ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Denmark's Sector Responsibility Principle: A Tedious Cyber Resilience Strategy

Mikkel Storm Jensen | Royal Danish Defence College, Copenhagen, Denmark | ORCID: 0000-0003-3995-3020

Abstract

In 2014, Denmark launched its first national strategy for cyber resilience of critical infrastructure (CI). The 'National Cyber and Information Security Strategy' and its two subsequent successors from 2018 and 2022 follow the Sector Responsibility Principle (SRP). According to the principle, the state distributes the task of achieving and maintaining societal resilience to individual sectors, for example, health, energy supply, or finance, while maintaining central oversight and responsibility for implementation. Denmark is not alone in taking this approach: in fact, all the Nordic countries have applied some version of SRP. Danish governments have over the last decade taken significant steps to implement and facilitate societal cyber resilience through development of institutions, strategies, legal measures, and public-private partnerships (PPP). That said, Danish governments have gone less far than, for example, Finland's to take measures to achieve efficacy, and significant weaknesses are still left to be addressed. The article outlines the principles behind SRP and, using mainly Danish examples, demonstrates why implementation of SRP is both legally, organisationally, and technically difficult but also politically 'unpleasant'. Resilience is desirable but also a tedious chore. An inherent risk with SRP at both strategic, political level and individual private or public entity level are incentives to strive for legal compliance, rather than operational efficacy and act more according to a 'sector responsibility avoidance principle'. In that light, the article outlines how the SRP has been implemented in Denmark so far, along with examples

Received: 09.10.2023

Accepted: 10.04.2024

Published: 05.07.2024

Cite this article as:
M.S. Jensen, "Denmark's sector responsibility principle: A tedious cyber resilience strategy," ACIG, vol. 4, no. 2, 2024, DOI: 10.60097/ACIG/189870

Corresponding author:
Mikkel Storm Jensen, Royal Danish Defence College, Denmark; E-mail: msje@fak.dk
0000-0003-3995-3020

Copyright:
Some rights reserved (CC-BY):
Mikkel Storm Jensen
Publisher NASK

OPEN ACCESS

of both what drives the effort and challenges to successful SRP implementation.

Keywords
cyber, strategy, resilience, sector responsibility principle

1. Introduction

Danish governments have over the last decade taken significant steps to implement and facilitate societal cyber resilience through the development of institutions, strategies, legal measures, and public-private partnerships (PPP).[1] Denmark is not alone in taking this approach: in fact, all the Nordic countries have applied some version of Sector Responsibility Principle (SRP) [1]. In 2014, Denmark launched its first national strategy for achieving cyber resilience of critical infrastructure (CI). The 'National Cyber and Information Security Strategy' [2] and its two subsequent successors from 2018 [3] and 2021 [4] follow SRP. According to the principle, the state distributes the task of achieving and maintaining societal resilience to individual sectors, for example, health, energy supply, or finance, while maintaining central oversight and responsibility for implementation. However, Danish governments have gone less far than, for example, Finland's to ensure the efficacy of the implemented strategies. According to North Atlantic Treaty Organization's (NATO) 2020 evaluation, weaknesses in governance of resilience measures are still left to be addressed [5, p. 5]. This raises the question: why Denmark has not gone as far as Finland?

The literature on societal resilience strategies explains the sound principles behind SRP. This article seeks to add nuances to this body of literature by looking at the Danish case with an eye to identify incentives against implementing SRP with efficacy, rather than formal compliance as the main goal at both macro and micro levels.

After a literature review, the article outlines the principles behind SRP and demonstrates why it is a good strategic approach for states to achieve cyber resilience in modern, digitalised, and diverse economies. Methodologically, the article demonstrates why implementation of SRP in practice is not only legally, organisationally, and technically very difficult but also politically 'unpleasant' using mainly Danish examples. Denmark is a relevant case for studying potential weaknesses in cyber resilience strategies, as it is a highly digitalised society that has consistently scored high in international evaluations of national cybersecurity, although its position has

1——While the author is a serving officer with the Danish armed forces, the statements in this article are his own and do not present the position of the Danish Defence or the Danish Government.

fallen since ITU's initial evaluation in 2015 [6, 7]. The article takes its outset in the, so far, three Danish national information and cybersecurity strategies as well as the accompanying European Union (EU) NIS and NIS 2 directives. This presents methodological challenges: there are no formal definitions of a strategy, but according to, for instance Yarger and Bartholomees' [8] strategies should include political ends and explicit theories of success regarding assumed causalities between allocated means and appropriate ways. This allows observers to identify, assess, and discuss risks, for example, from potentially inadequate means or questionable ways and evaluate the theory of success' internal causality or compare with the result of other strategies in similar empirical contexts. Held to Yarger and Bartholomees' standards, the Danish strategies are lacking in content. Particularly the 2021 strategy [4] is mainly a list of aspirational ends, while ways and particularly allocated means are not specified in detail. This constitutes an analytical weakness, as the lack of explicit ways and means leaves a large amount to the external observer's interpretation. Even so, the approach gives indications as to where weaknesses may lay in the presented strategies, illustrated anecdotally with empirical observations from resilience-related events as they appear in reputable news sources or other reporting.

To governments as well as their citizens and enterprises, resilience is desirable but also a tedious chore that takes away resources from core services. An inherent risk with the SRP at both the strategic, political level and the individual private or public entity level is incentive to strive for legal compliance rather than operational efficacy and act more according to a 'sector responsibility avoidance principle'. Having discussed this in principle, the article will outline how the SRP has been implemented in Denmark so far, along with examples of both what drives the effort and challenges to successful SRP implementation.

2. Cyber resilience strategy – a new academic field

The article's headline includes the three concepts of 'strategy', 'cyber resilience', and 'sector responsibility principle', which the present literature goes some way to define. As mentioned above, Yarger and Bartholomees provide an operational definition of strategy as a formulated theory of success on how ends are achieved by applying sufficient means in particular ways. Furthermore, Yarger and Bartholomees provide a framework for describing the level at which strategies are developed and implemented. In the present

case, the investigated Danish strategies are at what Yarger and Bartholomees define as the 'National Security Strategy' level, as the means deployed include all aspects of the national instruments of power [8, pp. 48–49]. National cyber resilience strategies can encompass a number of relevant topics: building a cyber-workforce, promoting public cyber literacy, etc. This article focuses on the state's task of protecting critical infrastructure, particularly its role in developing and implementing strategy in the shape of institutions and regulations and how PPP is enforced, encouraged, and facilitated. Here, Tiirma-Klaar provides an overview of the areas that states may include in cyber resilience strategies [9]. Cyber resilience as such, particularly at the tactical level as the concept applies to individual entities and organisations, is described from many perspectives, and for instance, Sepúlveda Estay et al. provide oversight of relevant literature [10]. A search for 'sector responsibility principle' on Google Scholar, however, provides only Jensen [11] in spite of the principle's widespread use in Scandinavia [1].

Identifying the state's objective to be 'resilience' rather than 'security' is an acknowledgement of a governing principle, where the state is more a gardener guiding and facilitating a complex society's ability to withstand, overcome, and emerge stronger from external blows, than an engineer trying to keep external blows from affecting the societal machine or assist in repairing it afterwards. The emergence and history of this approach are well described by, for instance, Walker and Cooper [12]. This principle and the state's role therein is brilliantly described by Dunn-Cavelty and Suter in their article 'Public-private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection' [13]. In this key piece, they describe how the strategic context for national resilience strategies has changed, particularly since the end of the Cold War. Modern economies used to be complicated, but some factors made it possible for the state to manage crisis through collection and analysis of information and central allocation of resources through commands, economic incentives, or patriotic encouragement [14, p. 2]. Critical infrastructure (CI) within, for example, production or communications was state-owned or run by domestic industries and based on standard communications systems like telephone, mail, order books, etc. This allowed a state to conduct 'business continuity management' (BCM) at a national level for extended periods. The world wars provided excellent examples of such state-run economies with 'PPP' based on central control [12, p. 3; 15]. But during the 1990s, many Western economies changed: state-run critical infrastructure was sold to private entities and these along with other domestic industries

often became international, either due to ownership or based on outsourcing from national or foreign subcontractors, always prone to change. At the same time, digitisation meant that command and control within critical infrastructure became based on innumerable and ever-changing systems [13, p. 180]. These and other changes transformed the basic structure of modern economies from complicated to complex, and made the hitherto successful central control approach to crisis management impractical [16, p. 46]. In the modern context the state's role is not to manage through direct intervention. The state's principal challenge is to create a framework that ensures – and facilitates – the individual sectors' resilience within critical infrastructure [13, pp. 183–186]. Only in the individual sectors are the necessary insights to identify, implement, and maintain resilience and overcome external blows [17]. Hence, the state must delegate the tasks involved to achieve resilience [18, p. 36; 19, p. 481]. Christensen and Lund-Petersen elaborate on the cyber aspects of PPP and resilience in 'Public-private partnerships on cyber security: A practice of loyalty' [20].

Dunn-Cavelty and Suter's analysis of meta-governance of self-organising networks identifies the state's tasks, thus: (1) define and communicating goals and priorities, (2) identify *status quo* and needs for action, (3) choose instruments, and (4) verify efficiency – and go to step 2 again [13, p. 185]. In practice, this means that to conduct meta-governance, a state should identify, designate, and keep track of CI, divided into sectors according to tasks to facilitate the emergence of networks. Also, it should set strategic objectives, for instance, through contracts, that sectors or individual suppliers must fulfil. Furthermore, set and enforce minimum standards, for example, ISO 27001 compliance, for cyber resilience in CI. And finally, it is important to facilitate PPP, for instance, by providing threat intelligence, promoting best practices, or improving access to reports and prosecuting cybercrime.

It is important to note that delegating the tasks does not mean delegating the responsibility: comprehensive security, including BCM of the nation's critical infrastructure, remains the state's responsibility towards its citizens even if the actual infrastructure involved has been sold to a private contractor [18, p. 37]. Furthermore, it is important to note that except for the financial sector, market forces are often insufficient to incentivise individual entities in CI, whether public or private, to achieve the levels of resilience that would be sufficient from a societal perspective [11, p. 5; 21, p. 266]. And, again it must be reiterated that the task of developing and implementing the necessary strategies is simple in principle, but

very difficult in practice and hampered by strong incentives that can lead to sub-optimisation at both strategic and individual levels. Dr. Kerttunen, who took part in developing Finland's comprehensive cyber resilience strategy, has expressed it thus:

> What is the best strategy? It is relevant, optimized, updated, and implemented! There are three categories of states when it comes to cyber strategies: those without strategies, those with utopian strategies that cannot be implemented, and those with realistic strategies that are poorly implemented [1, p. 275; 22].

In Denmark, SRP is the guiding principle for resilience, including cyber resilience. This is stated by law and entails that the authority or institution, for instance ministry, who has the day-to-day responsibility for a task, also has the responsibility for planning, and resolving this task in a crisis [23, 24]. The fact that Denmark is now implementing its third cyber resilience strategy and has achieved some results, with its two predecessors placing Denmark in the third category of Dr. Kerttunen's conceptual framework. The next section elaborates on the strengths and weaknesses of the Danish approach.

3. Denmark's cyber resilience strategies

Since 2001, Denmark has had national strategies for the public sector's, citizens', and corporations' use of the cyber domain [25]. In 2014, the first national strategy for cyber and information security was introduced. It had set basic objectives, for instance, requiring ISO27001 implemented in government entities as well as some other concrete measures in identified CI in the telecommunications and energy sectors. Furthermore, it provided guidance to the newly established national Computer Emergency Response Team (CERT), Centre for Cyber Security (CFCS) under the Danish Defence Intelligence Service, and National Cyber Crime Centre (NC3) under the police, and initiated a program of information collection to establish *status quo* and identify major weaknesses [2]. The first strategy thus followed the model for meta-governance quite closely. The plan was to build on the results of this strategy with the introduction of a more extensive strategy in 2017. Developments were also driven forward by the introduction of the EU's Directive 2016/1148 concerning measures for a high common level of security of network and information systems – in daily terms, the NIS directive, which Denmark as an EU member was obliged to implement [26].

However, the initial plan did not hold. In 2016, the Ministry of Defence was tasked with developing a new strategy, and relevant ministries were ordered to participate in the process. However, after repeated delays, the government transferred the task to the Ministry of Finance. Likely, the lack of progress was due to the fact that efforts to develop individual ministries' contributions to the strategy had to compete with the ministries' core functions and were not given priority. In Denmark, the Ministry of Defence has no means to influence the quality and scale of other ministries' efforts. Also, while the Ministry of Defence was responsible for the cross-ministerial coordination, it was not provided extra funding with which to facilitate its progress. The Ministry of Finance has significantly more influence on other ministries through the power of the purse and a new strategy was eventually presented by an entity established under the ministry for the purpose, Digitaliseringsstyrelsen ('the Board for Digitization') in 2018 [3; 11, p. 10]. While Denmark has no official definitions of what constitutes CI, the commission for the strategy included designated sectors within which entities could be designated as CI, namely energy, health, transport, telecommunications, finance, and maritime transport. This was supplemented by the criteria for CI designation of the EU's NIS directive [3, pp. 38–40; 20, p. 3; 26, 27]. The 2018 strategy included both concrete initiatives to increase CI resilience but also initiatives to facilitate PPP. Part of the strategy was that each of the designated sectors should develop individual resilience strategies, a process that was completed by the end of 2018 [28]. Furthermore, the strategy introduced a central entity (a 'styregruppe' or 'control group') and an accompanying reporting framework with the task of staying informed on how the implementation progressed in individual sectors and facilitating the sharing of, for instance, best practice between sectors [3, pp. 43–45]. Like its predecessor, the 2018 strategy follows the recommendations of meta-governance by building on the information collected after the first strategy was implemented and focusing on concrete initiatives with stated deadlines to establish and facilitate the individual sector's ability to improve resilience, including PPP.

In December 2021, Digitaliseringsstyrelsen presented Denmark's current strategy [4]. Compared with its two predecessors, it is less concrete: more describing intents and ambitions than stating objectives and setting deadlines [21, p. 261]. The 2021 strategy outlines a continuation and expansion of the previous strategies, for example, by the establishment of decentralised cyber and information security entities (DCIS). It also expands the state's practical facilitation of individual citizen's and enterprise's cyber resilience, for example, by establishing a new hotline for identity

theft, strengthening the police's capability to prosecute cybercrime, and a special entity dealing with the cyber security challenges for small- and medium-sized enterprises (SMEs) that make up a significant part of the Danish economy [4, pp. 11, 14]. As such, the strategy continues to follow the principles of meta-governance, but its less concrete form and more aspirational formulations make it less immediately applicable. There is an underlying and accompanying set of documents that much more explicitly outlines the implementation of the strategy to the individual sector; however, while formally unclassified, these are not accessible to the public.

According to the strategy's preamble, the plan is to follow up with a new strategy in 2024. In this regard, it is interesting to observe what role Digitaliseringsstyrelsen, which has been leading the process since 2017, play. In December 2022, Digitaliseringsstyrelsen was removed from the Ministry of Finance's portfolio and formally made an independent ministry. However, a ministry is responsible for two diverse areas: digital governance and equal gender rights [29]. Recalling the Ministry of Defence's difficulties in moving the development of the second strategy forward in 2017, the new Ministry of Digital Governance and Gender Rights may experience similar challenges regarding a 2024 strategy.

4. Challenges to Denmark's implementation of SRP and cyber resilience

Recalling Dr. Kerttunnen's quip about national cyber resilience strategies, at this point it is relevant to review what the principle challenges are to Denmark's implementation of its cyber resilience strategies through the SRP doctrine, and consider how they manifest themselves.

Initially, it must be fully acknowledged that developing, implementing, and maintaining national cyber resilience strategies is always going to be an extremely difficult task legally, economically, technically, organisationally, etc. Hence, the following sections are in no way intended as condescending vis-à-vis the attempts that are done. Furthermore, realising that the tasks involved are truly daunting, the analysis does not address these difficulties, but instead address the challenges presented by incentives for complacency at both political-strategic and individual level.

The nature of these challenges is perhaps best illustrated with an example from the United States: In May 2021, Colonial Pipeline, a private enterprise that delivers fuel to most of the US east coast,

was paralysed as a result of a ransomware attack conducted by Russian cybercriminals. As a result, fuel supplies immediately dropped by 45%. Seventeen states had to declare a state of emergency that in some areas lasted for weeks as transportation of persons and goods came to a halt. Forensics later assessed that the ransomware attack had been possible because Colonial Pipeline lacked basic cyber security measures in place [30–32]. What went wrong? Was the enterprise not designated as CI? Was there no resilience strategy in place? Was Colonial Pipeline not in compliance with regulations? It turned out that strategy was in place, and the enterprise was designated as CI complying its rules and regulations. However, those rules were basically that Colonial Pipeline should read the government's – here TSA's – recommendations, and then follow those if felt inclined to. Colonial had read the recommendations, and were thus in compliance. But it was not inclined not to follow them, hence they had no effect. The rules have now been changed [31, 33].

How could such an in hindsight obviously inefficient approach to cyber resilience be developed and implemented? There are four good reasons at play: (1) Designating CI is politically unpleasant; (2) requiring and upholding demands for CI is politically unpleasant; (3) having updated and detailed insight into CI's cyber resilience or lack thereof is politically unpleasant; and (4) paying for cyber resilience is generally unpleasant (for an extensive elaboration of these arguments, see Jensen [11, 34]). To go through these four drivers that incentivise neglect of resilience measures, cyber or otherwise, let us review them individually.

Designating CI is unpleasant: When the state designates a private or public entity as CI, it either implicitly or explicitly imposes some demands regarding resilience measures that non-CI entities are not subjected to. This imposes extra costs for the CI-designated entity that has to be covered either by adding to the price of the provided services or compensated in some manner. Hence, there is an economic incentive against designating infrastructure as CI that may counterbalance operational considerations.

In the Danish case, it may be difficult to demonstrate this challenge with regard to cyber resilience, but a look at Denmark's interpretation of EU's directive No. 2008/114/EF may illustrate how relevant decision makers may be reluctant to designate infrastructure as CI. The EU directive defines 'European critical infrastructure' or 'ECI' as 'critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at

least two Member States' [35, p. L345/77]. In Denmark's case, one could expect, for example, bridges across the straits, transnational power and internet cables, or Copenhagen Airport (CPH), the largest in Scandinavia, to be designated as ECI. However, as of 2022, no Danish infrastructure was ECI. Why? Because there are substitutes in principle if less so in reality: for instance if the bridge to Sweden breaks down, there is a ferry. From an operational perspective, this may make little sense and probably goes against the spirit behind the EU directive. However, this is how the ministries for transport and energy interpret the letter of the directive when they biannually report 'no ECI in Denmark' to Brussels. Thus, Denmark is in compliance with the directive but IT has no effect if the EU's intent IS to strengthen ECI's resilience [21, p. 263]. That said, compliance with the EU's NIS directive and the recently updated version, NIS 2 has been and will continue to be a very important driver of the implementation of cyber resilience measures in Denmark [26, 36]. In February 2024, the Danish Ministry of Defence stated that the implementation of NIS 2 in Denmark was delayed, but it is still expected to be in place in 2024 [37].

Requiring and upholding standards for CI is unpleasant: Not only do these demands add costs to the provided service as described above, but the demanding entity, here the government, also has to allocate resources to enforce and keep track of their implementation, a further draw on resources.

In this regard, the nature of the sector also plays a role. Within the governance sector, implementing resilience requirements should in principle be a question of issuing commands and expecting the entities to follow orders. However, in 2014, as part of Denmark's initial strategy, government agencies were ordered to implement the ISO 27001 standard by the end of 2016. Even so, by December 2022 only two-thirds had done so in spite of 'a high degree of attention from leaders on the task' [4, pp. 19–20; 38]. Hence, implementation of even relatively simple resilience requirements is not unproblematic even within the government and likely also not in other public sectors, for instance, health. In the financial sector, market forces drive cyber resilience and security in advance of governmental requirements. In the telecommunications and energy sector, the involved enterprises are private but highly concentrated to a few large entities that are very capable technically regarding cyber security and resilience which enables sparring on relevant requirements and their implementation between these entities and the government. The transport sector, on the other hand, is similarly

composed of private enterprises, but many are SMEs that often have little or no skills when it comes to cyber and their IT systems and potential vulnerabilities are very diverse.

Insight into status of resilience is unpleasant: Knowing that cyber resilience in CI is sub-par entails a political responsibility to react. Not knowing provides 'credible deniability' and the SRP can become 'a sector responsibility avoidance principle' if political leadership in case of incidents due to lack of resilience can get away with the excuse that according to SRP, it is the sector's and even individual entity's task to ensure sufficient resilience.

As mentioned, the Danish 2018 strategy put a framework in place for CI sectors to report to a central entity on progress on the implementation of resilience measures and share best practices [3, p. 45]. However, the framework does not set specific formats or timelines for reporting. Occasional interviews with entities involved in the process suggest that while such reporting takes place, it is with uneven intervals and in different formats across different CI sectors. The lack of central oversight and the accompanying lack of resilience measures enforcement in Denmark in even very critical CI were recently demonstrated in a highly critical report from 'Rigsrevisionen', the Danish Parliament's special investigations board. It states the following:

> The cyber security resilience of the 13 critical IT systems selected for this study is not satisfactory. The resilience of one of the authorities, where Rigsrevisionen examined several IT systems, is particularly unsatisfactory. The consequence of inadequate cyber security resilience is that critical services provided by the public sector risk being either seriously disrupted or impossible to deliver. It should be noted that the level of cyber security resilience varies between the authorities in the study [39, p. 3].

This suggests that the Danish strategies do not go as far to gain insight into the status of cyber resilience as they could. For comparison, in Finland, the government has gone considerably further: they identified the problems presented by uneven reporting in 2015, and since 2017, Finnish CI sectors have reported monthly to the government's national security committee in a fixed format involving a 22-point matrix. This committee, established in 2013, conducts monthly meetings and submits an annual report to the president [40, 41].

Exacerbating the lack of central awareness, there is no overall authority tasked with coordinating the individual sector's planning and preparation between incidents [20, p. 1435]. Denmark's designated crisis management organisation only come together in extraordinary situations and only temporarily have the authority to deal with the effects of a crisis [23]. The tasks of coordinating individual sector's planning and preparation is delegated according to the SRP. But, as the example with implementation of ISO 27001 demonstrates, even under SRP, giving an order to implement resilience measures does not mean it is carried out – even within the public sector. With SRP's decentralised responsibility for the implementation of the upcoming cyber strategy follows that individual ministries must interpret what their responsibility entails [34]. At the same time, the ministries evaluate themselves when assessing whether their respective sectors live up to their interpretation of their responsibility. This introduces significant risk that the sectors do not have a shared understanding of their tasks and that they do not give them the same priority – a fact also noted above by Rigsrevisionen. Biannual national exercises since 2006 have consistently been highlighting this in their 'Conclusions' [42, p. 5; 43, p. 6].

Paying for resilience is unpleasant: Under most circumstances, cyber resilience is not the core business for neither public nor private entities. Hence, resilience measures take away human and capital resources from whatever that core business is. In public service sectors, for example, health, the societally optimal level of resilience is in no way influenced by market forces, and hence arbitrarily set by political leadership. In private sectors, market forces have some influence, but the economically optimal dedication of resources to resilience may be far less from an individual enterprise's perspective than from the general society if the failure of that enterprise results in significant costs, as second-order effects of its failure ripple through the economy. Consider, for example, a small de-icing company that is critical for the function of a major airport in winter. Their revenue, and hence market incentive to ensure BCM, comes nowhere near the cost to society if aircraft cannot take off on a winter day due to a cyberattack. Historically, only in the Danish financial sector, market forces have been sufficient to drive cyber resilience to a very high level [44]. In the case of public sector, the political level can decide how much resources are taken from other tasks and dedicated to resilience, but who and how should the difference between the general society's and the small airport enterprise's incentive to invest in resilience be covered?

Recent research indicates that cyber security and resilience are often not a high priority in Denmark's many SMEs. In some cases, this is because implementation appears economically and/or technically challenging. In other cases, the task is too far from the experience and expertise of SMEs' leadership to rise to a sufficient level of attention to result in taking action [45, 46]. Since the introduction of the first national Danish strategy in 2014, Danish governments have primarily placed funding for implementation on the defence budget [47, p. 13; 48, p. 11]. This is in light of the magnitude of the task likely insufficient to cover the actual costs in all sectors. For instance, the Confederation of Danish Industry (Dansk Industri, DI) that promotes the interests of the SME sector assessed it as unlikely that the allocated 270 mio. DKK were sufficient to cover the 34 initiatives presented in the 2021 strategy [4, p. 5; 49].

5. The SRP is the right principle for Danish cyber resilience, but demonstrated political priority does not fully match stated ambitions

As the examples of this article have demonstrated, the state's role in establishing and maintaining comprehensive cyber resilience in CI is both highly complex and fraught with political and economic incentives to give the task less priority than a purely operational perspective might recommend. The Russian full-scale invasion of Ukraine in February 2022 has accentuated the need for resilience and the state's role in that regard. Denmark's national CERT has, along with other Western intelligence services, warned about an increased risk of Russian 'hactivism', and Danish banks, airports, ministries, and other CI have been the target for Russian distributed denial-of-service (DDOS) attacks [50–55].

The Danish strategies have, since 2014, along with EU's NIS directives, established a framework for solving the task. The strategies have, like in the rest of Scandinavia, built on SRP and contain the elements necessary to replace the state's role as 'the societal engineer' of the past with 'the societal gardener' of today and tomorrow. Governments from both sides of the parliament have built on their predecessors' strategies to establish institutions and frameworks to, for instance, identify and designate CI, assess the level of resilience, provide threat warning, and facilitate PPP. Also, the latest strategy's focus on SME opened a new and important area for implementing measures for cyber resilience.

However, as demonstrated by the examples, the implemented policies have still been insufficient to overcome incentives to give the

task less than the necessary priority, even within the public sectors, as demonstrated by the limited progress of ISO27001 implementation and the serious deficiencies in CI systems identified by Rigsrevisionen. SRP is the proper tool for the task, but the inherent threat from implementing it as the 'sector responsibility avoidance principle' has yet to be overcome – a challenge that Denmark shares with all Nordic countries that apply SRP [1, p. 274]. Ambitious headlines in the current and coming strategies do not decide the outcome. Only the government's will and tenacity actually implement resilience measures through oversight, control, facilitation, guidance, and resource allocation.

References

[1] M.S. Jensen, "Cyberresiliens, sektorprincip og ansvarsplacering – nordiske erfaringer," *Internasjonal Politikk*, vol. 77, no. 3, pp. 266–277, 2019, doi: 10.23865/INTPOL.V77.1369.

[2] Regeringen. (Dec. 2014). *National strategi for cyber-og informationssikkerhed – Øget professionalisering og mere viden*. København. [Online]. Available: http://www.fmn.dk/nyheder/Documents/National-strategi-for-cyber-og-informationssikkerhed.pdf. [Accessed: Aug. 19, 2020].

[3] Finansministeriet. (2018). *National strategi for cyber-og informationssikkerhed*, Finansministeriet. [Online]. Available: http://www.fmn.dk/nyheder/Documents/National-strategi-for-cyber-og-informationssikkerhed-2018.pdf. [Accessed: Aug. 19, 2020].

[4] Regeringen. (Dec. 2021). *The Danish National Strategy for Cyber and Information Security*, Regeringen. [Online]. Available: https://www.cfcs.dk/globalassets/cfcs/dokumenter/2022/ncis_2022-2024_en.pdf. [Accessed: Jan. 8, 2023].

[5] North Atlantic Treaty Organization (NATO). (2020). *NATO Defence Planning Capability Review 2019/2020 Denmark C-M (2020) 0026 (DK-Overview)*, NATO. [Online]. Available: https://www.fmn.dk/globalassets/fmn/dokumenter/aarsrapporter/nato/-nato-defence-planning-capability-review-2019-2020-.pdf. [Accessed: Feb. 6, 2023].

[6] UN International Telecommunication Union (ITU). (2015). *Global Cybersecurity Index 2014*, ITU, Geneva. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf. [Accessed: Feb. 29, 2024].

[7] UN International Telecommunication Union (ITU). (2021). *Global Cybersecurity Index 2020*, ITU, Geneva. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf. [Accessed: Feb. 29, 2024].

[8] H.R. Yarger, J.B. Bartholomees, "Toward a Theory of Strategy: Art Lykke and the U.S. Army War College Strategy Model," Strategic Studies Institute, US Army War College, 2012. [Online]. Available: https://www.jstor.org/stable/resrep12116.6. [Accessed: Jan. 13, 2021].

[9] H. Tiirmaa-Klaar, "Building national cyber resilience and protecting critical information infrastructure," *Journal of Cyber Policy*, vol. 1, no. 1, pp. 94–106, 2016, doi: 10.1080/23738871.2016.1165716.

[10] D.A. Sepúlveda Estay, R. Sahay, M. B. Barfod, C.D. Jensen, "A systematic review of cyber-resilience assessment frameworks," *Computers & Security*, vol. 97, p. 101996, 2020, doi: 10.1016/j.cose.2020.101996.

[11] M.S. Jensen, "Sector responsibility or sector task? New cyber strategy occasion for rethinking the Danish sector responsibility principle," *Scandinavian Journal of Military Studies*, vol. 1, no. 1, pp. 1–18, 2018, doi: 10.31374/sjms.3.

[12] J. Walker, M. Cooper, "Genealogies of resilience: From systems ecology to the political economy of crisis adaptation," *Security Dialogue*, vol. 42, no. 2, pp. 143–160, 2011.

[13] M. Dunn-Cavelty, M. Suter, "Public-private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection," *International Journal of Critical Infrastructure Protection*, vol. 2, no. 4, pp. 179–187, 2009, doi: 10.1016/j.ijcip.2009.08.006.

[14] K.C. Lauta, R. Hoffmann, L.B. Struwe, "Cyberwarfares Udfordringer af Begrebet Kritisk Infrastruktur," Københavns Universitet, Center for Militære Studier, Copenhagen, 2013. [Online]. Available: http://curis.ku.dk/ws/files/66128849/Cyberwarfare.pdf. [Accessed: Aug. 19, 2020].

[15] S. Broadberry, M. Harrison, "The economics of World War I: An overview," in *The Economics of World War I*, M. Harrison and S. Broadberry, Eds., Cambridge University Press, Cambridge, 2005, pp. 3–40, doi: 10.1017/CBO9780511497339.002.

[16] M. Carr, "Public-private partnerships in national cyber-security strategies," *International Affairs*, vol. 92, no. 1, pp. 43–62, 2016, doi: 10.1111/1468-2346.12504.

[17] J. Brassett, N. Vaughan-Williams, "The politics of resilience from a practitioner's perspective: An interview with Helen Braithwaite OBE," *Politics*, vol. 33, no. 4, pp. 229–239, 2013, doi: 10.1111/1467-9256.12027.

[18] J. Brassett, N. Vaughan-Williams, "Security and the performative politics of resilience: Critical infrastructure protection and humanitarian emergency preparedness," *Security Dialogue*, vol. 46, no. 1, pp. 32–50, 2015, doi: 10.1177/0967010614555943.

[19] M. Duffield, "Challenging environments: Danger, resilience and the aid industry," *Security Dialogue*, vol. 43, no. 5, pp. 475–492, 2012, doi: 10.1177/0967010612457975.

[20] K.K. Christensen, K.L. Petersen, "Public-private partnerships on cyber security: A practice of loyalty," *International Affairs*, vol. 93, no. 6, pp. 1435–1452, 2017, doi: 10.1093/ia/iix189.

[21] M.S. Jensen, "Cyberresiliens og kritisk infrastruktur: Vanskelige udfordringer og trælse løsninger," in *Cybertrusler: Det Digitale Samfunds Skyggeside,* Jeppe T. Jacobsen and Tobias Liebetrau, Eds., Djøf Forlag (Jurist og Økonomforbundets Forlag), Copenhagen, 2022.

[22] M. Kerttunen, Lecture at George C. Marshall European Center for Security Studies, Garmisch-Partenkirchen, Germany, Dec. 06, 2021.

[23] Beredskabsstyrelsen (BRS). (2022). *Krisestyringssystemet i Danmark*, Beredskabsstyrelsen. [Online]. Available: https://www.brs.dk/da/arbejdsopgaver/om-krisestyring-og-redningsberedskabet/krisestyringssystemet-i-danmark/. [Accessed: Apr. 22, 2022].

[24] Forsvarsministeriet. (2017). Bekendtgørelse af beredskabsloven, vol. LBK nr 314 af 03/04/2017. Forsvarsministeriet. [Online]. Available: https://www.retsinformation.dk/eli/lta/2017/314. [Accessed: Sep. 29, 2021].

[25] Digitaliseringsstyrelsen. (2023). *The Danish Digital Journey*, Digitaliseringsstyrelsen. [Online]. Available: https://en.digst.dk/policy/the-danish-digital-journey/. [Accessed: Aug. 17, 2023].

[26] European Union (EU). (2016). *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 — Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union*, European Parliament. [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN. [Accessed: May 13, 2018].

[27] Forsvarsministeriet, "Kommisorium for the tværministerielle arbejde med den nationale strategi for cyber-og informationssikkerhed 2017–2019," Danish Ministry of Defence, København (Copenhagen), 2016.

[28] Forsvarsministeriet. (2019). *Nye sektorstrategier skal ruste samfundet mod cyberangreb*, Forsvarsministeriet. [Online]. Available: https://fmn.dk/da/nyheder/2019/2019/nye-sektorstrategier-skal-ruste-samfundet-mod-cyberangreb/. [Accessed: Sep. 30, 2021].

[29] Ministry of Digital Governance and Gender Rights. (2023). *Ministry of digital governance and gender rights*, DIGMN. [Online]. Available: https://english.digmin.dk/. [Accessed: Aug. 17, 2023].

[30] D.E. Sanger, N. Perlroth, "Colonial pipeline hack reveals weaknesses in US cybersecurity," *The New York Times*, 2021. [Online]. Available: https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html?referringSource=articleShare. [Accessed: May 17, 2021].

[31] W. Turton, K. Mehrota, "Hackers breached colonial pipeline using compromised password," Bloomberg.com, Jun. 04, 2021. [Online]. Available: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password. [Accessed: Sep. 29, 2021].

[32] D. Uberti, "TSA pipeline oversight faces scrutiny after colonial hack," *Wall Street Journal*, May 13, 2021. [Online]. Available: https://www.wsj.com/articles/tsa-pipeline-oversight-faces-scrutiny-after-colonial-hack-11620898202. [Accessed: Sep. 29, 2021].

[33] Republican Policy Committee (RPC). (2021). *Infrastructure cybersecurity pipelines*, RPC. [Online]. Available: https://www.rpc.senate.gov/policy-papers/infrastructure-cybersecurity-pipelines. [Accessed: Jan. 6, 2022].

[34] M.S. Jensen. (Nov. 1, 2017). Author's interview with Center for Cyber Security.

[35] European Union (EU). (2008). *Raadets 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. [Online]. Available: http://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=CELEX:32008L0114&from=DA. [Accessed: Mar. 9, 2017].

[36] European Union (EU). (Dec. 14, 2022) *Directive (EU) 2022/2555 of the European parliament and of the council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No. 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive),*

European Parliament. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1692616271604. [Accessed: Aug. 21, 2023].

[37] Center for Cyber Security (CFCS). (2024). *Nye regler om cybersikkerhed bliver forsinkede*, Forsvarsministeriet. [Online]. Available: https://www.fmn.dk/da/nyheder/2024/nye-regler-om-cybersikkerhed-bliver-forsinkede/. [Accessed: Mar. 21, 2024].

[38] Digitaliseringsstyrelsen. (2017). *Resultatet af undersøgelse af status paa implementering af ISO27001-principper i staten*, Digitaliseringsstyrelsen, København. [Online]. Available: https://digst.dk/media/16012/resultat-for-staten-2017.pdf. [Accessed: Apr. 9, 2018].

[39] Rigsrevisionen. (2022). *Report on the cyber security resilience of the public sector*, Folketinget, Rigsrevisionen. [Online]. Available: https://uk.rigsrevisionen.dk/audits-reports-archive/2022/nov/report-on-the-cyber-security-resilience-of-the-public-sector. [Accessed: Aug. 21, 2023].

[40] Turvallisuuskomitea. (2017). *Implementation programme for Finland's cyber security strategy*, Security Committee Finland Ministry of Defence, Helsinki. [Online]. Available: https://www.turvallisuuskomitea.fi/index.php/en/component/k2/132-implementation-programme-for-finland-s-cyber-security-strategy-for-2017-2020. [Accessed: Sep. 22, 2018].

[41] Finland Security Committee. (2015). *Secure Finland – Information on comprehensive security in Finland, Helsinki*, Finland Security Committee. [Online]. Available: https://www.turvallisuuskomitea.fi/index.php/en/component/k2/47-secure-finland-information-on-comprehensive-security-in-finland. [Accessed: Apr. 4, 2017].

[42] Beredskabsstyrelsen (BRS). (2017). *Evaluering af krisoev 2017*, Beredskabsstyrelsen. [Online]. Available: https://www.brs.dk/globalassets/brs---beredskabsstyrelsen/dokumenter/krisestyring-og-beredskabsplanlagning/2020/-evaluering-af-krisoev-2017-.pdf. [Accessed: May 26, 2022].

[43] Beredskabsstyrelsen (BRS). (2016). *Evaluering af KRISØV 2015*, BRS. [Online]. Available: https://www.brs.dk/globalassets/brs---beredskabsstyrelsen/dokumenter/krisestyring-og-beredskabsplanlagning/2020/-evaluering_af_krisoev_2015-.pdf. [Accessed: Jan. 06, 2022].

[44] S. Goll. (2022). *Nordisk samarbejde i finanssektoren styrker kampen mod cyberkriminalitet*, Finans Danmark. [Online]. Available: https://finansdanmark.dk/nyheder/2017/nordisk-samarbejde-i-finanssektoren-styrker-kampen-mod-cyberkriminalitet/. [Accessed: Jan. 6, 2022].

[45] V. Arildsen. (2021). *Ny rapport: Cybersikkerhed er underprioriteret i danske virksomheder*, UN International Telecommunication Union (ITU). [Online]. Available: http://itu.dk/Om-ITU/Presse/Nyheder/2021/Ny-rapport-cybersikkerhed-er-underprioriteret-i-danske-virksomheder. [Accessed: Jan. 06, 2022].

[46] O. Kulyk, J. Mauro. (Dec. 2020). *Assessment on the status of cybersecurity in Denmark*, SDU, Odense, Dec. [Online]. Available: https://ascd.dk/results/report.pdf. [Accessed: Jan. 06, 2022].

[47] T. Bramsen. (2021). *Et styrket dansk cyberforsvar*, Forsvarsministeriet. [Online]. Available: https://fmn.dk/globalassets/fmn/dokumenter/nyheder/2021/-et-styrket-dansk-cyberforsvar-2021-ua-.pdf. [Accessed: Jul. 15, 2021].

[48] Regeringen. (Jan. 28, 2018). *Forsvarsforlig 2018*, Regeringen. [Online]. Available: https://www.regeringen.dk/nyheder/2018/forsvarsforlig-2018/. [Accessed: Jan. 29, 2021].

[49] J.Ø. Wittorff. (2021). *Erhvervsorganisationer alvorligt bekymret over Danmarks nye cyber-strategi: Det er ikke nok*, Computerworld. [Online]. Available: https://www.computerworld.dk/art/259045/erhvervsorganisationer-alvorligt-bekymret-over-danmarks-nye-cyber-strategi-det-er-ikke-nok. [Accessed: Jan. 06, 2022].

[50] L. Friis. (2022). *Københavns Lufthavn advarer efter flere russiske hackerangreb: Vi har en galoperende cyberrisiko*, Berlingske.dk. [Online]. Available: https://www.berlingske.dk/content/item/1688115. [Accessed: Aug. 21, 2023].

[51] E.K. Stephensen. (2023). *Forsvarsministeriet udsat for cyberangreb – TV 2*, nyheder.tv2.dk. [Online]. Available: https://nyheder.tv2.dk/samfund/2023-05-12-forsvarsministeriet-udsat-for-cyberangreb. [Accessed: Aug. 21, 2023].

[52] I. Meesenburg. (2023). *Finansministeriet ramt af cyberangreb*, DR. [Online]. Available: https://www.dr.dk/nyheder/seneste/finansministeriet-ramt-af-cyberangreb. [Accessed: Aug. 21, 2023].

[53] M. Mezouri. (2023). *Prorussisk hackergruppe står bag angreb mod danske banker, siger it-sikkerhedsekspert og Danske Bank – TV 2*, nyheder.tv2.dk. [Online]. Available: https://nyheder.tv2.dk/tech/2023-01-10-prorussisk-hackergruppe-staar-bag-angreb-mod-danske-banker-siger-it. [Accessed: Aug. 21, 2023].

[54] Center for Cybersikkerhed (CFCS). (2022). *Cybertruslen mod Danmark i lyset af Ruslands invasion af Ukraine*, CFCS. [Online]. Available: https://www.cfcs.dk/da/cybertruslen/trusselsvurderinger/ruslands-invasion-af-ukraine/. [Accessed: Apr. 19, 2022].

[55] Cybersecurity & Infrastructure Security Agency (CISA). (2022). *Russian state-sponsored and criminal cyber threats to critical infrastructure*, CISA.gov. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa22-110a. [Accessed: Jun. 18, 2022].