronger lead organizations (MoJ and NSM) and increased use of network-solutions*.

5. Analysis

5.1 Introduction

In this chapter I attempt to answer the second research question asked in chapter one.

- *How can instrumental, cultural-institutional and neo-institutional theory explain these trends?*

I will use the tools provided by the theories described in chapter 2 on the empirical data presented in chapter 4. The analysis is separated into subchapters according to the three main approaches of instrumental theory, cultural-institutional theory and neo-institutional theory. The four major trends described above are analyzed within each of these subchapters.

Some important clarifications: Some key empirical events are intertwined in the major trends. This create danger of analyzing these events two or more times. To avoid that, I have chosen to center the first trend around the contradictory nature of the two main organizing principles and its consequence. Therefore, MoJ's increased coordination authority in 2017 is not emphasized in the analysis of the first trend, but rather put in the fourth trend since it is a key event underlining the gradual development of stronger lead organizations. Similarly, the trend concerning the double cross-sectoral coordination system emphasizes the creation and continuation of that system, while the transition of ICT security to MoJ is addressed in the fourth trend.

5.2 Instrumental theory

The central government organize according to two contradictory principles

The organization of ICT security policy, and public security at large, are faced with fundamental challenges of specialization and coordination. One central organization cannot have responsibility for it all. Thus, responsibility for security must be decentralized. At det same time, responsibility and accountability at central government level is also needed to coordinate, ensure a more holistic approach and coherence in policy. The empirical data shows that ICT security policy has been organized according to two contradictory principles. The first principle has been the responsibility principle which make organizations responsible for a policy or service-delivery in a normal situation are also responsible for its security aspects. At ministry level, this organizing principle has made each ministry responsible for security in its own sector. The other principle is a horizontal coordination principle which place responsibility for security across sectoral boundaries at one or two ministries.

The ministerial responsibility of civil security had been relatively unchallenged until the

early 1990s. With the 1992 Buvik report a central expectation in instrumental theory about coordination problems was first brought to light. Which principle of horizontal specialization a set of organizations are organized according to, will affect coordination pressure. Also, the degree of specialization will affect the degree of coordination pressure (Gulick 1937, Egeberg 2012). The ministerial rule system entailed that ministries were horizontally specialized, and each ministry coordinated its sector vertically. The accompanying managing principle for security organization followed the same line of organizational thinking. The Buvik report in the early 1990s (NOU, 2006: 6, p. 52) argued in line with theoretical expectations, the result was a fragmentated system with horizontal coordination problems at ministry level. Also, most official reports have argued similarly and called for stronger horizontal coordination to revolve the coordination problem (NOU, 2000: 24; NOU, 2006: 6; NOU, 2015: 13). Many horizontal coordination measures have been adopted in attempts to reduce these problems (Kgl.res., 16.09.1994; Kgl.res., 03.11.2000; St. Meld., nr. 17 (2001-2002)). To a large degree these coordination measures have followed an instrumental logic in the sense that organizational solutions have tried to promote more horizontal coordination. However, the principles of ministerial rule and cross-sectoral coordination do not easily go together.

The organization of horizontal coordination functions placed at MoJ and MoI&T/MoR&A can to a large extent be characterized as lead agency models (Boin, Busuioc, & Groenleer, 2014). The model entails to concentrate policy capabilities on a transboundary issue to one or a limited number of organizations in a mixture of hierarchy and network (ibid: 11-12). The network elements relate to the lead agency's multiple connections to other relevant organizations. While, the hierarchical elements are associated to its ability to impose control on other organizations in the network (Christensen, Lægreid, & Rykkja, 2016, p. 893).

The contradiction between these two main principles are illustrative with the dimensions of specialization and coordination (Gulick 1937, Egeberg 2012). The ministerial principle, as already touched upon, is characterized by horizontally specialized ministries, and that each ministry coordinate its sector vertically. While, the coordination responsibility in its pure form entails vertical specialization to MoJ and MoI&T/MoR&A above the other ministries and horizontal coordination across ministry level. That is the opposite of the former. The result has been constant tensions about authority between these two contradicting principles of organizing civil security because they cannot operate fully at the same time.

In the implementation of these two principles at ministry level a central feature has been weak authority of the lead organizations. The structural dimensions of specialization and coordination (Gulick 1937, Egeberg 2012), and the negotiation variant of instrumental theory

(Christensen et. al. 2007: 34, 43-44), offer important insights. Since the central government primarily has been organized according to the ministerial rule system it makes all ministries heavily involved with coordination of security policy (within its sector). Therefore, multiple actors are involved, which brings relevance to the negotiation variant. The negotiation variant emphasizes that decision-making processes reflects conflicts of interests, which leads to bargaining, compromises and ambiguous results (ibid). From this perspective it is observable that a horizontal coordination function at ministry level placed on MoJ was in conflict with the security responsibilities at all the other ministries. To manage this conflict of interests it seems like the resulting compromise was an attempt to do two things at the same time: To keep the sectoral responsibilities and establish a cross-sectoral coordination function.

Since the negotiated policies during the 1990s and 2000s (Kgl.res., 16.09.1994; Kgl.res., 03.11.2000; St. Meld., nr. 17 (2001-2002)) did not reduce sectoral responsibilities of all ministries, MoJ's authority was limited to counseling and recommendations. Therefore, the organizational balance has given primacy of ministerial responsibility, while the cross-sectoral coordination responsibility has been of secondary character. Thus, the lead ministries ability to impose control over the other ministries has been limited. Because of that secondary nature, uncertainty about the MoJ and MoI&T/MoR&A responsibility across sectors has characterized ICT and public security policy field.

On agency level, coexistence of responsibility principle and coordination principle is also evident. One of NSM's key ICT security tasks were related to coordination. Most prominent coordination projects are the interconnected Alert system for digital infrastructure (VDI) and Computer Emergency Response Team (CERT) (St. Meld, nr. 39 (2003-2004); St. Meld., nr. 17 (2006-2007)). In short, VDI refers to the sensor system placed on critical infrastructures and organizations in both private and public sector. The sensors provide information about the digital threat. CERT is a continuation of VDI offering increased coordination capacity to other operators or owners of critical digital infrastructure in case of coordinated cyber-attacks (ibid). Thus, in relation to the lead agency model elements, VDI and CERT connect key operators and owners of critical digital infrastructure in a network.

There are important similarities to the creation of the cross-sectoral coordination function at MoJ discussed above. The decentralized and fragmented nature of ICT security was defined as a problem. Also, the creation of the coordination function did not remove the lines of responsibility put in place by the responsibility principle (St. Meld, nr. 39 (2003-2004)). Therefore, it seems like two contradictory systems similar to the ones on the ministerial level. However, the inconsistency and tensions between the responsibility principle and the

centralized coordination is not as observable, and therefore a key difference. The contradiction at ministry level fuels tensions about authority and decision-making power. On the more operational level it seems like the coordination done by NSM through VDI and CERT is more centered around flow of information about occurrences and vulnerability reducing measures within the network of organizations. The coordination seems to operate more smoothly. Whether NSM's coordination can be considered a pure network arrangement (Klijn & Koppenjan, 2012) is uncertain. NSM is formalized as the central node in which information flows through. NSM's positions seems more formal than a "shadow of hierarchy" (Christensen, Lægreid, & Rykkja, 2016, p. 893). It rather seems like a lead agency (Boin, Busuioc, & Groenleer, 2014) where NSM's lead function is more centered around flow of information within the network and less about imposing hierarchical control. With the reduced hierarchical elements it seems to reduces tensions with the responsibility principle.

From the perspective of complexity and hybridity the introduction of coordination policies is very interesting. Structural complexity takes us back to the dimensions of vertical and horizontal specialization, where high complexity entails strong degree of both types of specialization (Christensen & Lægreid, 2011; Egeberg, 2012; Gulick, 1937). To begin with the consequences of the responsibility principle first. It placed responsibility for security on every organization, with an overarching sectoral responsibility on each ministry. With the high number of organizations involved, the responsibility principle must be considered complex in itself, although the majority of interaction (coordination) is vertical between each ministry and its sector organizations. With the introduction of the coordination principle each sector received an additional set of scrutiny by the security sector. The result was more actors, interactions and information flows which led to increased structural complexity of civil security organization. Therefore, complexity must be considered increased.

Complex organizational arrangements don't have to be hybrid, but when complex organizational arrangements lead to lasting tensions and inconsistencies they result in hybridity (Christensen & Lægreid, 2011, p. 410). It is evident that the mixture of these two organizational principles at ministry level are inconsistent and contradictory to each other. The tension is particularly related to the question of authority which pull in different directions. Because of these lasting, build-in tensions, the organization of civil sector security must be considered hybrid. However, hybrid design is not viewed as negative by Christensen and Lægreid, but rather a systemic feature of modern governments with the advantage of flexibility (2011, p. 420). It seems like the most significant advantages of organizing according to these contradictory principles is that it gives flexibility of coordination in both directions. That is, the

responsibility principle promotes vertical coordination down the sectors while the coordination principle promotes horizontal coordination across them. Thus, it seems the mixture of these two principles increases overall coordination capacity. Hybrid solutions to complex and transboundary problems like security seems needed to score high on instrumental thinking. The central instrumental challenge is rather about the balance between these contradictory organizing principles. Since the balance clearly favors the ministerial responsibility prior to the 2017 policy (its consequences are discussed below in the fourth section), the hybrid arrangement's positive effects on horizontal integration seems limited. This is in line with previous research and emphasis on "the eternal coordination problem" of civil sector security (Fimreite, Lango, Lægreid, & Rykkja, 2014, pp. 73-74).

On the operational level, NSM's coordination function clearly increases complexity since an additional structure is introduced, but the contradictory features are not as prominent. The more crisis management-oriented coordination structure is more centered around coordination of information within a network and not so much about hierarchical authority. This trait reduces tensions about responsibility and therefore degree of hybridity.

From the perspective of public administration regimes, the cross-sectoral coordination efforts are particularly interesting in relation to Joined-up government. Joined-up Government (JUG), Whole-of-Government (WG) or other types of post-NPM reforms, typically promote coordination initiatives aimed at wicked issues which falls between organizational boundaries, administrative level or policy sectors. These reforms strengthen the political-administrative center, and offers more integration and stronger coordination measures (Christensen & Lægreid, 2007). The introduction of coordination policies in the 1990s and early 2000s is characteristic of JUG-reforms in that they try to solve security issues across organizational boundaries and policy sectors and seek more integration. The establishment of NSM's VDI/CERT coordination function clearly follows JUG's emphasis on strengthening of the center, since only the decentralized system existed previously.

The complex double coordination system in ICT security policy at ministry level

The section above is centered around the existence of the two contradictory and competing organizing principles of ministerial responsibility and cross-sectoral coordination responsibility. Another major trend in ICT security policy has been the existence of two partly contradictory and competing ministry level organizations to enforce that cross-sectoral coordination. This double coordination system at ministry, which lasted from 1997 until 2013, are according to the empirical material a unique trait of ICT security policy since no other

subfield of public security has had similar organization set up.

With the 1997 creation of the lead ICT and ICT security ministry model was cross-sectoral ICT policy connected with security policy. It promotes more collaboration and coordination across organizational borders and sectors as expected when facing wicked problems. By connecting ICT policy with ICT security, the policy change followed the well-established responsibility principle, which seems coherent and in line with an instrumental logic. Thus, this organizational change in isolation seems to follow expectations of instrumental theory. However, with the coordination function at MoJ in mind the 1997 policy does strike a bit odd from the instrumental perspective because it seems to lack coherent organizational thinking. The empirical reality became highly complex on both the vertical and horizontal dimensions (Egeberg, 2012)

On the vertical dimension, it is striking that both MoI&T and MoR&A lacked structural connection to the security sector and the central auditing agencies NSM and DSB. It not only affected their possibility to vertically coordinate these agencies tasks and actions, it also limited information flows upwards from the agency level. With few central actors under traditional hierarchical authority, MoI&T/MoR&A were far from the hierarchical variant expectations about strong vertical lines of command and it weakened coordination authority in ICT security policy. (See Figure 3: Map of the two lead ICT security ministries and Figure 4: Map of key ICT security actors.)

On the horizontal dimension at ministry level, MoI&T/MoR&A was horizontally specialized to address ICT security, a subfield within security policy in the civil sector. While, MoJ was horizontally specialized to address civil sector security policy in broader sense. Most notably, the specialization included protection of critical functions and infrastructure (St. Meld., nr. 17 (2001-2002)). This was a clear case of overlap which brought uncertainties and build-in tensions about responsibility. By consequence, the double coordination system entailed hybridity (Christensen & Lægreid, 2011). Additionally, the responsibility of the lead ICT and ICT security ministry partly overlapped with MoT&C's sector responsibility, most notably in electronic communication policy which was governed by the underlying agency PTT/Nkom. Thus, the lead ICT and ICT security ministry was squeezed between MoJ's public security responsibility on one side and MoT&C's sector responsibility for electronic communication on the other. It seems that the hybrid design and lack of holistic organizational thinking on the horizontal dimension fostered substantial coordination pressure between these ministries.

In order to resolve these horizontal and vertical coordination problems, the supplementary organizational body CCIS was created. It indicates some instrumental thinking

since it was a secondary organizational solution to an apparent problem. However, it cannot be considered instrumental in the fullest sense because the underlying tensions and inconsistencies of the lapping duties were still present. CCIS were characteristic of vertical specialization with collegial elements which tends to reduce the degree of hierarchical commando authority and decision-making processes typically are based on arguing, bargaining or voting (Egeberg 2012: 4). Actually, due to MoI&T/MoR&A's lack of vertical connection through the traditional government structures, CCIS became an important source of authority to the lead ICT and ICT security ministries, although limited to secondary means. MoI&T/MoR&A lack of authority seems even weakened when also "the shadow of authority" is considered (Christensen, Lægreid, & Rykkja, 2016, p. 893). Formally MoI&T/MoR&A chaired CCIS (St. Meld., nr. 17 (2006-2007)). All the other three ministries, MoD, MoJ and MoI&C, had hierarchical command over highly relevant organizations to ICT, security or both. Since the lead ICT security ministry lacked important vertical roots it clearly seems like the weakest ministry in this network. The multitude of actors and weak hierarchical authority promoted decision-making processes on ICT security policy based on bargaining and compromises, in line with negotiation variants expectations. The complexity of this system is apparent in that decision-making processes followed supplementary structures and needed compromise and bargaining *before* they could be coordinated outwards across government sectors.

From an instrumental perspective it is very surprising that the empirical data does not find any horizontal coordination body that connected MoI&T/MoR&A to all ministries. Inability to push ICT security policy across ministry level has been evident (Riksrevisjonen, 2010: dokument nr. 1), which can be explained by the lack of organizational tools – together with the primacy of ministerial rule as discussed in the section above. It seems like the high number of involved actors, overlapping duties, and unclear responsibilities within the policy field of ICT security, pulled attention to coordination primarily inwards to resolve these uncertainties rather than outwards to all ministries and sectors.

Christensen and Lægreid argue that hybrid design that pull in different directions can have advantages of flexibility (2011, p. 420). In the section above, we have seen how the contradictory ministerial responsibility and cross-sectoral coordination responsibility can have advantages of increased coordination outcome. The advantages are not as evident in this case. The hybrid design of two partly overlapping coordination ministries in ICT security policy, seems rather to have promoted inaction and weaker cross-sectoral coordination ability.

The governing of ICT security policy during 1997-2013 points towards New Public Governance (NPG) (Osborne, 2010). By the early 2000s the state's organization of ICT security

must be considered plural because of the many actors involved is the delivery of ICT security. The policy-making processes were therefore spread out to several processes between government sectors and administrative levels. In the effort to bring together all these actors with CCIS the features of NPG really kick in. With CCIS an interorganizational network became these central allocation and coordination mechanism of ICT security policy, while few actors were under traditional hierarchical authority typical of OPA (ibid).

NSM's cross-sectoral nature

When we turn to the agency level of ICT security policy, the unique organization of National Security Authority (NSM) has been the major trend. The agency operates in the interface of the military and civil sector and across the public and private sectors.

From the instrumental perspective, decision-makers are purpose-oriented rational problem-solvers. They follow a logic of consequence and use organizations purposefully as tools to solve or reduce problems (Christensen, Lægreid, Roness, & Røvik, 2009, pp. 33-35). However, public security policy in general, including the subfield of ICT, constitute a major problem to handle because of its transboundary character, which is typical of wicked problems (Head, 2008; Head & Alford, 2015).

The implications of 1998 security law and its delegation of tasks and authority is a very interesting case of instrumental thinking to a wicked problem. In particular, the horizontal specialization principle is interesting. Gulick (1937) distinguishes between four types of horizontal specialization principles: purpose/sector, process, clientele and territory. The central government is predominantly organized according to the sector principle at both ministry and agency level. However, the security law delegated tasks to NSM across military sector, civil government and private sector companies. Therefore, the government did not follow the horizontal specialization principle of purpose/sector in a strict fashion. Rather, the importance of the process principle is striking, since the tasks primarily demanded technical skills and professional knowledge about security – including ICT security aspects. Outside the security law, NSM was delegated several security tasks specific to ICT which also followed process principle rather than purpose/sector principle of horizontal specialization (St. Meld, nr. 39 (2003-2004)). The presence of the clientele principle is also evident, since NSM was directed towards owners or operators of digital critical infrastructure and functions to society.

Since the policy field overall primarily was organized according to purpose/sector principle with clear separations between military and civil sector, NSM's portfolio produced a sectoral mixture and hybridity. The wide range of tasks and responsibilities pull in different

directions and provokes hybridity. With this organizational thinking, tensions and coordination pressure is resolved mostly within NSM. Thus, this multifunctional, complex and hybrid character fostered a holistic approach to ICT security. What typically makes wicked problems so inherently difficult is the inability to view them holistically. Problems go across policy sectors and organizational boundaries (Head, 2008; Rittel & Webber, 1973). From an instrumental perspective, the creation of a civil-military hybrid organization therefore seems like a very rational and instrumental way to reduce the transboundary problem of ICT security.

The mixture of military and civil tasks made NSM's organizational position within the military defense organization problematic since it did not reflect its the new transboundary character. The decision-making process and resulting horizontal separation and vertical specialization as a designated directorate, followed instrumental expectations as it offered an organizational solution to NSM's widened mandate. However, the question of NSM's ministry level connection showed weaker instrumentality, the hierarchical variant in particular. Institutional factors were clearly at play, but the process can also be understood by the negotiation variant. MoD and MoJ clearly had competing interest since both wanted authority and control over NSM. The negotiated result was that both ministries shared hierarchical authority over NSM – MoJ in civil matter and MoD in military matters (See Figure 2: Map of NSM and its parent ministry organization). The lack of a unified solution to NSM's parent ministry connection must be understood by the ministry level's horizontal specialization principle of sector/purpose and NSM's specialization according to process and clientele which went across sectoral lines (Gulick, 1937).

From the perspective of complexity and hybridity NSM is a very interesting case (Christensen & Lægreid, 2011). The delegation of tasks across military, civil government and private sectors, and shared parent ministry model, clearly shows that the direction of complexity increased considerably. This complex structural mixture in the interface of civil and military sectors inherently lead to hybridity. The hybrid organization of NSM seems like an evident case of advantages of flexibility (Christensen & Lægreid, 2011, p. 420). NSM is the only ICT security organization at agency level. Whether an incident on critical digital infrastructure is within the category of public security (civil) or state security (military) can be difficult to answer without knowledge about potential perpetrators and his/her motivation. With the hybrid design NSM becomes the relevant state actor regardless. Compared to crisis response to terrorist attacks and object security, central government capabilities are divided between key organizations in the military and justice sector which fuel interorganizational tensions and conflict about responsibility (Riksrevisjonen, 2018: dokument nr. 3:11). Thus, concentration of

capabilities into a civil-military hybrid actually seems to reduce complexity and tensions, and strongly in line with an instrumental approach to transboundary problems.

In the broader picture of public administration trends the organization of NSM is interesting. Old Public Administration (OPA) is characterized by an integrated state predominantly on the vertical dimension (Osborne, 2010) and is tightly linked to the ministerial rule system. On the other hand, Joined-up Government (JUG), Whole-of-Government (WG) or other post-NPM reforms typically promote coordination initiatives aimed at wicked issues which falls between organizational boundaries, administrative level or policy sectors. These reforms, mostly seen as a response to NPM's structural devolution, strengthened the political-administrative center, offered more integration and stronger coordination measures (Christensen & Lægreid, 2007). The organization of NSM seems to violate traits typical of OPA and NPM. From an OPA perspective it is a bit odd that sectoral boundaries are not followed, and that the directorate is not clearly governed by one ministry but two. How to view the organization of NSM from a NPM perspective can go in two completely different directions. On one side, the multitude of tasks and cross-sectoral nature is surprising because it creates a lot of purposes. It would be more in line with NPM at least to horizontally separate NSM as a military organization and a civil one, alternatively according to the different aspects of the security law. On the other hand, NSM can be viewed as a single-purpose organization in a broad sense, since NSM is organized according to security without consequences of sectoral boundaries. The NPM-understanding of NSM is diverges, but the former argument seems stronger. The complex portfolio and multifunctional character of NSM pulls in different directions and create several purposes.

By bringing together a range of tasks across military-civil and private-public sectors, the organization of NSM seems more in line with Joined-up government thinking. It integrates several aspects of ICT security, and security at large, and is a rare case of military and justice sector integration. New Public Governance (NPG) elements are also striking. The shared parent ministry system clearly shows plural traits of interdependent organizations (Osborne, 2010). However, the NPG elements are most visible in all the ICT security networks rooted in NSM. The already discussed VDI and CERT coordination networks (St. Meld, nr. 39 (2003-2004)) show this tendency early on. This tendency is increased by new networks connecting the surveillance and security organizations (common cyber coordination center), sectoral auditing bodies (coordination arena) and the complexly assembled National cyber security center (NOU, 2018: 14; Nasjonal sikkerhetsmyndighet, 2018).

Slow development in direction of stronger lead organizations

The nature of coordination power across ministry sectors has been a contested issue in the central government since the horizontal coordination structure was first introduced in the mid-1990s. Instrumental theory predicts that the structural organization of a policy field will shape behavior and performance (Egeberg, 2012). The ministry level organization of horizontally specialized ministries with sectoral responsibility according to ministerial rule create a plurality of important actors. Therefore, the hierarchical variants expectations of few decision-makers, homogenous processes and common interests (Christensen, Lægreid, Roness, & Røvik, 2009, pp. 34, 42-43) have been far from the empirical reality. Instead, prominence of the negotiation variants expectations of multiple actors, competing interests and compromises (ibid, pp. 34, 43-44) are much closer to reality. The competing interests, as established in the first section, is due to conflicting notions of authority between every ministry's sector responsibility and cross-sectoral coordination responsibility. Thus, measures of cross-sectoral coordination capacity have been a continuously bargained issue. The slow developments of ICT security policy therefore must be attributed to structural organization of the central government and ministerial rule system, although institutional factors are also at play.

The organization of coordination functions has primarily been based on the lead agency model (Boin, Busuioc, & Groenleer, 2014). Since the mid-1990s capabilities on public security policy, including ICT security, has centered on MoJ (Kgl.res., 16.09.1994; Kgl.res., 03.11.2000; St. Meld., nr. 17 (2001-2002)). The 1997 creation of a competing and designated lead ministry in ICT security policy (Kgl.res., 19.12.1997) was surprising from the instrumental perspective and its continuation until 2013 as well. Institutional factors seem highly relevant in explaining both the creation and the continuation. With the transition of ICT security to MoJ (Kgl.res., 22.03.2013) instrumental factors seem more at play as it was a clear response to criticism from 2005 and onwards (Riksrevisjonen, 2005: dokument nr. 3:4; NOU, 2006: 6; Riksrevisjonen, 2010: dokument nr. 1; Nasjonal sikkerhetsmyndighet, 2011). The 2013 policy is particularly interesting because it stands out from a general trend in this case about ICT security. The addition of new secondary measures to promote more collaboration and coordination has usually been the case. Furthermore, often these policies have increased complexity and hybridity. On the other hand, ICT security's transition to MoJ is structural integration through horizontal de-specialization. Arguably, it led to less complexity and tensions since MoJ no longer was opposed by another lead ministry and the connection between agency level and ministry level became clearer. This structural integration must be considered an important factor leading to strengthened lead ministry coordination of ICT security.

A considerable shift in direction of strengthening MoJ's lead agency role occur in 2017. The Official Norwegian Report on digital vulnerabilities defined weak coherence in different sector's security measures as highly problematic and argued for stronger coordination powers at MoJ (NOU, 2015: 13). In line with instrumental thinking MoJ was given authority to determine requirements in public security policy and national standards to ICT security measures over all civil ministries (Kgl.res., 10.03.2017). Since MoJ's cross-sectoral coordination previously was limited to counseling and recommendations, the hierarchical elements to MoJ's lead agency model was significantly increased. The introduction of instruction power also entails that relevance of the hierarchical variant of instrumental theory emerges. Previously, decisions about ICT security measures has been spread out to all ministries, but now the number of actors is reduced to one. The 2017 policy therefore create a commando-structure within the ministry level (see Figure 6: Map of MoJ's increased authority across ministry level). The flexibility of coordination in both directions, as touched upon towards the end of the first section, therefore seems increased. MoJ ensures horizontally integrated, national standards, and each ministry ensure implementation vertically down its sectors. The mixture of, or balance between, these two main principles of responsibility and coordination seem more evenly balanced with the 2017 policy. The "eternal coordination problem" of civil sector security policy (Fimreite, Lango, Lægreid, & Rykkja, 2014, pp. 73-74) does not seem so eternal after all.

In isolation this process and solution is significantly instrumental, but most reports on security in the civil sector prior to the 2015 report have argued similar problems and solutions (NOU, 2000: 24; NOU, 2006: 6). So, a central question is why now? Awareness about the transboundary nature of security threats and need for coordination has increased during these two decades with report after report. It can be argued that the increased emphasis on these problems have shifted compromise towards strengthened coordination power. Also, it might not be a coincidence that a report on ICT security provoked this reaction. ICTs are a considerable vulnerability all organizations and sectors face which demand high expertise to reduce (NOU, 2015: 13). However, the picture is not clear, and it is a difficult question with no unambiguous answers based on my data. An instrumental logic seems linked with cultural ones as well.

Central to the lead agency model is also network elements (Boin, Busuioc, & Groenleer, 2014). The tendency towards strengthened lead agency organizations also is visible on this dimension, with creation of designated ministry level network and a network directed towards private collaboration both chaired by MoJ (NOU, 2018: 14). Thus, MoJ does not only has

hierarchical power but also network tools to ensure horizontal coordination. At agency level, the increased use of networks centered at NSM also show tendency towards strengthened lead agency model. Similar to CERT, the new network solutions at NSM does not seem centered around hierarchical coordination but rather sharing of information, tools and standards in a more horizontal fashion.

From the perspective of public administration paradigms, MoJ's increased authority seems highly compatible with Joined-up government, as it strengthens the political-administrative center of ICT security and create a more integrated state. The management through networks also bring attention to NPG.

In conclusion, by the end of the empirical time frame, the shifts in balance between the two organizing principles of central government significantly promote a more hierarchical model of cross-sectoral coordination. By strengthening horizontal integration, a more holistic approach to ICT security seems possible.

5.3 Cultural-institutional theory

The central government organize according to two contradictory principles

A major trend of ICT security policy and public security policy at large, the organizing principles of the ministerial responsibility principle and cross-sectoral coordination responsibility at ministry level are in contradiction to each other. Weak implementation of the latter also characterizes the policy field. In the instrumental analysis, the coexistence has been understood as a structural hybrid with tensions about hierarchical authority. Furthermore, the weak implementation of the cross-sectoral coordination system was shaped by the negotiation variant because of conflict of interest and resulting compromise. When turning to the cultural-institutional approach, informal norms, values, roles and identities influence on government actors, decision-making processes and solutions are at center (Scott, 2014; Christensen, Lægreid, Roness, & Røvik, 2009; Olsen, 2007). Institutional path dependencies and gradual transformations also is explored (Mahoney, 2000; Pierson, 2000; Streek & Thelen, 2005).

The dominating organizational principle of the central government has been the ministerial rule system which dates back to the 1800s (Christensen, Egeberg, Larsen, Lægreid, & Roness, 2007). Responsibility for security at ministry level has followed the organizational system of ministerial rule. Therefore, this way of organizing the central government has been institutionalized and infused with value over a vast time span (Selznick, 1957). With this line of reasoning, when the 1992 Buvik report proposed a coordination function at MoJ (NOU, 2006: 6, p. 52), it was in opposition to the institutionalized norms about ministries' self-

governance over its of sector. Thus, the two organizing principles must be considered as cultural contradictions with build-in cultural tensions as well.

The logic of appropriateness is interesting when we turn to the implementation of these contradictory organizing principles. The logic of appropriateness holds that actors do what is thought of as acceptable, fitting and reasonable in relation to the given norms, values, identities and roles (Scott, 2014, pp. 64-66; Olsen, 2007, p. 3). This logic follows a matching process, where situations are coupled with identities which in turn leads to appropriate actions (Christensen, Lægreid, Roness, & Røvik, 2009, p. 54). In this case the situation central government actors faced was introduction of a competing principle about responsibility and authority in security policy. The situation can be characterized as an existential threat to the ministerial rule system. The identities of central actors primarily centers around norms and values of the ministerial rule and sectoral self-governance. Thus, the result of this coupling made the appropriate action to resist the coordination policy and ensure primacy of ministerial responsibility.

In path-dependency theory change is mostly understood as small adjustments within the path because decisions made in the formative years of an institutional arrangement are reproduced and create increasing returns (Mahoney, 2000; Pierson, 2000). Alternatively, changes are massive and linked to critical junctures which entails external shock to the system and divergence to a new path (Mahoney, 2000). Based on Streeck and Thelen's (2005) typology of change, these are either incremental processes leading to continuity or abrupt processes that lead to discontinuity. The institutional arrangement of the ministerial rule system and the accompanying responsibility principle is a system, or path, that has been reproduced over many decades and even centuries. When faced with the contradictory coordination principle since the 1990s and onwards, the ministerial responsibility has kept primacy. Therefore, it can be argued that the path is intact and that the coordination principle only is an adjustment without substantial effects.

A quite opposite argument can also be made. The fall of the Soviet Union and the end of the Cold War can arguably be viewed as an external shock to security policy which induced a critical juncture. Shortly after the new institutional arrangement of cross-sectoral coordination at MoJ was proposed by the 1992 Buvik report and later adopted by the government (Kgl.res., 16.09.1994; Kgl.res., 03.11.2000). In line with the theory (Mahoney, 2000, p. 513) the alternatives of MoD and Ministry of Industry as coordination ministries were also considered (NOU, 2006: 6, p. 52).

Even though the latter argument touches upon some important aspects it also has several

weaknesses. Firstly, the process of creating MoJ's coordination function cannot be considered abrupt. It was not until the early 2000s that the coordination arrangement contained any substantial cross-sectoral features, and it has been continuously under development. Secondly, the preexisting institutional arrangement of ministerial responsibility was not replaced. Therefore, the resulting change was not a massive divergence to a new path as shock-induced critical junctures expect. This leads to the former argument. Self-reproducing mechanisms and increasing return explain the prevalence of ministerial responsibility to a large degree. However, it is more uncertain if the establishment of MoJ's coordination function can only be considered incremental adaptation serving to continue the path. I will argue that the establishment of cross-sectoral coordination principle during the 1990s and early 2000s represents some kind of discontinuity since ministerial responsibility and vertical coordination no longer was the only basis of coordination. This leads to the relevance of the third type of institutional change.

Streeck and Thelen (2005) argues that incremental change with transformative results is not only possible, but frequent. As already touched upon, the process of implementing MoJ's cross-sectoral coordination function has been step-by-step. The initial proposal by the Buvik report (NOU, 2006: 6, p. 52), the first royal resolution about the coordination function (Kgl.res., 16.09.1994), the second royal resolution about cross-sectoral auditing and control (Kgl.res., 03.11.2000), increased agency level support, more defined role (St. Meld., nr. 17 (2001-2002)) and creation of the ministerial coordination council for public security (St. Meld., nr. 22 (2007-2008)) are all important steps in an incremental process. (Also, more recent policies could have been included, but they do not affect this line of reasoning, and will be analyzed in the fourth and final section.) Arguably, the result of all these changes has moved in direction of two coexisting institutional arrangements of security coordination. Thus, the policy changes led to incremental discontinuity of the pre-1990s organization of civil sector security.

Streeck and Thelen distinguish between five types of gradual transformative change, although layering seems most relevant to the empirical material. Layering is a type of change when a new system is put on top of an existing one, so that two or more systems coexists. Layering often occurs as amendments, additions or revisions to an existing institutional arrangement (Streek & Thelen, 2005, pp. 22-24). It is already established that the ministerial rule system and accompanying responsibility principle has been the main system of organization. Furthermore, the cross-sectoral coordination responsibility did not remove ministerial responsibility, but they rather coexisted with new coordination arrangements as a

secondary system. Therefore, it seems like the introduction of the cross-sectoral coordination principle must be view as a case of layering.

The complex double coordination system in ICT security policy at ministry level

Another major trend in ICT security policy has been the existence of two partly contradictory and competing ministry level organizations to enforce cross-sectoral coordination from 1997 until 2013. The double coordination system is a unique feature of ICT security within the larger realm of public security. The creation and further implementation of the lead ICT and ICT security ministry model scored low on instrumental factors, particularly in relation to instrumental logic, rational problem-solving and the hierarchical variant. This can indicate relevance of institutional factors.

When it comes to the creation of the lead ICT and ICT security ministry model both logic of appropriateness and path-dependency offer important insight. I will begin with the former. The situation from a logic of appropriateness-perspective (Olsen, 2007) : The existence of a lead ICT ministry without security responsibilities was already operative. During the 1990s attention to civil security increased, which also must have entailed attention to ICT security aspects. Political-administrative identities and normative foundation centered around ministerial rule and responsibility principle. As already touched upon, the 1994 policy about MoJ's cross-sectoral coordination responsibility was in opposition to the dominant way of organizing the central government and was weakly implemented by 1997. The coupling of situation and identities (Christensen, Lægreid, Roness, & Røvik, 2009, p. 54) seems to make combining ICT policy with security aspects the most fitting and reasonable action.

Path-dependency theory highlights the stability of institutions and institutional arrangements. Decisions in the formative years are reinforced by its institutional environment, increasing returns mechanisms occur and paths become locked-in (Mahoney, 2000; Pierson, 2000). However, institutions may vary in their ability to create rapid and decisive self-reinforcing mechanisms after its creation. If they do a path will be lock-in. If these self-reinforcing mechanisms are generated more gradually institutions may not be able to capitalize on its early advantage and can be overcome by alternative solutions (Mahoney, 2000, p. 515). In the section above it is established that MoJ's cross-sectoral coordination function did not come about abruptly, but rather in a gradual transformative fashion. Therefore, it seems like the development of MoJ's coordination function was characterized by weak and gradual reinforcing mechanisms. As predicted by the theory, this institutional arrangement was indeed overcome by an alternative solution.

On the other hand, MoI&T seemed more able to create relatively rapid and decisive self-reinforcing mechanisms and lock in. It survived the policy process behind the 2002 white paper, which clearly made MoJ's duties overlap those of MoI&T. Rather, MoI&T position as lead ICT security ministry was further reinforced shortly after with the creation of CCIS. Thus, both the creation and the further continuation of the complex double ministry level coordination system seem heavily based on cultural-institutional factors.

The institutional arrangement of the lead ICT and ICT security ministry model also draws attention to Streeck and Thelen's (2005) gradual transformative change. Even though the policy was introduced in 1997, supporting measures like designated department ministry MoI&T, inter-ministry policy group and CCIS took years to implement, which indicate an incremental process eventually leading to discontinuity. However, the coordination arrangement did not reduce the security responsibility of each ministry nor cross-sectoral coordination at MoJ, but rather served as a supplement or addition. As the existing institutional system was not changed, the creation of the lead ICT and ICT security ministry model seems like another case of layering. The institutional coordination system of ICT security therefore was based on three systems. Ministerial rule as the main system, cross-sectoral coordination from MoJ as the second, and cross-sectoral coordination from MoI&T/MoR&A as the third. Alternatively, the creation of the lead ICT and ICT security ministry model can be viewed as a case of conversion. Conversion occurs when institutions are redirected to new goals, functions or purposes which can origin from new environmental and external factors, as for example technological developments and vulnerabilities (Streek & Thelen, 2005, pp. 26-28). Since a cross-sectoral ICT coordination function was already at place, the addition of security aspects can be understood as redirection to security aspects due to vulnerability concerns. I find both arguments fairly applicable to the data.

NSM's cross-sectoral nature

The institutionalized norms and values about the organization of central government are heavily founded on the ministerial rule, sectoral self-governance and clear policy sector boundaries. In security policy the clear separation between MoD and military sector organizations and MoJ and civil security organizations have followed this institutionalized pattern. Therefore, from the perspective of cultural-institutional theory and logic of appropriateness (Scott, 2014; Olsen, 2007), the delegation of tasks to NSM across sectors seem surprising because it breaks with the established norms. When NSM received all these new tasks across sectoral boundaries its position within the military high command also became inappropriate. From a cultural-

institutional perspective the horizontal separation as a designated directorate can be understood as a way to find a more appropriate solution (Olsen, 2007).

With NSM's hybrid design in between institutionalized sectors, its ministry level connection became a matter of conflict. From the institutional perspective it must be understood as an institutional battle between policy sectors and competing appropriateness. NSM's long history of being a military organization, institutionalized relation to MoD and NSM's task still was partly related to state security. While MoJ find NSM's widened mandate to stretch far into the civil sector, making a military leadership inappropriate. Furthermore, MoJ was at the time in a process of strengthening its position as civil sector lead ministry in security policy (Lægreid & Serigstad, 2006). With these competing cultural views, it seems like the match between situation and identities (Christensen, Lægreid, Roness, & Røvik, 2009) offered only one appropriate solution, namely to combine MoJ and MoD parent ministry function.

The hybrid structural design of NSM also seem to promote cultural complexity (Christensen & Lægreid, 2011). NSM's original position within the military defense organization means that it has a history of military culture. This makes NSM culturally compatible with MoD as parent ministry. MoJ, on the other hand, comes from a civil culture dominated by lawyers, law-enforcement and police professions. This seem to complicate NSM's vertical steering in civil matters. Also, in relation to NSM's widened civil mandate cultural factors seems to be at play. NSM through VDI/CERT showed limited ability to cooperate with civil sector organization in the first half of the 2000s (Riksrevisjonen, 2005: dokument nr. 3:4, p. 9). Culture and norms are not a static since the process of institutionalization is something that happens over time (Selznick, 1957; Christensen, Lægreid, Roness, & Røvik, 2009, p. 59). NSM's increased collaboration with civil actors both vertically (MoJ) and more horizontally across government sector and with major private companies (NOU, 2018: 14; Nasjonal sikkerhetsmyndighet, 2018), it arguably seems like NSM increasingly is developing a civil-military hybrid culture.

Based on Streeck and Thelen's (2005) typology of institutional change, NSM's widened cross-sectoral mandate, new organizational design and ministry steering clearly points in direction of discontinuity. How to conceptualize the process of change is more uncertain. If it is to be viewed as an abrupt process points towards path-dependency's critical juncture. Critical junctures are usually seen as a result of an external shock leading to divergence to a new path (Mahoney, 2000). Also, they are viewed as critical because after the new institutional arrangement is adopted it is increasingly difficult to go back, i.e. increasing return mechanisms occur (Mahoney, 2000, p. 513; Pierson, 2000). Although the decision-making process took

several years, the result clearly changed the institutional system of ICT security at agency level since there had not been any organizations with a wide range of civil-military tasks before. This seems like a major institutional change implemented quite abruptly. And, it certainly seems critical since the arrangement has been very stable and locked in after the creation with observable increasing returns mechanisms at play. However, the absence of an external shock reduces theoretical strength.

If it is to be viewed as an incremental process leading to gradual transformative change, emphasis must be put on the preexistence of NSM and MoD's continued parent ministry function. The 1998 security law only placed new tasks on the institution which led to some institutional changes. From this perspective conversion, i.e. redirection to new goals, functions and purposes (Streek & Thelen, 2005, pp. 26-28), seems highly relevant. Furthermore, the key ICT security projects VDI and CERT was not operative and connected to all relevant organizations immediately, but rather established collaborations gradually. Thus, insights from both critical juncture and gradual transformation hold important explanatory force. In conclusion, to synthesize these insights, it does not seem to be a complete divergence to a new path, but rather a conversion of the institutional system of transformative character with critical implications.

Slow development in direction of stronger lead organizations

In the development of horizontal coordination policies at ministry level cultural factors have been important. Path-dependency emphasize decisions made in formative years create lasting institutional paths (Mahoney, 2000). I argued in the first section that the cross-sectoral coordination function at MoJ met a lot of cultural-institutional resistance during the 1990s and early 2000s. The resistance was based on the institutionalized ministry rule system and accompanying responsibility principle, which limited horizontal coordination authority to recommendations and counseling. It seems like these decisions made in the formative years locked in an institutional balance between ministerial responsibility and cross-sectoral coordination with primacy of the former. New measures during the 2000s seem like adaptations within the institutional path. The institutional balance even "survived" the external shock of July 22nd 2011 and immediate policy responses, which show the strength of cultural-institutional factors. The effects of the central government's history of organizing according to ministerial rule must therefore include cultural factors to the structural ones in explaining the slow developments of horizontal coordination policies at ministry level. However, some events during the 2010s have important implications to the lead organizations.

Another source of weak horizontal coordination of ICT security policy has centered on the complex system of two horizontal coordination organizations. In the analysis of its creation, two sections above, I argued that it entailed a discontinuity of the institutional coordination arrangement. Therefore, by logical consequence, the 2013 transition of ICT security from MoR&A to MoJ (Kgl.res., 22.03.2013) also must entail some sort of discontinuity. The central question must be directed to whether the process should be considered incremental or abrupt. Path-dependency place importance on increasing returns and self-reproducing mechanisms of institutional arrangements, and that weak self-reproduction can lead arrangements being overcome by others (Mahoney, 2000; Pierson, 2000). Furthermore, substantial changes usually occur as critical junctures because of external shock and divergence to new paths (ibid). Both the result and process of coordinated ICT security policy was a matter of criticisms since 2005 and onwards with increasing strength (Riksrevisjonen, 2005: dokument nr. 3:4; NOU, 2006: 6; Riksrevisjonen, 2010: dokument nr. 1; Nasjonal sikkerhetsmyndighet, 2011). It therefore seems like the institutional arrangement of the lead ICT and ICT security ministry faced weak self-reinforcing mechanisms, and the transition of ICT security to MoJ was a result of that. Based on critical juncture emphasis must be put on the external shock of July 22nd and the inclusion of ICT security in the Bleikelia report (Fimreite, Lango, Lægreid, & Rykkja, 2014, p. 70).

For the ICT and ICT security ministry model this change was abrupt, which indicate a high relevance of critical juncture and divergence to a new path. However, from a broader perspective this does not seem as clear for several reasons. Firstly, as already described was the main driver behind the change a long process of negative feedback, rather than a sudden external shock to the ICT security policy field. Secondly, MoJ was beforehand lead ministry for public security policy, which included an overarching responsibility for ICT security as for example the 2002 white paper showed (St. Meld., nr. 17 (2001-2002)). MoJ was also parent ministry to the ICT security agency NSM in civil matter, and deputy leader in CCIS. And thirdly, MoR&A kept several its ICT responsibilities and pushed digitalization policy across public sector, just not with overarching security responsibility. Therefore, the change shows clear incremental tendencies and point towards gradual transformation. Previously argued, the creation of the ICT and ICT security model was the third system layered on ministry level coordination of ICT security. The transition to MoJ therefore seems like a case of *de-layering*. That is, instead of a new system being added to the existing one, this is rather an institutional subtraction. However, Streeck and Thelen (2005) do not use the term in subtracting fashion, I am therefore uncertain how appropriate this conception really is. Alternatively, the transition can be viewed as a conversion of policy responsibility from MoR&A to MoJ. In conclusion,

the transition of ICT security to MoJ should be understood as an incremental process with the discontinuing result of making MoJ as the only institutional arrangement concerning cross-sectoral ICT security policy.

The 2017 increased cross-sectoral coordination authority to MoJ is highly interesting from an institutional perspective (Kgl.res., 10.03.2017). The cultural resistance against this kind of authority and the locked institutional balance ensuring primacy of ministerial responsibility has been one of the defining themes up until this point. Therefore, it seems like the increased authority would not have been possible without changes in informal norms and attitudes about what constitute appropriate cross-sectoral coordination authority. Norms, values and culture are not static things. The process of institutionalization and development of cultural features are predominantly understood as evolutional, natural processes, due to gradual adaptation to internal and close external environment (Selznick, 1957; Christensen, Lægreid, Roness, & Røvik, 2009, p. 59). Since the 1990s, attention to civil security and society's vulnerabilities have increased tremendously with reports, white papers, research and so on. A central theme has been coordination and the need to strengthen it. All these inputs make an evolution of attitudes not strange at all, rather it seems natural.

I find July 22nd and the following Inquiry report particularity relevant. The Inquiry report brought attention to leadership, culture and attitudes, and argued main problems were inability to recognize risk, coordination/collaboration, and willingness to clarify responsibilities (NOU, 2012: 14). The shock of July 22nd clearly brought attention to risk with many small policy changes and to coordination through the formal introduction of the collaboration principle (St. Meld., nr. 29 (2011-2012)). However, the contradiction between responsibility principle and cross-sectoral coordination was ambiguous about responsibility. It seems like the middle-to-long-term effects of July 22nd and the Inquiry report's attention to cultural factors have led to changed willingness to clarify responsibility between these contradictory principles – making it more appropriate to centralize responsibility on MoJ.

The 2017 policy was not a fundamental change to the overall system, since the responsibility principle also was emphasized. Even though the increased authority limits to overarching requirements and standards, the policy arguably represents a discontinuity since it gave MoJ a hierarchical authority it had previously lacked. The incremental nature of MoJ's strengthened position as lead ministry is highly evident since it is a process that can be traced back to 1994. Therefore, Streeck and Thelen's (2005) gradual transformation seems like an appropriate way of understanding MoJ's gradual development.

In relation to the development of NSM as increasingly the cornerstone ICT security

agency, the relevance of Streeck and Thelen's (2005) gradual transformation seems more uncertain. The increasing use of networks centered on NSM – to promote more coordination across the surveillance and security services, auditing organizations and a multitude of actors in national cyber-security center – does not change the overall institutional arrangement of responsibility. Rather these changes seem to take advantage of the institutional re-design of NSM in the early 2000s through additional secondary structures. Path-dependency theory argues that within an institutional framework, actors (both individuals or organizations) are encouraged to specialize, deepen relationships to other actors and develop particular identities. These actions increase the attractiveness of the existing institutional system relative to other hypothetical ones (Pierson, 2000, p. 259). The creations of new networks centered around NSM seems like clear cases of other actors deepening relationships to NSM, creating self-reproducing and increasing returns mechanisms to the institutional framework. The development of NSM as lead agency therefore seems like path-dependent adaptations after the critical transformation in the early 2000s.

5.4 Neo-institutional theory

The central government organize according to two contradictory principles

The neo-institutional perspective draws attention to institutionalized environment organizations operate within, and the symbolic adaption to this environment and its expectations organizations need to demonstrate (Scott, 2014; Meyer & Rowan, 1977). From this perspective the initial establishment of the contradictory coordination function at MoJ can be viewed a symbolic response to demands from the external environment, with the Buvik report as the initial source of legitimation problems to the security sector. Thus, this was the first time "coordination" of civil sector security got status as an institutionalized myth in the empirical timeframe. However, the legitimacy problems were not massive to the security sector, and the broader organizational thinking about governments were influenced by the myths of NPM in the early and mid-1990s. The external cultural norms (myths) of "strong horizontal coordination" therefore must be considered weak, which can explain the ambiguous policy and weak implementation.

MoJ's lead ministry function was clearly strengthened in the early 2000s (St. Meld., nr. 17 (2001-2002)). Interestingly, when we look at the institutional environment around the turn of the millennia, Joined-up government and other post-NPM reforms emerged internationally (Christensen & Lægreid, 2007), and the vulnerability report set the stage nationally and within the security sector (NOU, 2000: 24). The institutionalized environment on several levels

therefore shifted around the same time, all with demands of more horizontal coordination. Also, to the security sector, the end of the Cold War clearly brought increased attention to civil security policies. Arguably, the government's emphasis on MoJ's coordination role show tendencies of symbolic action in search of legitimacy. Tendencies of over-selling the coordination role is also evident since MoJ horizontal role was limited to counseling and recommendations. The organization according to two contradictory principles, with relative low implementation of the new coordination principle, points towards double-talk (Brunsson, 2006).

The coordination function CERT at NSM, on a more operational level, is highly interesting from a neo-institutional point of view. DiMaggio and Powell argue that organizations tend to resemble other organization which face a same set of environmental conditions (DiMaggio & Powell, 1983, p. 149). CERT-units already existed as an ICT crisis response unit in several key allied countries (St. Meld, nr. 39 (2003-2004)). CERT clearly has features of an organizational prescription to ICT security on operational level. The creation of a Norwegian CERT therefore points towards isomorphism (DiMaggio & Powell, 1983). Most evidently, CERT seem like an organizational mimic in response to the uncertainties new digital technology presented. The call for improved digital crisis response came from the professional community itself, which points toward elements of normative isomorphism as well.

The complex double coordination system in ICT security policy at ministry level

The 1997 creation of (Kgl.res., 19.12.1997), which led to the complex double coordination system at ministry level, shows some symbolic elements. The policy seems like effort in search of legitimacy directed towards the Norwegian population. It symbolizes that the government take security threats of ICT with great seriousness and take appropriate coordination measures accordingly. The later creation of CCIS also mimics inter-ministerial networks popularized by JUG (Christensen & Lægreid, 2007). The unrealistic organizational thinking indicates overselling and symbolic nature of the lead ICT and ICT security ministry model.

However, the document analysis has not found similar solutions to ICT security in other countries, which indicate that the system is not an organizational prescription and evident case of isomorphism.

NSM's cross-sectoral nature

The reframing of security policy after the Cold War towards increased focus on civil aspects seems like a key contextual factor from a neo-institutional perspective. Thus, by late 1990s the external cultural norms (Scott, 2014) about security valued both military and civil aspects. The

1998 security law's delegation of tasks to NSM across military and civil sectors therefore indicate a response to that shift (Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), 1998). However, with the re-design of NSM and its dual parent ministry model the picture is not as clear. On one side, the new line of command in civil matters from MoJ to NSM serve as a strong symbol and strengthen the myth of MoJ in charge of civil sector security (St. Meld., nr. 17 (2001-2002), p. 8). On the other hand, the hybrid design and dual parent ministry system is uncommon both in Norwegian central government and in the organization of security internationally. It therefore does not indicate a homogenization process and score very low on isomorphism (DiMaggio & Powell, 1983).

Slow development in direction of stronger lead organizations

Neo-institutional theory stresses the importance of the institutional environment organizations operate within, and the need demonstrate that they are acting on what is collectively valued (Scott, 2014; Christensen, Lægreid, Roness, & Røvik, 2009). During the 1990s and early 2000s, the government started to get legitimacy problems as the external environment demanded more coordination. To demonstrate that they are acting on what is collectively valued, the symbol of MoJ as a coordinative lead ministry of security in the civil security seems to be promoted more and more. With the shock and tragedy of the July 22nd terror, and the Inquiry commission's emphasis on weak coordination and unwillingness to clarify responsibility, among other things (NOU, 2012: 14), the central government were under immense external pressure. The change of name from Ministry of Justice and Police to Ministry of Justice and Public Security (Kgl.res., 11.11.2011) was a highly symbolic measure to signalize MoJ's responsibility for civil sector security. The change to make MoJ permanent lead ministry in crisis situations and (more relevant to this analysis) the transition of ICT security policy to MoJ also strengthen the myth of MoJ in charge of civil sector security. The implementation of the collaboration principle (St. Meld., nr. 29 (2011-2012)), which did not change any responsibilities, also seem to be a symbolic response to the external environment.

From this perspective, it seems a bit surprising that the strengthened coordination authority of MoJ (Kgl.res., 10.03.2017) was not part of the immediate post-July 22nd policies, as it furthers the myth of MoJ as lead ministry for civil security. Maybe, the Inquiry commission's emphasis on cultural aspects rather than structural did not provide enough external pressure to cause such a measure at the time. However, the commission's emphasis on the need to clarify responsibilities points in the other direction (NOU, 2012: 14).

Some of the network solutions in recent years clearly points towards neo-institutional

factors. The network for national information security, which gathers all ministries and are chaired by MoJ, seems like a complete copy of the ministerial coordination council for public security created in late 2000s (St. Meld., nr. 22 (2007-2008); NOU, 2018: 14). While, the national cyber-security center at NSM, which gathers a broad spectrum of actors within government, private companies and civil society, seems highly influenced by the similar centers established in Denmark, Netherlands and Great Britain. Neo-institutionalists argue that organizations become more homogenic due to constraining process that forces a unit to resemble other units which face a same set of environmental conditions. Mimic isomorphism is typical when organizations face uncertainties, from for example new technologies like ICTs. Then organizations look at successful or legitimate organizations and imitate their solutions (DiMaggio & Powell, 1983). Both of these networks seem like evident cases of mimic isomorphism. It is in line with the theoretical expectation that the central government is receptive to organizational solutions in allied countries like Denmark, Netherlands and Great Britain, and give them status as successful and legitimate. It is interesting to observe that the ministerial coordination council for public security, an organizational arrangement within the central government, has status as legitimate and is mimicked in this way.

6. Summary, conclusions and implications

6.1 Overview of the study

This study is an analysis of the major organizational features, solutions and trends in the central governments ICT security policy since the 1990s until 2018. The study is based on the research questions:

- *What are the major organizational trends in the central government's ICT security policy since the 1990s until 2018?*
- *How can instrumental, cultural-institutional and neo-institutional theory explain these trends?*

The methodical approach is a theoretical interpretative case study (Andersen, 2013), where the instrumental and institutional theories have guided the presentation of the empirical material and the analysis. The choice of public management and administration theories is based on their ability to analyze organizational solutions, features and administrative policies. The structural-instrumental dimensions of vertical and horizontal specialization and coordination have been central to the analysis (Gulick, 1937; Egeberg, 2012). The instrumental logic of consequence, purpose-oriented rationality, view of organizations as tools, and variants of hierarchy and negotiation have also been central explanatory factors (Christensen, Lægreid, Roness, & Røvik, 2009). The institutional theory has supplemented the theoretical understanding and explanations. Normative and cultural aspects (Scott, 2014), the logic of appropriateness (Olsen, 2007), path-dependency (Mahoney, 2000; Pierson, 2000), gradual transformative change (Streek & Thelen, 2005) and neo-institutional factors (DiMaggio & Powell, 1983; Meyer & Rowan, 1977) have been central institutional explanatory factors.

The methodical approach has been qualitative content analysis of relevant public documents, which entails searching for underlying themes in the material being analyzed (Bryman, 2012, p. 557). A wide range of documents has been collected and analyzed. The primary sources have been Auditor General reports, Official Norwegian reports, white papers, royal resolutions, information security strategies and laws. I will now turn to summarizing the major findings from this analysis, and its implications.

6.2 Summary of empirical material

The empirical data has shown that the 1994 establishment of a cross-sectoral coordination function at MoJ represents the initial break from the original decentralized and fragmented system of public security (Kgl.res., 16.09.1994). However, the cross-sectoral responsibly was

only layered on top of the existing system, thus created a complex and inconsistent arrangement with build-in uncertainty and tensions. The uncertainty and tension were in particular about the balance between the sectoral responsibility of each ministry on one side, and the level of cross-sectoral authority at MoJ on the other. MoJ gradually strengthened its position as lead ministry of public security with 2000 royal resolution (Kgl.res., 03.11.2000), improved agency level support from DSB and NSM, and a more clearly defined lead ministry responsibility in 2002 white paper (St. Meld., nr. 17 (2001-2002)). However, the cross-sectoral coordination authority was limited to counseling and recommendations, and was therefore relatively weak.

The 2002 white paper for the first time defined the concept 'public security', where critical functions and infrastructure were included in the definition. Since many critical functions and infrastructure were (and increasingly are) digital, MoJ's lead ministry function became intertwined with ICT security. However, another cross-sectoral coordination function was established at ministry level between MoJ's initial coordination function in 1994 and its broadened mandate in the early 2000s. The 1997 establishment of the lead ICT and ICT security ministry model connected cross-sectoral ICT policy with its security aspects (Kgl.res., 19.12.1997). MoI&T was the initial ministry to hold that role, until MoR&A took over in mid-2000s (Kgl.res., 01.10.2004). The model lasted until 2013 (Kgl.res., 22.03.2013). In that period, the government operated with a complex and inconsistent double cross-sectoral coordination system at ministry level in ICT security matters. The central feature of both MoI&T and MoR&A was their lack of structural connection to the security sector and its auditing agencies. The complexity at ministry level was reduced when the ICT and ICT security model was abolished, and ICT security policy was transferred to MoJ's public security portfolio in 2013.

At the agency level, National Security Authority (NSM) became the key organization. The 1998 security law delegated a wide range of security task to NSM, which went across the military and civil sectors, and across public and private sectors (Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), 1998). Many of these tasks were ICT security related. Additionally, NSM was delegated ICT security tasks outside of the security law, like administrating Norway's Computer Emergency Response Team (CERT) (St. Meld, nr. 39 (2003-2004)). This was a secondary coordination structure on top of the existing decentralized responsibility system. NSM's civil-military nature resulted in a unique dual parent ministry model, shared between MoD and MoJ. Although NSM is characterized by highly complex and hybrid design, its advantages are also prominent. With a design in the interface of the military and civil sector, they are the only key ICT security organization in the central government at agency level. It allows for a flexible approach to ICT security threats without concerns of the

traditional boundaries between public security (civil sector) or state security (military sector).

During the last few years of the empirical time-frame have the field of ICT security seen an increasing use of network-oriented coordination measures centered around MoJ at ministry level and NSM at agency level (St. Meld., nr. 10 (2016-2017); NOU, 2018: 14). Some of these arrangements are directed towards coordination across government, while others are gathering actors from private sector and civil society. Another significant development in recent years is that MoJ has received increased coordination authority. The 2017 policy gave MoJ authority to determine requirements and national ICT standards (Kgl.res., 10.03.2017). This marks a substantial shift in the balance between the ministerial responsibility and the cross-sectoral authority of MoJ. Based on the empirical material, I find the following major trends of ICT security policy:

1. The central government has been organized according to two contradictory principles since mid-1990s.

2. Coordination of ICT security policy at ministry level was enforced by two actors from 1997 until 2013.

3. The key ICT security agency (NSM) uniquely operates in the interface of the military and civil sector.

4. ICT security policy is characterized by slow developments, but the policy field has gradually developed in direction of stronger lead organizations (MoJ and NSM) and increased use of network-solutions.

6.3 Conclusions

1. The central government has been organized according to two contradictory principles since mid-1990s.

The introduction of the horizontal coordination function at MoJ in the mid-1990s (Kgl.res., 16.09.1994) seem to arise from a fundamental expectation of instrumental theory. Which principle of horizontal specialization a set of organizations are organized according to, will affect coordination pressure (Gulick 1937, Egeberg 2012). The ministry level of the central government has been based on the ministerial rule system and responsibility principle for many decades, which have led to fragmented system of strong sector-oriented horizontal specialization and primarily vertical coordination. The introduction of the horizontal coordination function seems to follow instrumental thinking as it is an organizational solution to promote a more holistic approach to security policy. However, the two principles of

organizing bring constant tensions about authority which highlights the hybridity of the arrangement. The advantages of the hybrid system (Christensen & Lægreid, 2011, p. 20) centers on the promotion of coordination in both the vertical and horizontal direction.

The negotiation variant of instrumental theory and cultural-institutional theory show strong explanatory force in the processes behind and outcome of relative weak implementation of coordination functions during the 1990s and early 2000s. Both explanations center on the preexisting ministerial rule system. From a structural-instrumental and negotiation perspective (Christensen, Lægreid, Roness, & Røvik, 2009, pp. 34, 43-44), this has created a plurality of actors involved in security policy at ministry level. To centralize coordination would therefore in conflict with the interests of the other ministries. The compromise was to organize according to both principles, however with primacy of ministerial responsibility. The cultural-institutional theory, on the other hand, brings attention to normative aspects (Scott, 2014; Selznick, 1957). The ministerial rule system has been highly institutionalized and infused with value over many the decades. The introduction of a coordination function at MoJ was therefore in opposition to the culturally appropriate system of ministerial self-governance. Thus, the resistance from the other ministries must also be considered a cultural one.

Neo-institutional factors seem also at play in the creation of horizontal coordination polices. After the end of the Cold War, the civil security sector received increasing external pressure to be better coordinated. In UK and elsew here, Joined-up government and other coordination reforms were becoming increasingly popular ways of thinking about central government around the turn of the millennia (Christensen & Lægreid, 2007). The response by Norwegian government to promote more coordination seem like symbolic responses to demonstrate they are acting on what is collectively valued (Scott, 2014; Meyer & Rowan, 1977). The weak implementation of horizontal coordination measures, until 2017, indicate over-selling and double-talk (Brunsson, 2006).

On an operational level, the combination of the decentralized system of the responsibility principle and a centralized coordination mechanism also coexisted, after the prescription CERT was introduced in an isomorphic fashion in early 2000s (DiMaggio & Powell, 1983). However, compared to two principles at ministry level, this coexistence did not foster tensions in the same manner because the coordination function centered primarily on flow of information in the network rather than hierarchic control.

2. Coordination of ICT security policy at ministry level was enforced by two actors from 1997 until 2013.

The creation of the ICT and ICT security ministry model (Kgl.res., 19.12.1997) does in isolation show instrumentality as it promotes horizontal coordination of a transboundary problem. However, in relation to the already established coordination function at MoJ, the 1997 policy show weak holistic and instrumental thinking. The main explanation centers around path-dependency theory (Mahoney, 2000) and MoJ's inability to rapidly self-reproduce its coordination function during the 1990s, which created room for a competing institutional arrangement to be established. The 1997 policy also seem to follow a logic of appropriateness (Olsen, 2007) as it connected cross-sectoral ICT policy with the institutionalized principle of responsibility.

With two actors at ministry level with coordination responsibility the myth of "coordination" was prominent. However, in reality, the double coordination system was highly complex and difficult to manage. With the structural dimensions of vertical and horizontal specialization and coordination (Egeberg, 2012) it is visible that both MoI&T and MoR&A lacked important structural connections to the security sector. Also, there was a lot of overlap of and uncertainty about responsibility between the two coordination ministries, and in relation to the sector responsibility of Ministry of Transportation and Communication (MoT&C) and PTT/Nkom. It led to massive coordination pressure and negotiation was needed within the policy field before policies could be horizontally coordinated across ministry level, which already was a difficult task due to the primacy of ministerial responsibility.

3. The key ICT security agency (NSM) uniquely operates in the interface of the military and civil sector.

In explaining the multifunctional, complex and hybrid organization of NSM instrumental factors show strong explanatory force. The delegation of tasks primarily followed the specialization principle of process, and partly clientele, rather than purpose/sector (Gulick, 1937; Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), 1998; St. Meld, nr. 39 (2003-2004)). This prompted a transboundary approach to ICT security issues across military, civil government and private sectors. What make wicked problems so inherently difficult to manage is the inability to view them holistically since they go across policy sectors and organizational boundaries (Head, 2008; Head & Alford, 2015). Therefore, concentration of capabilities into one multifunctional, civil-military hybrid seems to be strongly in line with an instrumental approach to transboundary problems like ICT security.

The process of deciding the ministry level connection to NSM, on the other hand, was characterized by negotiation variant due to competing interests and cultural-institutional factors

due to competing view of appropriate solutions. It ended with a compromise and mixed solution with both MoD and MoJ as parent ministries. Due to the uniqueness of this parent ministry model, neo-institutional factors seem less relevant. However, the solution did strengthen the myth of MoJ in charge of civil sector. The re-design of NSM it does not seem to be a complete divergence to a new path, but rather a conversion of the institutional system of transformative character with critical implications (Streek & Thelen, 2005; Mahoney, 2000).

***4. ICT security policy is characterized by slow developments, but the policy field has gradually developed in direction of stronger lead organizations (MoJ and NSM) and increased use of network-solutions*.**

The slow developments in the field of ICT security, and public security at large, in particular at the ministerial level, must be attributed to the ministerial rule system and responsibility principle as the main principle of organizing. From the structural perspective this system created a plurality of actors in conflict with a centralized coordination ministry, which fostered negotiation and ambiguous horizontal coordination measures. From a cultural-institutional perspective, strong horizontal coordination policies are in opposition to the highly institutionalized ministerial rule system and responsibility which foster cultural resistance. Also, the emphasis on formative years in path-dependency (Mahoney, 2000) seems highly relevant in explaining the slow developments. In the formative years in 1990s and early 2000s, the secondary nature of horizontal coordination was established. It seems like this institutional pattern to a large degree has been re-produced and difficult to break with – it even survived the immediate aftermath of July 22nd 2011.

The important change in direction of strengthening MoJ as lead ministry, the 2013 transition of ICT security from MoR&A (Kgl.res., 22.03.2013), seem in line with instrumental thinking. It offered an organizational solution (structural de-specialization) to the massive coordination problems between key ICT security actors, and reduced complexity and tensions. It can also be understood by the lead ICT and ICT security ministry model's inability to self-reproduce and maintain itself (Mahoney, 2000). However, the key development in strengthening MoJ as lead ministry was the instruction authority of 2017 (Kgl.res., 10.03.2017). In isolation it followed an instrumental logic as it offered a much-needed authority to ensure more coherent policy across sectors. However, there had been many calls for strengthened coordination authority before. It seems like the policy change would not have been possible without changes in informal norms and attitudes about what constitute appropriate cross-sectoral coordination authority. What factor or factors have caused this change is uncertain.

One explanation center on the effects of July 22nd, its resulting focus on security measures, and the emphasis of the Inquiry commission on cultural factors and unwillingness to clarify responsibilities (NOU, 2012: 14). Another explanation center on the multitude of feedback from reports and research over the years which continuously emphasize the need for more coordination. Thirdly, it seems nontrivial that a Norwegian Official Report on ICT security provoked this reaction (NOU, 2015: 13). ICTs are a considerable vulnerability and threat to service-delivery in all sectors where robust measures demand on high expertise and standardization. However, the picture is not clear. A cultural logic seems linked with an instrumental as well.

The result of the 2017 policy marks a substantial shift in the balance between ministerial responsibility and horizontal coordination at MoJ, as an evident commando-structure within the ministry level is put in place. The horizontal coordination system therefore went from a network-model in direction of a hierarchical model. The centralization of decision-making in overarching matters seems to significantly promote a more integrated and holistic approach to ICT security. The development of the coordination function at MoJ clearly follows a gradual transformation (Streek & Thelen, 2005) with policies in direction of a lead agency model (Boin, Busuioc, & Groenleer, 2014) being added continuously since 1994. The further development of NSM as a lead agency rather seems like smaller additions and adaptions within the institutional framework put in place in the early 2000s (Pierson, 2000).

From the perspective of public administration paradigms, it is evident that Old Public Administration (OPA) is still highly relevant. The primary organizational principle in ICT and public security is based on sectoral responsibility. However, it is also evident that the policy field is going in direction of Joined-up government (JUG) and New Public Governance (NPG) (Christensen & Lægreid, 2007; Osborne, 2010). Strengthened coordination authority and emphasis on viewing ICT security across sectors are typically elements of JUG. While, NPG-elements are visible in the widely use of network arrangements as a mode of governing, and in the increased emphasis on public-private cooperation.

6.4 Implications

Based on the analysis it seems like the problem of ICT security is too complex to manage without turning to complex and hybrid organizational solutions that are filled with tensions. That is, no universal organizational solutions are applied by the Norwegian government, and neither does it seem possible. Two key issues are prominent. One centers on the sectoral divide between military and civil security. While security policy is divided into sectoral line, actual

modern-day security threats often are more hybrid. The case of ICT security shows a rare solution to this issue with the transboundary organizing of NSM at agency level. With concentration of ICT security capabilities into one civil-military organization a holistic approach seems clearly enhanced, compared to a situation with two ICT security organizations on each side of the divide. However, on ministry level the issue of the sectoral divide is still prominent.

The other key issue centers around the contradiction between ministerial responsibility for security in its sector versus a lead ministry with overarching responsibility – and the constant tension about authority between these principles of organizing. Without some instruction power at the lead ministry, positive coordination and integrated policies have proved difficult due to the plurality of actors and heterogenic decision-making processes. Therefore, the 2017 policy marks an important shift in balance between these principles and indicate a more hierarchical coordination model. It seems like the hybrid arrangement can operate more harmoniously after 2017, where MoJ has some vertically specialized authority to coordinate horizontally across ministry level and each ministry coordinate these requirements and standards vertically down its sectors.

In chapter 3 methods, I argued that this case belongs to the larger universe of public security most clearly, but also to how governments handle wicked problems and of organizational trends in the central government overall. External validity in qualitative research centers on the generality of the study (Johannessen, Tufte, & Christoffersen, 2016, p. 233). Thus, what generated knowledge from this case is transferable to these other phenomena?

Fimreite, Lango, Lægreid & Rykkja (2014, pp. 73-74) highlighted the problems of fragmentation, pulverization of responsibility and weak coordination mechanisms in public security. These problems illustrate a fundamental challenge with the Norwegian central government, because it is difficult to establish strong coordination function. In the introduction, I asked whether these coordination problems have been similar in ICT security policy. During the period of 1997-2013, I will argue ICT security policy had formidable coordination problems, unlike other subfields of public security. ICT security policy was in this period coordinated by two ministries, which brought overlap, uncertainties and tensions. A key issue was also that MoI&T/MoR&A, which had primacy over MoJ in ICT security during those years, lacked traditional hierarchical authority over key security and auditing organizations at agency level. With the sectoral responsibilities of MoI&C and PTT/Nkom for electronic communication in the mix, an extremely complex situation with major coordination pressure within the field of ICT security occurred. The collegial governing system proved unable to

provide sufficient coordination across government, and ICT security had to integrated to MoJ's portfolio to reduce complexity. It seems, therefore, like the coordination problems of ICT security during 1997-2013 have exceeded the problems of public security. The implication for future organization of public security seems to be that enforcement of cross-sectoral coordination by two ministries on overlapping security issues is not a good solution. Another lesion learned seem to be the importance of traditional hierarchical control over key agency level organizations. Without clear vertical connection, the lead ministry ends up in a complex collegial system of governing, fueled by tensions.

In the introduction, I also asked if the coordination problems still are manifest as of 2018. It actually seems like public security policy pulled off a bit of a surprise with the 2017 policy about strengthened coordination authority to MoJ since it broke with the institutionalized pattern. To go from recommendations and counseling to determine requirements in public security policy and national ICT standards across ministry level is a significant change in coordination authority. Possibly, the effects are less fragmentation and more integration and less pulverization of responsibility since MoJ are more clearly in charge.

On the agency level, ICT security also seem to offer important insight to public security policy. The hybrid organization of NSM in the interface of civil and military sector, concentrating capabilities in only one organization, seems to enhance a holistic approach to ICT vulnerabilities and threats. Possibly, similar civil-military hybrids and concentration of capabilities into one organization can be effective in other aspects of security policy.

On the broader universe on how governments can handle wicked problems, this case can offer some implications (Head, 2008; Head & Alford, 2015). On the more operational level, it seems like creation of multifunctional, hybrid organization are central to view issues across traditional organizational and sectoral borders. On the ministerial level, it seems crucial that a lead ministry on a wicked issue has some instruction authority over the other ministries to ensure integrated policies. If not, negotiation and fragmentation seem bound to happen. This can for example be transferable to the transboundary issue of environmental policy, and imply that Ministry of Climate and Environment needs some authority over the other ministries to ensure coherent policies outside regulations through laws.

On the broader universe of trends in the central government more generally, this case offers interesting insight into the balance between the ministerial rule system and cross-sectoral coordination. The primacy of ministerial authority and secondary nature of cross-sectoral measures seem systematic of the central government. What is highly interesting is the 2017 break with dominance of the ministerial rule and that a lead ministry received authority across

the ministry level. Maybe, it can imply that similar JUG-measures can be possible to achieve on other transboundary issues in the future.

Strengths, weaknesses and future research

The strengths of this thesis lie in the collection of a wide range of public documents, and the content analysis approach. These documents have offered solid information about key organizational solutions and how the central government has been thinking. By viewing the information in relation to each other and over time, organizational features, consequences and trends has been researchable in a fairly valid and reliable way. However, the weakness lies in documents overarching level. Data-collection of more internal documents and/or interviews would have promoted more depth to the analysis. It would have offered more insight into how arrangements are operating or drivers behind changes. Three arrangements or changes suffer from these weaknesses – outside the more general problem of the confidential nature of security policy.

Firstly, the information about the ICT and ICT security ministry model, its creation and how it operated, is limited. It does not seem to be any previous research on this arrangement either. What was the organizational thinking of the Bondevik 1 government in 1997? And, why did the arrangement survive after the 2002 white paper clearly made MoJ responsible for overarching ICT security? These questions have not been answered fully by this thesis. Secondly, and more contemporary, the drivers behind the 2017 increased coordination authority is highly uncertain based on this empirical material. It is a key development in the organization of ICT and public security. Its context should be better understood and investigated more. Thirdly, the consequences of the 2017 policies should also be researched more. What are the actual consequences of MoJ's increased authority and how does the new network arrangements operate? What is defined as "requirements" and "national standards" which MoJ's authority is based upon? Are tendencies of positive coordination more visible?

References

ABC Nyheter. (2019). *Nettverksfeil slo ut all norsk flytrafikk*. Retrieved from https://www.abcnyheter.no/reise/reisenyheter/2019/02/08/195548186/nettverksfeil-slo-ut-all-norsk-flytrafikk

Adcock, R., & Collier, D. (2001). Measurement Validity: A Shared Standard for Qualitative and Quantitative Research. *American Political Science Review, vol 95 (3)*, pp. 529-546.

Andersen, S. (2013). *Case-studier og generalisering. Forskningsstrategier og design.* Bergen: Fagbokforlaget.

Boin, A., Busuioc, M., & Groenleer, M. (2014). Building European Union capacity to manage transboundary crises: Network or lead-agency model? *Regulation and Goverance, vol 8 (4)*, pp. 418-436.

Bouckaert, G., Peters, G., & Verhoerst, K. (2010). *The Coordination of Public Sector Organizations: Shifting Patterns of Public Management.* UK: Palgrave Macmillan.

Brattberg, Ø. (2014). *Tekstanalyse for samfunnsvitere.* Oslo: Cappelen Damm Akademisk.

Brunsson, N. (2006). *The Organization of Hypocricy: Talk, decisions and actions in organizations.* Copenhagen Business School Press / Liber / Universitetsforlaget.

Bryman, A. (2012). *Social Science Reseach.* Oxford: Oxford University Press.

Christensen, T., & Lægreid, P. (2007). The Whole-of-Government Approach to Public Sector Reform. *Public Administration Review, vol 67 (6)*, pp. 1059-1066.

Christensen, T., & Lægreid, P. (2011). Complexity and Hybridity in Public Administration—Theoretical and Empirical Challenges. *Public Organizations Review, vol 11 (4)*, pp. 407-423.

Christensen, T., Danielsen, O., Lægreid, P., & Rykkja, L. (2014). The Governance of Wicked Issues: A European cross-country analysis of coordination for societal security. *Uni Research Rokkan Centre. Working paper 6*, pp. 1-32.

Christensen, T., Egeberg, M., Larsen, H., Lægreid, P., & Roness, P. (2007). *Forvaltning og politikk.* Oslo: Universitetsforlaget.

Christensen, T., Lægreid, P., & Rykkja, L. (2016). Organizing for Crisis management: Building Governance Capacity and Legitimacy. *Public Administration Review, vol 76 (6)*, pp. 887-897.

Christensen, T., Lægreid, P., & Rykkja, L. (2018). Establishing a National Police Emergency Response Center: How Urgency Led to Delay. *Risk, Hazards & Crisis in Public Policy, vol 9 (2)*, pp. 183-204.

Christensen, T., Lægreid, P., & Rykkja, L. (2018). Reforming the Norwegian police between structure and culture: Community police or emergency police. *Public Policy and Administration, vol 33 (3)*, pp. 241–259.

Christensen, T., Lægreid, P., Roness, P., & Røvik, K. (2009). *Organisasjonsteori for offentlig sektor.* Oslo: Universitetsforlaget.

Crowther, G. (2017). The cyber domain. *The cyber defense review*, pp. 63-78.

DiMaggio, J., & Powell, W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review, vol 48 (2)*, pp. 147-160.

Egeberg, M. (1999). The impact of bureacratic structure on policy making. *Public Administration, vol 77 (1)*, pp. 155-170.

Egeberg, M. (2012). How bureaucratic structure matter: An organizational perspective. In G. Peters, & J. Pierre, *The SAGE handbook of public administration* (pp. 157-168). London: SAGE Publications Ltd.

Fimreite, A., Lango, P., Lægreid, P., & Rykkja, L. H. (2014). *Organisering, samfunnssikkerhet og krisehåndtering.* Universitetsforlaget.

Forsvarsdepartementet, Nærings- og handelsdepartementet & Justis- og politidepartementet. (2003). Nasjonal strategi for informasjonssikkerhet.

Forynings- og administrasjonsdepartementet, Justis- og politidepartementet, Forsvarsdepartementet & Samferdelsdepartementet. (2007). Nasjonale retningslinjer for å styrke informasjonssikkerheten 2007-2010.

Gerring, J. (2007). *Case Study Reseach.* Cambridge: Cambridge University Press.

Gulick, L. (1937). Notes on the theory of organization. In L. Gulick, & L. Urwick, *Papers on the science of administration.* New York: Institute of Public Administration.

Hammond, T. (1990). In defense of Luther Gulick's "Notes on the theory of organization. *Public Administration, vol 68 (2)*, pp. 143-173.

Head, B. (2008). Wicked problems in public policy. *Public policy, vol. 3 (2)*, pp. 101-118.

Head, B., & Alford, J. (2015). Wicked problems: Implications for public policy and management. *Administration and society, vol 47 (6)*, pp. 711-739.

Hood, C. (1991). A Public Management For All Seasons. *Public Administration, vol 69 (1)*, pp. 3-19.

Johannessen, A., Tufte, P., & Christoffersen, L. (2016). *Introduksjon til samfunnsvitenskaplig metode.* Oslo: Abstrakt forlag.

Justis- og Beredskapsdepartementet. (2013). Virksomhetsstrategi 2013-2017.

Justis- og beredskapsdepartementet, Forsvarsdepartementet, Samferdelsdepartementet & Fornyings- & administrasjonsdepartementet. (2012). Nasjonal strategi for informasjonssikkerhet.

Kavanagh, D., & Richards, D. (2001). Departementalism and Joined-Up Government: Back to the future. *Parliamentary Affairs, vol 54 (1)*, pp. 1-18.

Kgl. res. (20.12.1996). Omorganisering av departementsstrukturen fra 1. januar 1997.

Kgl.res. (01.10.2004). Omorganisering av departementsstrukturen fra 1. oktober 2004.

Kgl.res. (03.11.2000). Instruks om innføring av internkontroll og systemrettet tilsyn med det sivile beredskapsarbeidet i departementene.

Kgl.res. (10.03.2017). Ansvaret for samfunnssikkerhet i sivil sektor på nasjonalt nivå og Justis- og beredskapsdepartementets samordningsrolle innen samfunnssikkerhet og IKT-sikkerhet.

Kgl.res. (11.11.2011). Endring av navn fra Justis- og politidepartementet til Justis- og beredskapsdepartementet.

Kgl.res. (15.06.2012). Instruks for departementenes arbeid med samfunnssikkerhet og beredskap, Justis- og beredskapsdepartementets samordningsrolle, tilsynsfunksjon og sentral krisehåndtering.

Kgl.res. (16.09.1994). Om Justisdepartementets samordningsfunksjon på beredskapssektoren og om rådet for sivilt beredskap.

Kgl.res. (19.12.1997). Omorganisering av departementsstrukturen fra 1. januar 1998.

Kgl.res. (22.03.2013). Overføring av samordningsansvaret for forebyggende IKT-sikkerhet fra Fornyings-, administrasjons- og kirkedepartementet til Justis- og beredskapsdepartementet.

Kgl.res. (29.08.2003). Vedtak om opprettelse av Direktoratet for smfunnssikkerhet og beredskap.

King, G., Keohane, R., & Verba, S. (1994). *Designing Social Inquiry: Scientific Inference in Qualitative Research.* Princeton: Princeton University Press.

Klijn, E.-H., & Koppenjan, J. (2012). Governance network theory: past, present and future. *Policy & Politics, vol 40 (4)*, pp. 587-606.

Krasner, S. (1988). Sovereignty: An Institutional Perspective. *Comparative Political Studies, vol 21 (1)*, pp. 66-94.

Lov om elektronisk kommunikasjon (Ekomloven), 83 (07 04, 2003).

Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), 10 (03 20, 1998).

Lægreid, P., & Rykkja, L. (2015). Organizing for “wicked problems” – analyzing coordination arrangements in two policy areas. *International Journal of Public Sector Management, vol 28 (6)*, pp. 475-493.

Lægreid, P., & Rykkja, L. H. (2018). *Societal security and crisis management.* Palgrave Macmillan.

Lægreid, P., & Serigstad, S. (2006). Framing the Field of Homeland Security: The case of Norway. *Journal of Management Studies, vol 43 (6)*, pp. 1395-1413.

Mahoney, J. (2000). Path dependence in historical sociology. *Theory and Society, vol 29 (4)*, pp. 507-548.

March, J., & Olsen, J. (1989). *Rediscovering Institutions: The Organizational Basis of Politics.* New York, USA: The Free Press.

Meyer, J., & Rowan, B. (1977). Institutionalized Organizations: Formal Structure as Myth and Ceremony. *The American Journal of Sociology, vol 83 (2)*, pp. 340-363.

Nasjonal sikkerhetsmyndighet. (2011). Rapport om sikkehetstilstanden.

Nasjonal sikkerhetsmyndighet. (2018). *NSM etablerer Nasjonalt cybersikkerhetssenter*. Retrieved from https://www.nsm.stat.no/aktuelt/nsm-etablerer-nasjonalt-cybersikkerhetssenter/

NATO. (2016). *Cyber defense pledge*. Retrieved from https://www.nato.int/cps/en/natohq/official_texts_133177.htm

NOU. (2000: 24). *Et sårbart samfunn.* Oslo: Statens forvaltningstjeneste.

NOU. (2006: 6). *Når sikkerheten er viktigst.* Oslo: Departementenes servicesenter.

NOU. (2012: 14). *Rapport fra 22. juli kommisjonen.* Oslo: Departementenes servicesenter.

NOU. (2015: 13). *Digital sårbarhet - sikkert samfunn.* Oslo: Departementenes sikkerhets- og serviceorganisasjon.

NOU. (2018: 14). *IKT-sikkerhet i alle ledd.* Oslo: Departementenes sikkerhets- og serviceorganisasjon.

NRK. (2018). *PST etterforsker dataangrep mot fylkesmenn*. Retrieved from https://www.nrk.no/norge/pst-etterforsker-dataangrep-mot-fylkesmenn-1.14356745

NRK. (2019). *Dataangrepene mot Helse Sør-Øst*. Retrieved from https://www.nrk.no/nyheter/dataangrepet-mot-helse-sor-ost-1.13873606

Olsen, J. (2007). Understanding Institutions and the Logic of Appropriateness: Introductory Essay. *ARENA UiO, Working paper nr. 13*, pp. 1-16.

Osborne, S. (2010). *The New public governance? Emerging perspectives on the theory and practice of public governance.* London: Routledge, Taylor & Francis Group.

Pierson, P. (2000). Increasing Returns, Path Dependence, and the Study of Politics. *The American Political Science Review, vol 94 (2)*, pp. 251-267.

Pollitt, C., & Bouckaert, G. (2004). *Public Management Reform.* Oxford: Oxford University Press.

Riksrevisjonen. (2005: dokument nr. 3:4). *Riksrevisjonens undersøkelse av myndighetenes arbeid med å sikre IT-infrastruktur.*

Riksrevisjonen. (2010: dokument nr. 1). *Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2009.*

Riksrevisjonen. (2018: dokument nr. 3:11). *Riksrevisjonens undersøkelse av oppfølging av objektsikring – oppdatert.*

Rittel, H., & Webber, M. (1973). Dilemmas in a general theory of planning. *Policy sciences, vol 4 (1)*, p. 155.169.

Scharpf, F. (1994). Games Real Actors Could Play: Positive and Negative Coordination in Embedded Negotiations. *Journal of Theoretical Politics, vol 6 (1)*, pp. 27-53.

Scott, W. (2014). *Institutions and Organizations - Ideas, Interests and Identities.* London, UK: SAGE Publications, Inc.

Selznick, P. (1957). *Leadership in Administration.* New York: Harper & Row.

Simon, H. (1946). The proverbs of administration. *Public Administration Review, vol 6 (1)*, pp. 53-67.

St. Meld. (nr. 17 (2006-2007)). Eit informasjonssamfunn for alle. Fornyings- og administrasjonsdepartementet.

St. Meld. (nr. 39 (2003-2004)). Samfunnssikkerhet og sivil-militært samarbeid. Justis- og politidepartementet.

St. Meld. . (nr. 25 (1997-1998)). Hovedretningslinjer for det sivile beredskaps virksomhet og utvikling i tiden 1999-2002. Justis- og politidepartementet.

St. Meld. (nr 38 (2016-2017)). IKT-sikkerhet: Et felles ansvar. Justis- og beredskapsdepartementet.

St. Meld. (nr. 10 (2016-2017)). Risiko i et trygt samfunn. Justis- og beredskapsdepartementet.

St. Meld. (nr. 17 (2001-2002)). Samfunnssikkerhet - veien til et mindre sårbart samfunn. Justis- og politidepartementet.

St. Meld. (nr. 17 (2006-2007)). Eit informasjonssamfunn for alle. Fornyings- og administrasjonsdepartementet.

St. Meld. (nr. 22 (2007-2008)). Samfunnssikkerhet - Samvirke og samordning. Justis- og politidepartementet.

St. Meld. (nr. 29 (2011-2012)). Samfunnssikkerhet. Justis- og beredskapsdepartementet.

St. Meld. (nr. 47 (2000-2001)). Telesikkerhet og -beredskap i et telemarked med fri konkurranse. Samferdelsdepartementet.

St. Meld. (nr. 48 (1993-1994)). Langtidsplanen for den sivile beredskap 1995-1998. Justis- og politidepartementet.

Streek, W., & Thelen, K. (2005). *Beyond Continuity. Institutional Change in Advanced Political Economies.* Oxford, UK: Oxford University Press.

The Telegraph. (2018). *WannaCry cyber attack cost the NHS £92m as 19,000 appointments cancelled*. Retrieved from https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/

Thelen, K. (1999). Historical Institutionalism in Comparative Politics. *Annual Review of Political Science, vol 2*, pp. 369-404.

Tjora, A. (2010). *Kvalitative forskningsmetoder i praksis.* Oslo: Gyldendal Akademisk.