SCANDINAVIAN JOURNAL OF
MILITARY STUDIES

Jensen, M. S. (2018). Sector Responsibility or Sector Task? New Cyber Strategy Occasion for Rethinking the Danish Sector Responsibility Principle. *Scandinavian Journal of Military Studies,* 1(1), pp. 1–18, DOI: https://doi.org/10.31374/sjms.3

RESEARCH ARTICLE

Sector Responsibility or Sector Task? New Cyber Strategy Occasion for Rethinking the Danish Sector Responsibility Principle

Mikkel Storm Jensen
Royal Danish Defence College, DK
msje@fak.dk

Over the last two decades the state's traditional duty to defend its citizens against threats has been extended to a new man-made domain: the cyber domain. As part of this defence states have created systems for establishing a level of preparedness in order to ensure societies' resilience. 'Resilience' in this regard describes societal robustness – not only to deflect outside pressure, but also to absorb its effects and constantly adapt to changing conditions by collecting knowledge of negative events, learning from it and implementing the experience. Denmark's cyber resilience plays an increasing role, as digitisation has meant that threats in the cyber domain have changed from peripheral nuisances to questions of national security.

Hence, the Danish government has initiated the development of a new strategy for cyber and information security. Also, Denmark has committed to implementing the EU NIS Directive concerning measures for a high common level of security of network and information.

This report focusses on those governmental aspects of the strategy that play a role in Denmark's resilience against cyber threats. The report suggests that the new cyber strategy, along with the implementation of the EU NIS Directive, is an occasion to adjust the current interpretation of the sector responsibility principle. The report finds that the sector responsibility principle must remain the basic principle for governance of societal resilience in Denmark, but that adding some central authority and clarifying the division of responsibilities may overcome identified weaknesses in the current implementation of the principle.

Keywords: Cyber; Strategy; Resilience; Defence; Deterrence

Introduction

'Denmark is continuously facing a very high cyber threat'. These are the opening words of the Danish Defence Intelligence Service's (DDIS) national risk assessment for 2017 (Forsvarets Efterretningstjeneste, 2017). Over the last two decades the state's traditional duty to defend its citizens against threats has been extended to a new man-made domain: the cyber domain. As part of this defence states have created systems for establishing a level of preparedness in order to ensure societies' resilience. 'Resilience' in this regard describes societal robustness – not only to deflect outside pressure, but also to absorb its effects and constantly adapt to changing conditions by collecting knowledge of negative events, learning from it and implementing the experience. Denmark's cyber resilience plays an increasing role, as digitisation of society has meant that threats in the cyber domain have changed from peripheral nuisances to questions of national security (K. K. Christensen & Lund Petersen, 2017, p. 1435).

Hence, the Danish government has initiated the development of a new strategy for cyber and information security.[1] The intention is to build on the results of Denmark's first strategy from 2014 (Regeringen, 2016a, p. 47). Concurrently with this process, Denmark has committed to implementing the EU NIS Directive

[1] This article was submitted in January 2018 prior to the Danish government's release of the new strategy for cyber and information security on May 15, 2018.

concerning measures for a high common level of security of network and information before May 9, 2018 (Europa Parlamentet, 2016).

A comprehensive national cyber strategy must necessarily include various aspects such as building and maintaining a capable cyber workforce, establishing military cyber capabilities and invoking international cooperation and diplomatic efforts to influence and develop norms for the interaction of states in the cyber domain.

This report will focus solely on those governmental aspects of the strategy that play a role in Denmark's societal resilience against events originating from the cyber domain. The report suggests that the new cyber strategy along with the implementation of the EU NIS Directive is an occasion to adjust the current interpretation of the sector responsibility principle. The report finds that the sector responsibility principle must remain the basic principle for governance of societal resilience in Denmark, but that adding some central authority and clarifying the division of responsibilities may overcome identified weaknesses in the current implementation of the principle.

Recommendations: The Danish government should consider using the implementation of the new cyber and information security strategy and of the EU NIS Directive as an opportunity to:

- Establish more clear and operational institutional definitions of the terms 'critical infrastructure' and 'operator of essential services'.
- Improve the cross-sector coordination by ensuring that a single authority maintains situational awareness and can follow, guide and, if necessary, command the sector authorities' implementation and execution of Denmark's cyber resilience.
- Establish robust and detailed reporting mechanisms with common metrics for the implementation of the cyber strategy and the specific measures herein – measured not as money spent, but as actual outcome.
- Improve Public-Private Partnership (PPP) through the measures listed above and further facilitate PPP.
- Improve cross-sector coordination by appointing an authority to distribute costs connected with the implementation of the new cyber strategy when such costs cover more than one sector or fall between sectors.

The Report's Structure and Methods

The report goes through a number of theoretical arguments explaining why cyber resilience is crucial to national security regardless of what other defensive measures the government might employ against cyber threats. Then follows a discussion of the term 'critical infrastructure' with regard to national resilience and of why some variation of the sector responsibility principle is a pre-condition for cyber resilience in modern, complex societies. Having established that, the report demonstrates that there is a need to combine the sector responsibility principle with some degree of central authority, responsibility and ability to impose decisions in order for the principle to be an efficient means of governance. A description of Finland's governance of societal resilience is inserted as an example of a balanced approach to the division of central and sector responsibilities. Then follows a presentation of the upcoming cyber strategy, as described in the Danish government's directive from December 2016, and of the strategic leadership's expectations for the strategy, as expressed by the political parties represented in the Danish Parliament.

In the analytical part the report compares identified demands for centralisation of authority with the current situation in Denmark regarding cyber resilience and attempts to assess to which degree the upcoming cyber strategy will address the identified challenges.

The report is based on current, predominantly European and US literature on societal resilience, focussing primarily on threats emanating from the cyber domain. Initially the literature was reviewed in order to find arguments for alternatives to the sector responsibility principle. However, the theoretical arguments overwhelmingly suggested that this principle is an unmissable part of governance when it comes to developing cyber resilience in modern, complex societies. Hence, the literature was revisited to identify which elements of centralisation of authority are necessary to govern through implementation of the sector responsibility principle.

Alongside the review of theoretical literature, Danish and EU laws, directives and strategies were analysed along with recent scientific reports and article on relevant aspects of Denmark's cyber resilience.

The expectations for the upcoming strategy of Denmark's political and strategic leadership were established through interviews conducted between September and November 2017 with the spokespersons on defence issues from the parties represented in parliament. The civil servants' work on developing the strategy was mapped out through interviews with the Ministry of Defence, the Danish Agency for Digitisation, the Centre for Cyber Security (CFCS) and the Danish Emergency Management Agency. The Council for Digital Security (Rådet for Digital Sikkerhed) was interviewed to include viewpoints from the private sector. Due to the ongoing work (as of January 2018) on the strategy, the Danish Agency for Digitisation, which has been appointed by the Ministry of Finance to oversee the cross-ministerial coordination, was severely restricted in its ability to disclose details regarding the process. Finally, a number of interviews were conducted in Copenhagen and Helsinki in September and November 2017 with key persons involved in research and governance within Finland's comprehensive security and cyber strategy; the aim was to gain insight into Finland's approach to balancing sector and central responsibilities.

Background: Cyber Resilience, Critical Infrastructure and Sector Responsibility

Cyber Resilience

Why is cyber resilience a necessity? In a modern society the government, corporations and citizens depend upon secure, uninterrupted exchange and storage of information in the cyber domain,[2] as described by the acronym CIA: Confidentiality, Integrity, Availability (Von Solms & Van Niekerk, 2013, p. 98). This makes societies vulnerable: Information can be spied upon, compromised or made inaccessible, while physical infrastructure controlled by computers may be damaged or even destroyed. Such events in the cyber domain can trigger negative physical, economic or even societal effects that may cascade through the many interconnections of modern societies.

Threats in the cyber domain originate from four different areas (Van Der Meer, 2013, p. 1):

- State actors conduct cyber network operations (CNO) in the form of network exploitation (CNE) to conduct espionage and to reconnoitre for opportunities to support military operations, or they conduct cyber network attacks (CNA) to impose their will on other states with 'cyber violence' or to sabotage strategic targets.
- Terrorists, political activists and fame-seeking individuals conduct attacks to attract attention to their cause through disturbance or destruction.
- Criminal actors seek financial gains by fraud, stealing data or 'kidnapping' data; this is done by scrambling data and demanding a ransom.
- Finally, human errors, natural disasters and unforeseen secondary effects of non-malign actions in the cyber domain may have the same negative effects as deliberate attacks.

In principle, there are three ways a state can protect society in the cyber domain (Nye Jr., 2016, pp. 54–58):

- Deterrence. A state can attempt to deter opponents from attacking by threatening to counter-attack in some way. Could this strategy work? Yes, and no. Those state actors who base their decisions on cost-benefit analysis may – perhaps – be deterred from attacks. Criminally and politically motivated attackers will continue to attack as long as there is any hope of financial gain or publicity. Accidents cannot be deterred from occurring.
- Protection. A state can attempt to identify critical infrastructure and establish extraordinary protection measures around these in the cyber domain, perhaps even attempt to completely isolate them from the Internet. Could this strategy work? Yes, and no. Extra protection makes it more difficult to attack systems. But even the most elaborate protection will be under constant and innovative pressure from not only deliberate cyberattacks, but also the ever-present threat from human error, technical failure, other accidents or natural disasters. It is therefore likely that even highly protected systems will eventually be penetrated or fail in other ways.

[2] NATO's Cooperate Cyber Defence Centre of Excellence's homepage uses the Finnish definition of cyber domain: '*Cyber domain means an electronic information (data) processing domain comprising of one or several information technology infrastructures. Note 1: Representative to the environment is the utilisation of electronics and the electromagnetic spectrum for the purpose of storing, processing and transferring data and information via telecommunications networks. Note 2: Information (data) processing means collecting, saving, organising, using, transferring, disclosing, storing, modifying, combining, protecting, removing, destroying and other similar actions on information (data)*' (CCDCOE, 2013).

- Resilience. A state can develop society's cyber resilience. In this report cyber resilience is interpreted as the ability to bounce back and overcome negative effects of incidents emanating from the cyber domain. Could this strategy work? Yes. If you accept the assumption that hostile state actors base their decisions of whether or not to conduct an attack in the cyber domain on cost-benefit analysis, the benefit, understood as the impact of attacking a state with well-developed cyber resilience, will, all things being equal, be smaller. Hence, resilience will function as deterrence against rational state actors. Irrational or otherwise alternatively motivated state actors, criminally and politically motivated attacks, accidents and human errors will remain undeterrable, but the impact of incidents originating from these threats will be mitigated and recovery faster in a cyber-resilient society.

While deterrence by threats and special protection of critical infrastructure may thus have their place in any state's cyber strategy, resilience is indispensable with regard to ensuring society's ability to recover as fast as possible, when – not if! – negative effects of events originating in cyberspace occur. Thus, the part of the cyber strategy that involves resilience becomes part of the state's overall strategy for comprehensive security and business continuity management (BCM).

Critical Infrastructure

So the question is what infrastructure and which providers of services to include in a plan for resilience in order to conduct BCM with regard to cyber threats? A review of literature on the topic reveals two main theoretical schools of thought (Lauta, Hoffmann, & Struwe, 2013, p. 6):

- Standpoint 1: Modern societies are so complex that it is futile for a state to attempt to identify and extraordinarily protect any special infrastructure. Instead, the state's main effort should be to increase the general level of resilience.
- Standpoint 2: A state can and should identify particularly sensitive and important infrastructure and service providers and govern these according to special rules designed to increase their protection and resilience.

In Denmark there is no official, institutional definition of 'critical infrastructure' (more on that later in this report), but the term is mentioned in laws and regulations regarding physical infrastructure, IT infrastructure and provision of essential services. In Danish and EU public administration the term 'critical' is sometimes replaced by 'essential', but the interpretation is the same. Another term used is 'functions vital to society', which is described as 'activities, goods and services that provide the basis for society's general ability to operate' (Beredskabsstyrelsen, 2017, p. 7). In this report the fact that terms describing critical infrastructure is part of Danish law is interpreted as implicit acknowledgement in Danish governance of the second theoretical standpoint on the topic; meaning that it is possible and beneficial to identify some infrastructure and deliveries as especially critical or essential and to govern these under special rules in order to improve societal resilience.

Identification and special governance of infrastructure identified as especially significant after an analysis based on national security criteria can be traced back to the eighteenth century in Great Britain. The modern approach developed during the total mobilisation of the national economies during the world wars, where it was used to identify which part of one's own infrastructure to defend and which enemy infrastructure to attack to maximise the negative impact on the economy. Concurrently with this development many Western countries established organisations tasked with the administration and protection of infrastructure deemed critical. As fear of widespread destruction as a result of war diminished after the end of the Cold War in the late 1980s, interest in the area faded, but was revived by the terrorist attacks on the US on September 11, 2001. Initially the revitalised interest was resilience against terror attacks. Threats to national security originating in the cyber domain had been brought to the attention of the UN General Assembly in 1998 (Zahran, 1998). As these became more apparent over time, focus on critical infrastructure protection changed to cyber (Brassett & Vaughan-Williams, 2015, p. 40).

Why Is the Sector Responsibility Principle a Necessary Element of Societal Business Continuity Management?

The introduction of new public management and increasing privatisation of former government structures in the late 1970s spurred theoretical interest in the implications of the private sector's increasing share of critical infrastructure (Dunn-Cavelty & Suter, 2009, p. 180). The loss of direct national government control

over critical infrastructure due to privatisation was augmented by a parallel increase in international ownership in the private sector and meant that governments had to find new ways to influence societal resilience (Carr, 2016, p. 46).

The role of the state vis-à-vis its citizens is a huge topic, which will be simplified in the present analysis. The starting point of this discussion on the government's role is that the state, as described by Hobbes, has a social contract with its citizens and companies, according to which citizens authorise the state to provide security in exchange for their individual sovereignty (Pogson Smith, 1965, p. 133). Security, at this very basic level, is the core function of the state and cannot be outsourced (Dunn-Cavelty & Suter, 2009, p. 184). Thus, by privatising critical infrastructure and essential services the state may outsource tasks related to comprehensive security to other entities, but it cannot outsource the responsibility for those tasks' fulfilment. Bringing Hobbes' description of the social contract up to the present day, it is an integral part of the state's responsibility to protect its citizens and, by extension, companies to ensure a level of resilience enabling vital societal functions to continue to operate after negative impacts – including those originating from the cyber domain. While governments' control of critical infrastructure has been reduced or at the very least become more indirect with the introduction of neo-liberal methods of governing, the ability to uphold a democratically accepted level of resilience remains an important element in the legitimacy of the state vis-à-vis its citizens (Brassett & Vaughan-Williams, 2015, p. 37).

Right up to the end of the Cold War and the increasing globalisation in the 1990s, well-organised Western states were able to organise and control critical infrastructure and essential services through centralised command structures in case of crises. A significant share of the critical infrastructure was state-owned, and the remaining private sector was often composed of major companies whose ownership lay within national borders and thus could be influenced by patriotism or controlled by law. While internal lines of supply and communication might be complicated, they were manageable and not subject to change overnight. Technical means of communication and administration were likewise well-understood, and often the private sector would have a built-in resilience in the form of stores of goods and supplies that could be temporarily expropriated or otherwise be brought under state control. Hence, a model of societal BCM constructed around a centralised command and control organisation was possible in theory. During the two world wars the major antagonists' economies were run, albeit with limited efficiency, by centralised organisations that collected relevant information from the economies and, after analysis, produced orders to relevant entities in order to ensure societal BCM and the war effort (Walker & Cooper, 2011).

As stated above, today globalisation and privatisation of government services have changed the situation. Most critical infrastructure and essential services have been outsourced to companies that are often not even owned by national entities. These companies rely on networks of subcontractors and suppliers that are even further removed from direct government oversight and are likely to be changing constantly. At the same time, critical infrastructure, communication and production are now based on new and constantly evolving cyber-based technology and just-in-time delivery of supplies. In other words, societies have gone from being complicated to being complex. It follows that the task of collecting and processing sufficient amounts of information to react in time and produce orders to run the economy with any semblance of coherence has become insurmountable for a centralised organisation (Walker & Cooper, 2011).

Practical experiences from the United Kingdom demonstrate that BCM during crises in modern, complex societies requires local and updated knowledge to be resolved. They also demonstrate that the necessary prior planning, coordination and exercise activities may occur without the initiative of any central authority, but that this is often not the case. Centralised initiatives and demands for preparatory activities such as laws and regulations have a significant and positive effect on the level of resilience (Brassett & Vaughan-Williams, 2013, p. 235).

The change from complicated to complex societies has shifted the discussion on how to achieve resilience from a central approach inspired by mechanical models to neoliberal, dynamic and self-regulating approaches inspired by ecological models (Brassett & Vaughan-Williams, 2015, p. 36; Duffield, 2012, p. 481). In this paradigm the government's role is no longer to control events during crises, but to establish conditions that give the involved actors the abilities and incentives to react in an optimal manner. Along with this development another challenge has emerged over time in the cyber domain, namely a challenge to the traditional clear difference between governance under normal conditions and during crises, respectively. The new normalcy is that actors in cyberspace are under constant attack (Duffield, 2012, p. 479).

In case of a critical cyber incident, the 'point of the spear' of the stricken sectors is the only place where there is sufficient and updated knowledge about the involved cyber-based systems and interdependencies between essential providers and subcontractors to react in time and begin improvisations in order to sustain

vital services and begin to recover (Dunn-Cavelty & Suter, 2009, p. 183). Thus, a centralised, top-down command structure is generally not an applicable solution for societal BCM; the solution has to involve elements of the sector responsibility principle, where individual government sectors identify and administrate critical infrastructure through a combination of facilitation, motivation and law. Dunn-Cavelty and Suter demonstrate how sectors with the proper combination of organisation and incentives can operate as self-organising networks that contribute to societal resilience (Dunn-Cavelty & Suter, 2009).

During the Cold War Denmark's primary means of BCM was a doctrine and organisation under the headline 'total defence' (Forsvarskommissionen, 1997, p. 114). Total defence was a centralised model which through employment of the sector responsibility principle organised and trained cooperation between Denmark's military defence and other authorities responsible for communication, food distribution, transport, energy etc. As in many other Western societies most critical infrastructure was run by government-controlled entities, and essential providers in the private sector were mostly nationally owned companies (Lauta et al., 2013, p. 2). Hence, the task of the total defence of organising resilience and prioritising scarce resources was complicated, but not complex. To a large degree there was a linear and well-understood connection between action and effect, not least because a significant share of the involved actors were under the direct or indirect command of government entities. The challenge for the organisation of the total defence was therefore to collect and process relevant information and then react in a timely and appropriate manner.

Today the Danish society is no longer complicated; it is complex. The government has outsourced a significant share to networks of private corporations. As previously mentioned, there is no institutional definition of critical infrastructure in Denmark and, hence, no precise statistics on the share held on private hands. The U.S. Chamber of Commerce reports that private actors make up 85 % of what is defined by the Department of Homeland Security as critical infrastructure (U.S. Chamber of Commerce, 2018). As the health sector, one of the 16 sectors defined as critical, to a large degree is private in the U.S., but public in Denmark, a similar method of identifying privately owned critical infrastructure in Denmark would likely find the share to be somewhat less than 85 %, but still very significant (Departement of Homeland Security, n.d.).

Insight Without Outlook: Sector Responsibility and the Need for Central Authority

Sector Responsibility and the Need for Central Definitions of Critical Infrastructure

The process of identifying critical infrastructure in itself gives rise to a demand for centralised decision-making. In order to identify what constitutes as critical, all sectors have to work from a common, central decision on what is strategically important. In a democracy decisions regarding what is considered critical in a crisis and what is deemed less important should at the basic level be part of the political debate. Once decided, the implementation becomes part of a top-down process.

The individual sectors can only take on the role as self-organising networks with a view to optimising societal business continuity management if they have clear objectives towards which to self-organise. Therefore, the government should develop clear common objectives and priorities based on analysis of social, economic and security-related issues. These priorities and objectives should be communicated in a clear and timely manner to the individual sectors, which will enable them to identify critical infrastructure and providers of essential services. The next step for the central authority would be to monitor and assess the implementation in the individual sectors and coordinate activities that involve more than one sector or are in danger of not being addressed if considered peripheral to the core responsibilities of one or more sectors. Should the central monitoring authority realise a need to strengthen the coordination between or increase the efforts within sectors, it must identify the right means for doing so. The spectrum of methods goes from assistance to voluntary, self-motivated action to enforcement by law and threat of sanctions. The central authority must find ways to assess the effect of its actions on societal business continuity management, as implemented in the individual sectors, and adjust them accordingly in order to avoid sectors lagging behind the decided level of resilience, which incurs more risk than accepted, or sectors implementing excessive levels of resilience, which *ceteris paribus* will incur more costs than allocated to the task (Dunn-Cavelty & Suter, 2009, p. 184). As it is a basic assumption for this report's analysis that the government can outsource critical tasks, but not the responsibility for their fulfilment, and that a significant share of critical infrastructure is on private hands, cyber resilience in the public sector alone is insufficient to ensure societal resilience. Hence, the governance of resilience through the sector responsibility principle must involve private operators of critical infrastructure.

Sector Responsibility and the Need for Central Outlook

As described above, the individual sectors have excellent insight into their own operations, but limited outlook of cross-sector interdependencies. As a crisis develops, hitherto unidentified, but nevertheless important interdependencies between sectors may surface and go unnoticed by the individual sectors. Another potential issue is that the prioritisation of efforts to recover after an incident may be optimal seen from the stricken sector, but suboptimal seen from other sectors where second-order effects occur out of sight from the sector dealing with the incident.

This demonstrates the need for a central authority with a cross-sector outlook that can maintain situational awareness during crises and assist the individual sectors in coordinating and prioritising their efforts to recover. The same authority would also be tasked with prioritising limited resources such as the national computer emergency response teams (CERTs) according to a cross-sector assessment of the individual sectors' needs and roles in the society's BCM.

Sector Responsibility and the Need for Central Distribution of Costs

Another area where the need to combine sector responsibility with a central authority becomes very explicit is the distribution of costs associated with establishing resilience such as specifying critical infrastructure. All things being equal, the appointment of infrastructure as critical or of a provider as essential will incur extra costs. The provider will be called upon to take extraordinary measures compared with his prior non-essential status. These costs will add to the price of his services, meaning that the consumer will either get less on the same budget or have to pay more to receive the same amount as before. The sector identifying the provider as essential also incurs extra costs, as it now has to allocate resources to administer the essential provider and ensure that he actually implements and maintains the extraordinary resilience measures required by his new status as essential.

In principle, the individual sectors can be tasked with paying the extra costs themselves. This is defensible from a democratic perspective, as resilience is just another necessary aspect of conducting business and fulfilling a sector's societal obligations, and the allocated budget is an expression of the democratically elected government's priorities. However, this only applies to the intra-sector costs. Any cost of resilience that involves more than one sector or is not directly traceable to specific sectors has to be divided between sectors or funded separately by a central authority.

An Illustrative Example: Finland's Implementation of the Sector Responsibility Principle in Its Resilience Strategy

Due to its troubled history, close proximity to Russia and challenging climate and geography, Finland is internationally acknowledged for maintaining a very high level of societal BCM as part of its comprehensive security policy. Therefore, Finland is used as an example of how a state can approach the challenges of sector responsibility, critical infrastructure, the need for central outlook and distribution of costs, not only between sectors, but also between the public sector and entities in the private sector identified as essential.

In Finland Sectors Get Tasks, but Responsibility Remains Centralised

Finland's sectorial approach stems from a tradition of legally anchored strong sector autonomy that extends down to the level of the individual civil servant. *Auftrags taktik* – mission command – is an integrated doctrine for problem-solving pervading the entire administration, regardless of issue (Kerttunen, 2018). In Finland societal resilience, including cyber resilience, is a very high priority. Based on assessments of the threat environment, the government's national security committee develops strategic objectives on behalf of the government and then distributes the associated tasks among the individual sectors (Turvallisuuskomitea, n.d.). Nevertheless, in 2015, despite unquestionable and unflinching political support, the Finns realised that it was difficult to implement the adopted cyber strategy from 2013 across sectors in a coordinated and uniform manner (Makasiinikatu, 2013). In response, the security committee developed a common matrix of 22 topics according to which the individual sectors' progress was evaluated (*Implementation Programme for Finland's Cyber Security Strategy*, 2017; Author, 2017b).

The Role of the Security Committee in the Governance of Finland's Resilience

Established in 2013 under the Ministry of Defence, the government's national security committee conducts monthly meetings and produces an annual report, which is submitted to the president (Finland Security Committee, 2015). The centrally developed common matrix for assessing the implementation of the cyber strategy improves the sectors' ability to focus their efforts and helps them explain to the public why they

have to allocate resources for cyber resilience along with fulfilling their core functions. It also assists the government in distributing costs that are not immediately traceable to any specific sector. To summarise: In Finland the task of implementing and maintaining resilience lies with the sectors, but the responsibility for defining strategic objectives and implementing associated strategies – including distributing costs – lies with a single authority (Author, 2017b).

The Finnish Approach to Public-Private-Partnership and Societal Resilience

The Finnish National Emergency Supply Agency (NESA) reaches out to 1,500 corporations, all categorised in accordance with an assessment of their criticality to critical infrastructure and essential services ("The National Emergency Supply Agency – Huoltovarmuuskeskus," n.d.). The corporations are divided into seven sectors and subdivided into 20 committees that hold meetings several times a year. At these meetings the committee members are briefed on and share experiences with relevant security-related developments, including cyber threats, but many also use the opportunity to develop other business contacts not related to security issues. At the same time, the corporations keep the authorities updated on technical or other developments that may influence cross-sector interdependencies or mean that new corporations should be included in the organisation and current members be released from their obligations as essential. Sauli Savisalo, director of NESA's Infrastructure Department, has described the scope of NESA's ambitions as follows: 'It's just the top of the iceberg', he said, arguing that 1,500 corporations was perhaps not enough to sustain a truly sufficient level of Public-Private Partnership (PPP) and thus ensure Finland's resilience with regard to its critical infrastructure and providers of essential services (Author, 2017b).

Finland's Costs of Resilience Are Rising and Becoming More Visible

In Finland, PPP, with regard to resilience, has in the past to a significant degree been based on the patriotism and voluntary efforts of individuals. Voluntary action still plays an important role, but the costs of imposing resilience are rising or at least becoming more visible. One cause is that much critical infrastructure is no longer owned and run by the government, and the new private operators have to operate on market terms, whether they are Finnish patriots or disinterested foreign investors. This means that extra costs imposed by extraordinary demands due to resilience-related obligations must be stated in contracts, where they previously may have been less visible or even hidden in the budgets of government entities. However, the fact that costs are becoming more visible has not changed the general political will to sustain a high national level of readiness and resilience as an integrated element of Finland's comprehensive security strategy: 'Where resilience is strong, Russia don't take chances …' (Author, 2017g).

The Upcoming National Strategy for Cyber and Information Security

In December 2016 the Danish government put the Ministry of Defence in charge of a cross-ministerial effort to develop a new national strategy for cyber and information security (henceforth referred to as 'the cyber strategy'). The objective is summarised in this quote from the initiating directive: 'Maintaining systems and services that authorities, citizens and corporations can have confidence in is a precondition for the further development of the welfare society and the exploitation of digital possibilities. Threats against the information security are real and have second-order effects such as economic costs and loss of confidence in the development of digitisation as well as in the entities that fulfil functions vital to society. Solutions will continue to be balanced against costs, ease of use and efficacy'.[3] (Regeringen, 2016b).

Denmark has had national strategies for the public sector's, citizens' and corporations' use of the cyber domain since 2001 ("15 års fælles digitaliseringsstrategier|Digitaliseringsstyrelsen," 2017). The first national strategy for cyber and information security was introduced in 2014. It focussed on government entities as well as on the energy and IT sector and aimed to establish situational awareness regarding risks and weaknesses. Also, the strategy provided guidance for the newly established institutions Centre for Cyber Security (CFCS) under the Danish Defence Intelligence Service and the National Cyber Crime Centre (NC3) under the police (Regeringen, 2014).

The upcoming cyber strategy is meant to build upon the results achieved by its predecessor and to be extended to other sectors – partly by including more entities in the public sector, partly by increasing Public-Private Partnership (PPP). The government's directive can in broad terms be summarised as follows (Regeringen, 2016b):

[3] Author's translation of the original Danish text.

- The strategy must include the following sectors: energy, IT, transport, finance and health along with all government entities and institutions that perform essential societal functions. Other ministries whose responsibility includes elements relevant to the implementation of the strategy also participate in the cross-ministerial effort. All in all, 13 ministries are involved.
- The strategy should be developed based on the sector responsibility principle and facilitate cross-sector communication and knowledge-sharing.

Alongside the development and implementation of the cyber strategy Denmark has pledged to implement EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems, better known as the EU NIS Directive. The new strategy should facilitate this process.

Political Expectations on the Upcoming Strategy

As mentioned, while preparing this report interviews were conducted with the spokespersons on defence issues from the political parties (here mentioned by their Danish names) currently represented in the Danish Parliament. *Alternativet*, though, the latest new party to be represented in parliament, was not available for comments. The spokespersons were asked to describe their expectations on the upcoming strategy and their view on the role of the government in protecting society from threats originating in the cyber domain (Author, 2017a).

All the spokespersons expected the upcoming strategy to present concrete initiatives rather than general intentions. As part of these concrete initiatives, they expected the strategy to further define the role of the established cyber defence institutions, particularly the Centre for Cyber Security.

Looking at the centre-right wing of Danish politics, two of the government's three parties, *Venstre* and *Konservative*, had no further comments. Neither did the government's main supporting party, *Dansk Folkeparti*. The third member of the government, *Liberal Alliance*, expanded on its expectations; it believes the state is obligated to protect its citizens and corporations in the cyber domain, and that private-public partnerships in this regard as a leading principle should rest on voluntary cooperation. Also, the party was adamant that increased efficacy in cyber defence should not be achieved through increased surveillance and by compromising citizens' right to privacy.

The spokespersons from the centre-left wing of Danish politics, *Radikale Venstre*, *Socialdemokratiet*, *Socialistisk Folkeparti* and *Enhedslisten*, shared their right wing colleagues' general expectations for concrete initiatives. They all considered it important for the government to maintain situational awareness of critical infrastructure and providers of essential services, and that the government plays a central role as partner, organiser and facilitator of private-public partnerships. *Socialdemokratiet*, *Socialistisk Folkeparti* and *Enhedslisten* all expressed concern about whether cyber resilience, including the ability to coordinate and cooperate across sectors, was given sufficient priority by the government. *Socialistisk Folkeparti* especially was concerned about the difficulties of coordinating across sector boundaries, as each sector is responsible for its own cyber security. *Enhedslisten* was concerned about the risk of tasks falling between sectors and receiving only 'stepmotherly' attention.

Finally, on principle grounds, *Enhedslisten* was concerned about the constitutional aspects of the main national CERT, the Centre for Cyber Security, being a part of the Danish Defence Intelligence Service. Other parts of the Danish Defence Intelligence Service have no jurisdiction to operate within Denmark's borders, but when operating in its capacity as CERT, the centre falls under specific laws and special supervision by parliament to ensure the upholding of constitutional rights.

The Upcoming Strategy and the Identified Need for Centralisation of Responsibility

Very briefly, the development of Denmark's upcoming cyber strategy can be described as follows: In December 2016 the Ministry of Defence, which normally handles issues of national resilience and readiness, was instructed to coordinate the cross-ministerial aspects of developing and implementing a new cyber strategy. Initially the work was expected to conclude in May 2017, but this deadline was extended. At first the government did not allocate extra funds for the task (Regeringen, 2016b, p. 4).

After seven months with limited progress the government transferred the task of cross-ministerial coordination to the Ministry of Finance in August 2017 and allocated one-time funding of DKK 100 million (EUR 13.43 million) to cover cross-ministerial activities (Forsvarsministeriet, n.d.). The Ministry of Finance then delegated the task of cross-ministerial coordination to the Danish Agency for Digitisation and the strategy was, as of November 2017, expected to be ready for release in February 2018 (Author, 2017e). The Ministry

of Defence is still responsible for the parallel efforts to implement the EU NIS directive (Forsvarsministeriet, n.d.).

In principle, it should not be a particular organisational challenge to decide which government sectors should be included in the upcoming cyber strategy, take part in its development and prepare its implementation. The government ordered the respective ministries to participate in the process in 2016, and so they did. However, as demonstrated by the repeated delays and the transfer of the task to the Ministry of Finance, things turned out not to be so simple. It is very likely that the government decided to transfer the task from the Ministry of Defence to the Ministry of Finance because progress was too slow. It is also likely that the lack of progress was due to the fact that efforts to develop the individual ministries' contributions to the strategy had to compete with the ministries' core functions and were not given priority.

In this regard, there is no reason to blame the Ministry of Defence for the lack of progress; this ministry has no means to influence the quality and scale of the other ministries' efforts. Also, while the Ministry of Defence was responsible for the cross-ministerial coordination no extra funding was allocated to the task, which cannot have helped matters along. One of the government's reasons for re-delegating the task to the Ministry of Finance may have been the ministry's ability to better distribute the allocated DKK 100 million.

The Upcoming Strategy and the Need for Centralised Definitions of Critical Sectors

Unlike a number of other Western democracies such as the United Kingdom, the Netherlands, Sweden and the US, Denmark has no central institutional definition of critical infrastructure (C. K. Christensen & Lund Petersen, 2017, p. 3; CPNI, 2018; Departement of Homeland Security, n.d.; Ministerie van Justitie en Veiligheid, 2010, pp. 4–6; Swedish Civil Contingencies Agency (MSB), 2014, p. 12). Danish law merely points to a number of sectors as examples of critical sectors (Lauta et al., 2013, pp. 8–9). The closest we get to an official institutional definition is in 2010/1 LSF 197, *Forslag til Lov om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v.*, which states, 'The term "critical infrastructure" here comprises, in accordance with the term's interpretation in the realm of national readiness, those sectors that solve vital societal tasks such as the finance, the energy and the IT sector. The term is to be interpreted in a dynamic manner and will thus develop over time as society develops and may make it relevant to include new sectors under the term critical infrastructure'[4] (Ministeriet for Videnskab Teknologi og Udvikling, 2010, p. 18). Thus, Danish government sectors responsible for the administration of critical infrastructure must develop individual and dynamic interpretations of the term, and the wording of the law leaves them with considerable room for interpretation (C. K. Christensen & Lund Petersen, 2017, p. 3).

The task of interpretation is also expressed in this quote from the governments' directive for the upcoming cyber strategy: 'The strategy must focus on those sectors that solve vital societal tasks, and are in particular need of protection under the current risk assessment. Taking as its starting point the objective of developing at strategy that both includes a number of cross-sector efforts and addresses a number of chosen central sectors, the upcoming strategy could focus on the following sectors:

- Energy
- IT
- Transport
- Finance
- Health
- Government authorities and institutions solving vital societal tasks'.[5]

(Regeringen, 2016b, p. 3).

In spite of using the word 'could' instead of 'must' interviews with civil servants in the Ministry of Defence reveal that this list of sectors was considered an order, not a suggestion, when work with the upcoming cyber strategy commenced (Author, 2017f).

As mentioned, Denmark has also pledged to implement EU Directive 2016/1148 concerning measures for a high common level of security of network and information systems. The NIS Directive imposes on the member states the task to identify operators of essential services and to ensure that they live up to a number of demands focussing on ensuring cyber resilience. The intention is to increase the operators'

[4] Author's translation of the original Danish text.
[5] Author's translation of the original Danish text.

and, by extension, the member states' and thus the EU's cyber resilience (Europa Parlamentet, 2016). This raises the question of how narrowly member states interpret EU definitions of operators of essential services. The directive does not mention critical infrastructure, but instead defines operators of essential services as: a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities; b) the provision of that service depends on network and information systems; and c) an incident would have significant disruptive effects on the provision of that service (Europa Parlamentet, 2016, p. 14).

While the directive leaves some room for interpretation, it directly states that the intention of defining relatively narrow and operational criteria for the identification of providers of essential services is to ensure coherent application throughout the union: 'In order to ensure a consistent approach, the definition of operator of essential services should be coherently applied by all Member States. To that end, this Directive provides for the assessment of the entities active in specific sectors and subsectors, the establishment of a list of essential services, the consideration of a common list of cross-sectoral factors to determine whether a potential incident would have a significant disruptive effect, a consultation process involving relevant Member States in the case of entities providing services in more than one Member State, and the support of the Cooperation Group in the identification process. In order to ensure that possible changes in the market are accurately reflected, the list of identified operators should be reviewed regularly by Member States and updated when necessary. Finally, Member States should submit to the Commission the information necessary to assess the extent to which this common methodology has allowed a consistent application of the definition by Member States' (Europa Parlamentet, 2016, p. 4).

The Centre for Cyber Security explains the ongoing Danish implementation of the NIS Directive as follows: The NIS Directive will be implemented alongside the upcoming cyber strategy in accordance with the sector responsibility principle by the individual ministries responsible for the sector in question. The individual ministries will assess the need for and adjust laws within their sector. Also, the individual ministries will stage the criteria for providers of essential services and be responsible for their compliance with sector-specific rules regarding network and information security (Author, 2017d).

In the light of this statement, it may be useful to look at how member states, including Denmark, have interpreted previous EU directives regarding critical infrastructure. In 2008 the EU published directive 2008/114/EF on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (EU, 2008). The directive requires member states to identify critical infrastructures in the energy and transport sectors, the failure of which will affect more than one member state.

Hence, since 2008 the Danish ministries for energy and transport have submitted biannual reports to the European Commission arguing that no such critical infrastructure is present in Denmark. This means that neither the energy sector nor the transport sector has been able to identify *European* critical infrastructure, as defined by the directive, in Denmark. This is fully defensible, as there are alternatives that could alleviate the effects, should the potential candidates – e.g. Copenhagen Airport and the bridge across Øresund to Sweden – fail. Like Denmark, most other member states, including Sweden, have been unable to identify *European* critical infrastructure within their borders (Author, 2017c).

However, the member states' administration of the 2008 directive gives cause to consider the reasons for limiting what is considered providers of essential services when the NIS Directive is to be implemented:

From an *operational* standpoint, it is necessary to limit the designation of critical infrastructure and providers of essential services in order to focus.

From an *administrative* and *economic* standpoint, there are also significant incentives to limit the number: If a provider is categorised as essential, the NIS Directive requires the provider to live up to specific standards that must be integrated in the contract with the provider.

- This puts an extra burden on the provider compared to his competitors and will, *ceteris paribus,* induce costs that may increase the price of the provided service.
- At the same time, the designating authority must set aside resources to ensure that the designated provider lives up to the required standards.

Both aspects have a direct negative influence on the possibility to deliver and administer essential services at the same cost as before the services were designated as essential. While these negative effects will stand out clearly, the societal benefits of increased resilience will only become apparent in the event of crisis – a crisis that may never occur, if investments in resilience are sufficiently effective.

Thus, in principle there is a risk that the ministries administering the sectors could be tempted to prioritise economic concerns over operational ones when designating critical infrastructure or assessing whether the precautions they have taken are sufficient. Especially if, as in Denmark, no funding has been allocated to cover the expected increased cost of resilience when the upcoming cyber strategy and the NIS Directive are implemented. In Denmark, the assessment of what and who are designated is complicated further by the lack of centrally established criteria for critical infrastructure. On the other hand, the lack of criteria could in theory also cause ministries to go too far in their designation of critical infrastructure within their sectors. They would, however, have no economic incentive to do so.

The Upcoming Strategy and the Need for Centralised Outlook

Denmark has a designated crisis management organisation that will come together in extraordinary situations and temporarily have the authority to deal with the effects of a crisis (Beredskabsstyrelsen, 2015, p. 4–8). However, there is no overall authority tasked with coordinating the individual sectors' planning and preparation between incidents (Beredskabsstyrelsen, 2004a, p. 284; C. K. Christensen & Lund Petersen, 2017, p. 1). With regard to threats emanating from the cyber domain, the temporary nature of this construct is a special challenge. The institutions are designed to handle acute and discrete events limited in time and extent: natural disasters, terror attacks or, at worst, war. The cyber domain is characterised by a state of more or less permanent crisis: Public and private organisations and corporations are under constant pressure from criminals and state actors attempting to spy, steal, 'kidnap' or destroy data. Only in instances where attacks in the daily stream of cyber threats slip through the defences and cause severe negative second-order effects that may cascade through societal interdependencies is the crisis management organisation activated.

The Danish doctrine for BCM is, as described above, based on the sector responsibility principle. Sector responsibility and directions regarding civilian authorities' responsibility to plan and prepare are stated in the law on national preparedness, chapter 5, sections 24–28 (Forsvarsministeriet, 1992). The government's directive for the upcoming cyber strategy clearly states that it should build upon the sector responsibility principle and facilitate cross-sector communication and knowledge-sharing (Regeringen, 2016b, p. 2–3). As demonstrated previously in this report, there are good theoretical and practical reasons for basing societal resilience on the sector responsibility principle. The authority responsible for a particular area during a crisis is also responsible for the area during normal conditions and thus the one that holds the most detailed and updated knowledge and is best suited to respond.

A significant part of the practical implementation of both Denmark's first cyber security strategy and the NIS Directive consists of implementing ISO27001 standards in government institutions and private providers of essential services (Europa Parlamentet, 2016; Regeringen, 2014, p. 3). ISO-27001 is not a standard designed particularly for cyber security, but a systematic methodology for mapping and testing an organisation and its sub-contractors in order to achieve maximum robustness and resilience to overcome negative impacts – also in the cyber domain (Digitaliseringsstyrelsen, n.d.).

Where ISO-27001 is properly implemented and maintained, it will give the sectors deep insight into their internal conditions and dependencies. However, the method will only give limited insight into cross-sector interdependencies and strategic impacts of events in other sectors. Hence, there is still a need for a central authority conducting cross-sector knowledge-sharing, coordination and prioritisation of scarce resources such as the national CERT during crises.

Cross-sector knowledge-sharing and coordination can be divided into two separate, but somewhat overlapping tasks: cross-ministerial cooperation between the ministries responsible for particular sectors and strategic cooperation between public and private entities within and between sectors.

In Denmark, the two tasks are represented by two designated forums for cooperation: the Cross-Ministerial Contact Group Regarding Cyber Security (*Den Tværministerielle Kontaktgruppe vedrørende Cybersikkerhed*), which is a network of administrative ministry leaders, and the Strategic Forum for Cooperation on Cyber Security (*Det Strategiske Samarbejdsforum om Cybersikkerhed*), whose members comprise corporations, organisations and trade associations from the private sector (Forsvarsministeriet, 2016).

Cross-Ministerial Cooperation Is a Challenge

With the sector responsibility principle's decentralised responsibility for the implementation of the upcoming cyber strategy follows that the individual ministries must interpret what their responsibility entails (Author, 2017d). At the same time, the ministries evaluate themselves when assessing whether their respective sectors live up to their interpretation of their responsibility. This introduces the significant risk that the sectors do not have a shared understanding of their tasks and that they do not give them the same priority.

Reaching a common understanding of what sector responsibility means for the task of national preparedness was a challenge, even before the task of cyber resilience was added. The Danish Emergency Management Agency's annual national vulnerability report underlined the issue in 2006, and it has been a recurring theme in the evaluations of the national biannual crisis management exercises that have been carried out since 2003 (Beredskabsstyrelsen, 2006b, pp. 22–33) (Beredskabsstyrelsen, 2004b, 2006a, 2007, 2011, 2014, 2016).

According to the Centre for Cyber Security, there are presently different levels of maturity in the different sectors when it comes to implementing the existing and developing the upcoming cyber strategy. A source at the centre assess that the main ambition for the upcoming strategy is less to improve cross-sector coordination, but rather to get the strategy fully implemented within the individual sectors (Author, 2017d).

Public-Private Coordination Is Limited in Scope

Presently the direct and formal knowledge-sharing and coordination between private entities and the government regarding cyber resilience is limited in scope. Within the Strategic Forum for Cooperation on Cyber Security, the Centre for Cyber Security holds three briefings a year for relevant government organisations and invited private sector entities. The meetings are also used as an occasion for knowledge-sharing across sectors. There are no formal or established criteria determining which entities are invited, but the approximately 40 forum participants come from top management levels within IT, finance, energy, transportation and defence. In addition, a number of more technical focussed meetings are held in the Technical Forum (*Teknisk Forum*), where relevant experts can share knowledge. The content of the meetings is classified, and no minutes are released to the general public (Author, 2017d).

Besides these very specific forums for knowledge-sharing, the public and private sectors share information regarding cyber security in a number of other areas. An important venue for sharing technical and other information is when private corporations or public institutions report cyber attacks or other incidents. In Denmark, private corporations are as a rule not required to report cyber incidents. Since 2016, though, all government entities as well as private entities within specific areas – especially telecommunications – have been under obligation to report cyber attacks. Other entities are encouraged to do so voluntarily by the CFCS. The law on CFCS ensures that companies can report attacks and still maintain anonymity by preventing anyone outside the centre from accessing information on reported incidents (Center for Cybersikkerhed, 2016).

Like the Danish government, the Danish private sector regards threats in the cyber domain as serious. However, corporations look at these mainly from an economic perspective, whereas the government also considers national security aspects. Also, a British analysis suggests that many corporations have difficulties determining how much to invest in precautions against cyber incidents from an economic perspective of optimisation – and that there is a tendency to underestimate the necessary investments (Cornish, Livingstone, Clemente, & Yorke, 2011).

Hence, private entities and the government have different starting points for dealing with cyber incidents (K. K. Christensen & Lund Petersen, 2017, p. 1441).

- In Denmark, whenever possible, the government will split its handling of events along classical lines between national security issues and crime. National security issues are sophisticated attacks and advanced persistent threats, especially if they can be attributed to a state actor. These tasks fall under the Centre for Cyber Security operating under the Ministry of Defence, while criminal attacks fall under the police's Cyber Crime Centre (NC3), Ministry of Justice. Other attacks or events may fall under the auspices of the Danish Security and Intelligence Service – also under the Ministry of Justice – or the Danish Agency for Digitisation under the Ministry of Finance. These actors all have an interest in attribution and further investigation of the circumstances and modus of attack in order to improve their knowledge of cyber threats against Denmark (C. K. Christensen & Lund Petersen, 2017, p. 1442).
- The private citizen or corporation struck by a cyber incident is primarily interested in having it stopped and recover as fast as possible. If investigation of the origin and nature of the attack has any interest, its main focus is to identify the attack vector in order to avoid future incidents (K. K. Christensen & Lund Petersen, 2017, p. 1444). Citizens and corporations first encounter this conflict of interest when they wish to report an incident to the Danish authorities; first they have to decide between authorities (K. K. Christensen, Vejen, Og, & Lund Petersen, 2015, p. 6).

The Danish Council for Digital Security (*Rådet for Digital Sikkerhed*) is an independent organisation with members from a wide range of public and private institutions and organisations with an interest in digital

security and legal rights in the cyber domain. According to the council, major trade associations from the private sector participate in Centre for Cyber Security's meetings and find them mutually beneficial. In addition, these and other relevant organisations have been invited by the Danish Agency for Digitisation to contribute with their ideas and concerns to enlighten the development of the upcoming cyber strategy. One of the topics brought forward by the council was the establishment of a common portal for reporting incidents, thus relieving citizens and corporations of the burden of having to find out which authority to report incidents to. In general, the council finds it positive that the trend is towards more deliberate structures for authorities' handling of cyber and information security issues. However, they consider it a challenge that the individual sectors and ministries, from the council's perspective, lack experience in solving these tasks (Author, 2017h).

Also, the Council for Digital Security believes the cyber domain weaknesses that historically have been identified in the Danish administration of national preparedness through the sector responsibility principle will prove a challenge: Sectors have insight, but lack outlook, and coordination between sectors is difficult. Finally, the council is concerned that the strategy under development may not address the question of distribution of the costs of the implementation of the upcoming cyber strategy and the NIS Directive between the public and private sectors, especially in light of the fact that no funds have been allocated to operating costs (Author, 2017h).

Some private sectors, including the financial sector, have gone to greater lengths on the cyber security and resilience arena than required by law. Under the leadership of the Danish Central Bank (*Nationalbanken*) the financial sector established the Financial Sector Forum for Operational Resilience (FSOR) in 2016. FSOR has performed crisis and readiness exercises and since 2017 joined a Nordic financial cooperation on cyber security (FSOR, 2017) (Hansen, 2017). It is likely that the financial sector have gone ahead with these initiatives because it assessed the potential costs of being ill prepared for cyber threats to be greater than the costs of taking the necessary precautions. However, in other parts of the private sector the same market mechanisms would fail to bring cyber resilience to an optimal level from a societal perspective. It is not hard to imagine situations where the potential costs of failure due to cyber incidents for an individual corporation – and by extension the corporation's incentive to invest in cyber security – are much lower than the costs on society due to cascades of second-order effects.

The Upcoming Strategy and the Need for Central Distribution of Costs

In its directive for the upcoming cyber strategy the Danish government has not addressed the question of how costs that effect more sectors or fall between them should be distributed.

As previously stated, the government's original directive from 2016 did not include extra funding for development and implementation of the strategy (Regeringen, 2016b, p. 4). However, as the task of cross-ministerial coordination was redelegated to the Ministry of Finance in August 2017, DKK 100 million were allocated for these purposes (Forsvarsministeriet, n.d.).

However, this is one-time funding, primarily intended to cover initial cross-sectorial costs. It is not supposed to cover the individual sectors' internal costs, and no future funding has been allocated. The main share of the resources necessary for developing, implementing and sustaining the increased demands for cyber security must still be found in competition with the respective ministries' core tasks.

Therefore, it will be a standing task for the respective sectors to find the means themselves, and there will be an ongoing need for political decisions on how to distribute costs that are not clearly attributable to a specific sector.

Due to the ongoing efforts to develop the upcoming cyber strategy, the Danish Agency for Digitisation could not at the time of writing comment on the content of the strategy, including whether or not the involved ministries have a common understanding of how tasks, responsibilities and costs will be divided between them according to the sector responsibility principle (Author, 2017e).

Concluding Remarks: Denmark's Cyber Resilience Is Improving

After this long discussion and identification of weaknesses in the current Danish governance approach to cyber resilience, it is relevant to stress that both the Danish government's and the private sector's cyber resilience has improved in recent years.

The Centre for Cyber Security finds through its many encounters with both government and private entities that the ongoing implementation of Denmark's first cyber security strategy from 2014 has led to greater awareness and more mature and qualified cyber security initiatives throughout society. The centre expects this development to be augmented by the introduction of the upcoming cyber strategy and the implementation of the EU NIS Directive (Author, 2017d).

Conclusion: The Upcoming Strategy Is Unlikely to Address the Need for Introducing More Central Authority in the Danish Administration of the Sector Responsibility Principle

With the caveat that the upcoming cyber strategy is unfinished at the time of writing (January 2018), the present analysis gives rise to the following conclusions:

The need for central definitions of critical infrastructure: It is less likely that the strategy will establish clear institutional definitions of 'critical infrastructure' in Denmark. The task is not mentioned in the government directive. However, the implementation of the EU NIS Directive should force authorities responsible for the process to assess what and who are providers of essential services in accordance with the EU's more operational criteria.

The need for central outlook: The principle of sector responsibility has functioned as the governance guideline for national preparedness at least since 1992 (Forsvarsministeriet, 1992) without leading to a common understanding between the ministries involved of what those responsibilities entail. On this basis, it is unlikely that the Danish Agency for Digitisation will succeed in achieving a common understanding of the division of tasks and responsibilities for implementation and administration of the principle when it comes to national cyber resilience.

The need for central distribution of costs: Presently no extra funding has been allocated to cover the involved ministries' future costs deriving from the upcoming cyber strategy. It is to be expected that the 13 involved ministries will continue to have to prioritise tasks imposed by the cyber strategy in competition with their core tasks. Next to the question of how the public sector's share of the costs should be distributed stands the also unanswered question of how the increased costs of private corporations designated as essential or critical should be covered.

The Effect of the Upcoming Strategy and Implementation of the EU NIS Directive

Even so, the implementation of the upcoming strategy and the EU NIS Directive will very likely have a positive effect on Denmark's cyber resilience. All things being equal, the individual sectors will develop their cyber security as they implement the precautions and recommendations expected of the upcoming strategy. In addition, the implementation will augment awareness of the importance of cyber resilience, not least among managements in all involved sectors, private as well as public.

For those corporations and organisations that will be affected by the NIS Directive, the implementation of the ISO27001 standards will in principle ensure improved communication and coordination between both public and private entities in the respective sectors, because the systematic mapping of interdependencies, incident planning and preparation of means of communication in case of incidents are all elements found in the standards.

However, the cumulative effect on societal resilience will depend on the degree to which the authorities responsible for designating providers of essential services allow their operational assessments to be influenced by purely economic considerations.

Recommendations

The Danish government should consider using the implementation of the new cyber and information security strategy and of the EU NIS Directive as an opportunity to:

- Establish more clear and operational institutional definitions of the terms 'critical infrastructure' and 'operator of essential services'.
- Improve the cross-sector coordination by ensuring that a single authority maintains situational awareness and can follow, guide and, if necessary, command the sector authorities' implementation and execution of Denmark's cyber resilience.
- Establish robust and detailed reporting mechanisms with common metrics for the implementation of the cyber strategy and the specific measures herein – measured not as money spent, but as actual outcome.
- Improve Public-Private Partnership (PPP) through the measures listed above and further facilitate PPP.
- Improve cross-sector coordination by appointing an authority to distribute costs connected with the implementation of the new cyber strategy when such costs cover more than one sector or fall between sectors.

References

Beredskabsstyrelsen. (2004a). National Sårbarhedsudredning Udvalget for National Sårbarhedsudredning. Birkerød. Retrieved from: https://brs.dk/viden/publikationer/Documents/Sårbarhedsudredning_2004.pdf.

Beredskabsstyrelsen. (2004b). Samlet evalueringsrapport. Retrieved from: https://brs.dk/viden/publikationer/Documents/evauleringsrapport_KRISOEV_2003.pdf.

Beredskabsstyrelsen. (2006a). Evalueringsrapport. Retrieved from: https://brs.dk/viden/publikationer/Documents/KRISOEV-2005.pdf.

Beredskabsstyrelsen. (2006b). National Sårbarhedsrapport 2006. Retrieved from: https://brs.dk/viden/publikationer/Documents/National_Saarbarhedsrapport_2006.pdf.

Beredskabsstyrelsen. (2007). Tvaergående evaluering af Krisestyringsøvelse 2007 (KRISØV 2007). Retrieved from: https://brs.dk/viden/publikationer/Documents/KRISOV_2007.pdf.

Beredskabsstyrelsen. (2011). Evaluering af KRISØV 2011. Retrieved from: http://brs.dk/beredskab/idk/Documents/EvalueringsrapportKRISOV2011.pdf.

Beredskabsstyrelsen. (2014). Evaluering af KRISØV 2013. Retrieved from: http://brs.dk/viden/publikationer/Documents/KRISØV 2013 Evalueringsrapport.pdf.

Beredskabsstyrelsen. (2015). Krisestyring i Danmark. Birkerød: Beredskabsstyrelsen. Retrieved from: http://brs.dk/viden/publikationer/Documents/Krisestyring%20i%20Danmark.pdf.

Beredskabsstyrelsen. (2016). Evaluering af KRISØV 2015. Retrieved from: http://brs.dk/viden/publikationer/Documents/Evaluering%20af%20KRIS%D8V%202015.pdf.

Beredskabsstyrelsen. (2017). Nationalt Risikobillede 2017. København. Retrieved from: http://brs.dk/viden/publikationer/Documents/Nationalt-Risikobillede-2017-LowRes.pdf.

Brassett, J., & **Vaughan-Williams, N.** (2013). The Politics of Resilience from a Practitioner's Perspective: An Interview with Helen Braithwaite OBE. *Politics*, *33*(4), 229–239. DOI: https://doi.org/10.1111/1467-9256.12027

Brassett, J., & **Vaughan-Williams, N.** (2015). Security and the performative politics of resilience: Critical infrastructure protection and humanitarian emergency preparedness. *Security Dialogue*, *46*(1), 32–50. DOI: https://doi.org/10.1177/0967010614555943

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62. Retrieved from: http://web.b.ebscohost.com/ehost/pdfviewer/pdfviewer?vid=7&sid=c0cbd54c-87ea-4430-9752-aea6c6e012de%40sessionmgr101. DOI: https://doi.org/10.1111/1468-2346.12504

CCDCOE. (2013). Cyber Definitions. *CCDCOE*. Retrieved January 15, 2018, from https://ccdcoe.org/cyber-definitions.html.

Center for Cybersikkerhed. (2016). Vejledning til underretningsunderordning i tilfælde af cyberangreb. København: Forsvarets Efterretningstjeneste. Retrieved from: https://fe-ddis.dk/cfcs/CFCSDocuments/Vejledning%20til%20underretningsunderordning%20i%20tilf%C3%A6lde%20af%20cyberangreb%20(nyt%20govcert-nummer).pdf.

Christensen, C. K., & **Lund Petersen, K.** (2017). Cybertruslen: Kompleksitet der kræver (an)svar. København. Retrieved from: http://static-curis.ku.dk/portal/files/179618812/T_nketanken_Ret_Sikkerhed_Policy_Paper_Nr._1_Cyberkriminalitet_.pdf.

Christensen, K. K., & **Lund Petersen, K.** (2017). Public-private partnerships on cyber security: A practice of loyalty. *International Affairs*, *93*(10), 1435–1452. DOI: https://doi.org/10.1093/ia/iix189

Christensen, K. K., Vejen, O. L., & **Lund Petersen, K.** (2015). Trusler, kommunikation, nytte: Udfordringer ved offentlig-privat samarbejde om IKT-sikkerhed. København. Retrieved from: http://static-curis.ku.dk/portal/files/155552231/Udfordringer_IKT_5web.pdf.

Cornish, P., Livingstone, D., Clemente, D., & **Yorke, C.** (2011). Cyber Security and the UK's Critical National Infrastructure. *Chatham House*, *32*(5), 1. Retrieved from: https://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r0911cyber.pdf.

CPNI. (2018). Critical National Infrastructure. *CPNI*. Public website. Retrieved January 11, 2018, from: https://www.cpni.gov.uk/critical-national-infrastructure-0.

Department of Homeland Security. (n.d.). Critical Infrastructure Sectors. *Homeland Security*. Retrieved January 8, 2018, from: https://www.dhs.gov/critical-infrastructure-sectors.

Digitaliseringsstyrelsen. (2017). 15 års fælles digitaliseringsstrategier. Retrieved November 21, 2017, from: https://www.digst.dk/Strategier/Strategi-2016-2020/15-aars-digitaliseringsstrategi.

Digitaliseringsstyrelsen. (n.d.). Hvad er ISO27001?|Digitaliseringsstyrelsen. Retrieved January 11, 2018, from: https://www.digst.dk/informationssikkerhed/Implementering-af-ISO27001/Implementering-af-ISO27001/Hvad-er-ISO27001.

Duffield, M. (2012). Challenging environments: Danger, resilience and the aid industry. *Security Dialogue*, *43*(5), 475–492. DOI: https://doi.org/10.1177/0967010612457975

Dunn-Cavelty, M., & **Suter, M.** (2009). Public-Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, *2*(1), 179–187. DOI: https://doi.org/10.1016/j.ijcip.2009.08.006

EU. (2008). RÅDETS DIREKTIV 2008/114/EF af 8. december 2008 om indkredsning og udpegning af europæisk kritisk infrastruktur og vurdering af behovet for at beskytte den bedre EU. Retrieved from: http://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32008L0114&from=DA.

Europa Parlamentet. (2016). EU NIS Direktiv (Europa Parlamentets og Rådets Direktiv (EU) 2016/1148). Retrieved from: http://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32016L1148&from=EN.

Finland Security Committee. (2015). Secure Finland – Information on comprehensive security in Finland. Helsinki. Retrieved from: https://www.turvallisuuskomitea.fi/index.php/en/component/k2/47-secure-finland-information-on-comprehensive-security-in-finland.

Finland Security Committee. (2017). Implementation Programme for Finland's Cyber Security Strategy. Helsinki. Retrieved from: https://www.turvallisuuskomitea.fi/index.php/en/component/k2/132-implementation-programme-for-finland-s-cyber-security-strategy-for-2017-2020.

Forsvarets Efterretningstjeneste. (2017). Efterretningsmaessig Risikovurdering 2017. København. Retrieved from: https://fe-ddis.dk/SiteCollectionDocuments/FE/EfterretningsmaessigeRisikovurderinger/Risikovurdering2017.pdf.

Forsvarskommissionen. (1997). Fremtidens forsvar. København. Retrieved from: http://www.fmn.dk/videnom/Documents/Forsvarskommissionen-af-1997-Hovedbind-beretning.pdf.

Forsvarsministeriet. (1992). Beredskabsloven, Pub. L. No. LOV nr 1054 af 23/12/1992. Retrieved from: https://www.retsinformation.dk/Forms/R0710.aspx?id=52845.

Forsvarsministeriet. (2016). Samarbejde på cybersikkerhedsområdet. Retrieved September 5, 2017, from: http://www.fmn.dk/temaer/cybersikkerhed/Pages/Samarbejde-paa-cybersikkerhedsomraadet.aspx.

Forsvarsministeriet. (n.d.). Regeringen styrker indsatsen mod cybertrusler. Retrieved September 5, 2017, from: http://www.fmn.dk/nyheder/Pages/regeringen-styrker-indsatsen-mod-cybertrusler.aspx.

FSOR. (2017). Test af kriseberedskab gennemført med succes. Retrieved from: http://www.nationalbanken.dk/da/finansielstabilitet/Documents/FSOR_test af kriseberedskab.pdf.

Hansen, S. L. (2017). Nordisk samarbejde i finanssektoren styrker kampen mod cyberkriminalitet. Retrieved January 11, 2018, from: http://finansdanmark.dk/nyheder/2017/nordisk-samarbejde-i-finanssektoren-styrker-kampen-mod-cyberkriminalitet/.

Jensen, M. S. (2017a). Cyberstrategi – spørgsmål til politikerne. København.

Jensen, M. S. (2017b). Interview i Finland SEP og NOV 2017.

Jensen, M. S. (2017c). Interview med Beredskabsstyrelsen 27.11.2017.

Jensen, M. S. (2017d). Interview med Center for Cybersikkerhed 01.11.2017.

Jensen, M. S. (2017e). Interview med Digitaliseringsstyrelsen 24.11.2017. København.

Jensen, M. S. (2017f). Interview med Forsvarsministeriet JUN–NOV 2017. København.

Jensen, M. S. (2017g). Interview med Janne Kuusela, Director General, Defence Policy, MOD Finland 2.11.2017. København.

Jensen, M. S. (2017h). Interview med Rådet for Digital Sikkerhed 20.12.2017.

Kerttunen, M. (2018). Email from M. Kerttunen 25.1.18.

Lauta, K. C., Hoffmann, R., & **Struwe, L. B.** (2013). Cyberwarfares udfordringer af begrebet kritisk infrastruktur. Retrieved from: http://curis.ku.dk/ws/files/66128849/Cyberwarfare.pdf.

Makasiinikatu, E. (2013). Finland's Cyber Security Strategy. Helsinki. Retrieved from: https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf.

Ministerie van Justitie en Veiligheid. (2010). 2de inhoudelijke analyse bescherming vitale infrastructuur. Retrieved from: https://www.nctv.nl/binaries/bijl-1-2010-2e-inhoudelijke-analyse-bescherming-vitale-infrastructuur_tcm31-32507.pdf.

Ministeriet for Videnskab Teknologi og Udvikling. (2010). 2010/1 LSF 197 Forslag til Lov om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v. København: Folketinget. Retrieved from: https://www.retsinformation.dk/pdfPrint.aspx?id=136359.

Nye, J. S., Jr. (2016). Deterrence and Dissuasion in Cyberspace. *International Security*, *41*(3), 44–71. DOI: https://doi.org/10.1162/ISEC_a_00266

Pogson Smith, W. G. (1965). HOBBES'S LEVIATHAN REPRINTED FROM THE EDITION OF 1651 WITH AN ESSAY BY THE LATE (1st ed.). Oxford: Clarenden Press. Retrieved from: http://files.libertyfund.org/files/869/0161_Bk.pdf.

Regeringen. (2014). National strategi for cyber- og informationssikkerhed – Øget professionalisering og mere viden, December 2014. København. Retrieved from: http://www.fmn.dk/nyheder/Documents/National-strategi-for-cyber-og-informationssikkerhed.pdf.

Regeringen. (2016a). FOR ET FRIERE, RIGERE OG MERE TRYGT DANMARK. Regeringsgrundlaget. Copenhagen. Retrieved from: http://www.stm.dk/multimedia/Regeringsgrundlag2016.pdf.

Regeringen. (2016b). Kommissorium for det tværministerielle arbejde med den nationale strategi for cyber- og informationssikkerhed 2017–2019. Copenhagen: The Danish Government. Retrieved from: http://www.fmn.dk/nyheder/Documents/Kommissorium.pdf.

Swedish Civil Contingencies Agency (MSB). (2014). Action Plan for the Protection of Vital Societal Functions and Critical Infrastructure. Retrieved from: https://www.msb.se/RibData/Filer/pdf/27412.pdf.

The National Emergency Supply Agency – Huoltovarmuuskeskus. (n.d.). The National Emergency Supply Agency. Retrieved January 24, 2018, from: https://www.nesa.fi/organisation/the-national-emergency-supply-agency/.

Turvallisuuskomitea. (n.d.). What is the Security Committee? Retrieved January 11, 2018, from: https://www.turvallisuuskomitea.fi/index.php/en/.

U.S. Chamber of Commerce. (2018). Critical Infrastructure Protection, Information Sharing and Cyber Security. Retrieved January 8, 2018, from: https://www.uschamber.com/issue-brief/critical-infrastructure-protection-information-sharing-and-cyber-security.

Van Der Meer, S. (2013). Appendix 2. Deterrence as a security concept against cyber threats. *General Intelligence and Security Service*, *2*, 4–7. Retrieved from: https://www.clingendael.org/pub/2015/clingendael_monitor_2015_en/2_deterrence_as_a_security_concept_against_non_traditional_threats/pdf/appendix_2_cyber.pdf.

Von Solms, R., & **Van Niekerk, J.** (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102. DOI: https://doi.org/10.1016/j.cose.2013.04.004

Walker, J., & **Cooper, M.** (2011). Genealogies of resilience: From systems ecology to the political economy of crisis adaptation. *Security Dialogue*, *14*(2), 1–29. DOI: https://doi.org/10.1177/0967010611399616

Zahran, M. M. (1998). Role of science and technology in the context of security, disarmament and other related fields. Report of the First Committee. New York. Retrieved from: https://digitallibrary.un.org/record/264457/files/A_53_576-EN.pdf.

How to cite this article: Jensen, M. S. (2018). Sector Responsibility or Sector Task? New Cyber Strategy Occasion for Rethinking the Danish Sector Responsibility Principle. *Scandinavian Journal of Military Studies,* 1(1), pp. 1–18, DOI: https://doi.org/10.31374/sjms.3

Submitted: 26 January 2018 **Accepted:** 28 May 2018 **Published:** 11 July 2018