Fagfellevurdert

Internasjonal POLITIKK
Skandinavisk tidsskrift for Internasjonale Studier

Årgang 77, Nummer 3, side 266-277, 2019, ISSN 1891-1757, www.tidsskriftet-ip.no, Publisert september 2019

Fokus: Cybersikkerhet

Cyberresiliens, sektorprincip og ansvarsplacering – nordiske erfaringer

Mikkel Storm Jensen
Institut for Strategi, Forsvarsakademiet, Danmark

Sammenfatning

Siden 2003 har regeringerne i Norge, Danmark, Sverige, Finland og Island arbejdet med at udvikle og implementere nationale strategier for cyber- og informationssikkerhed. Strategierne omfatter mange forskellige områder; f.eks. institutionel kapacitetsopbygning, uddannelses- og forsvarspolitik, internationalt samarbejde etc. Denne artikel skitserer landenes forskellige strategier per august 2018[1] for statens rolle i samfundets cyberresiliens, dvs. de kritiske samfundsfunktioners evne til at modstå og overkomme negative effekter af hændelser med udspring i cyberdomænet. Endvidere skitserer artiklen de udfordringer, som regeringerne har konstateret, at opgavefordeling og ansvarsplacering har givet, samt hvordan implementeringerne af strategierne reflekterer disse erkendelser. Her har den finske regering vist sig mest konsekvent ved at placere ansvaret for implementeringen af cyberresiliens centralt i en magtfuld organisation og udstyre den med konkrete styringsredskaber og en stor, velintegreret kontaktflade til den private del af Finlands kritiske infrastruktur.

Nøgleord: cyber · resiliens · cyberforsvar · beredskab · offentligt-privat samarbejde · regeringsførelse · sektoransvar

[1] Artiklen blev opdateret i maj 2019, fordi Norge i januar 2019 lancerede en ny cyberstrategi, og Danmark samtidig implementerede individuelle cybersikkerhedsstrategier for seks sektorer med kritisk infrastruktur.

*Kontaktforfatter: Mikkel Storm Jensen, e-post: msje@fak.dk

Citation: Mikkel Storm Jensen (2019). Cyberresiliens, sektorprincip og ansvarsplacering – nordiske erfaringer. Internasjonal Politikk, 77(3): 266–277. http://dx.doi.org/10.23865/intpol.v77.1369

Indledning

De nordiske lande er alle digitaliserede i høj grad. Staterne har derfor en opgave i at opretholde samfundets cyberresiliens (her forstået som kritiske samfundsfunktioners evne til at modstå og overkomme negative effekter af uventede hændelser med udspring i cyberdomænet). Men staternes direkte kontrol over samfundet er begrænset. De løser opgaven i privat-offentlige samarbejder under anvendelse af sektoransvarsprincippet. (Christensen & Lund Petersen, 2017; Jensen, 2018). Erfaringerne fra alle de nordiske lande er, at det er en stor udfordring at implementere sektoransvarsprincippet effektivt på cyberområdet, og at staterne behøver klarere opgavefordeling og ansvarsplacering for at styrke landenes cyberresiliens.

Denne korte artikel giver først baggrunden for, at de nordiske lande i deres strategier for statens rolle i samfundets cyberresiliens har taget udgangspunkt i sektoransvarsprincippet. Derefter skitserer artiklen for hvert af landene hvilke udfordringer, administrationen af sektoransvarsprincippet gennem opgavefordeling og ansvarsplacering har givet, og hvordan landenes strategiimplementering reflekterer disse erkendelser. Artiklen konkluderer, at den finske regering er gået længst i sine bestræbelser på at overkomme udfordringerne.

Artiklen bygger på gennemlæsning af de nordiske landes cyber- og informationssikkerhedsstrategier, en del af de forudgående nationale rapporter samt nationale evalueringer af landenes beredskab i forhold til hændelser i cyberdomænet. Hertil kommer interviews med danske og finske embedsmænd i efteråret 2017. Da strategierne og de tilknyttede tiltag er i stadig udvikling, er der tale om et øjebliksbillede af situationen, som den fremstod i august 2018.

Hvorfor Basere Cyberstrategier På Sektoransvar?

Alle de nordiske landes cyberresiliensstrategier tager udgangspunkt i sektoransvarsprincippet, og det er der gode grunde til. Siden Hobbes' Leviathan udkom i 1651, har der været sat ord på statens kerneleverance i forhold til borgerne: Sikkerhed for liv og ejendom mod trusler til lands, til vands og i luften (DSB, 2016, p. 9; Pogson Smith, 1965, p. 133). Udviklingen af internettet har tilføjet behovet for at beskytte borgerne mod effekterne af krig, konflikt, kriminalitet og naturkatastrofer med udspring i cyberdomænet. De nordiske landes cyberresiliensstrategier er derfor supplementer til staternes øvrige resiliensstrategier.

Op gennem det 20. århundrede udviklede de nordiske lande resiliensstrategier under overskrifter som "Beredskab" eller "Totalforsvar", hvor staterne gennem komplicerede, men planlagte kommandoveje kunne tage direkte kontrol med kritiske dele af samfundsøkonomierne i tilfælde af krise eller krig. Da den kolde krig sluttede i 1989, og den umiddelbare krigstrussel faldt markant, faldt også den politiske opmærksomhed omkring disse beredskabsstrukturer stærkt. De nordiske lande, undtagen Finland, reducerede fra begyndelsen af 1990'erne deres beredskab og totalforsvar betydeligt (Lindgren & Ödlund, 2015). Samtidig indførte de som

andre vestlige stater new public management og privatiserede statslige virksomheder i deres kritiske infrastruktur (Dunn-Cavelty & Suter, 2009, p. 180). Globalisering og privatisering af kritisk infrastruktur havde en positiv effekt på omkostninger og effektivitet, men gjorde det samtidig vanskeligere for regeringerne at levere sikkerhed og håndtere kriser, fordi de godt kunne udlicitere de samfundskritiske opgaver, men ikke ansvaret for, at de blev udført (Arvidsson et al., 2016, p. 5; Brassett & Vaughan-Williams, 2015, p. 37; Dunn-Cavelty & Suter, 2009, p. 184; Ullring et al., 2006, p. 44). Udviklingerne medførte, at staten havde stadig mindre direkte kontrol med de involverede aktører og derfor måtte søge nye måder at sikre samfundets modstandsdygtighed på (Carr, 2016, p. 46; Dahlberg, 2015, p. 548). Terrorangrebet 11. september 2001 vækkede interessen for beredskab igen, og efterhånden som negative hændelser med udspring i cyberdomænet manifesterede sig, blev fokus udvidet fra håndtering af terrortrusler til cybertrusler. Samfundenes stigende kompleksitet gjorde samtidig, at overvejelserne kom til at handle om det emergerende begreb "resiliens". Hvor det 20. århundredes beredskabstankegang så samfundet som en kompliceret maskine, der kunne styres og repareres udefra, er resilienstankegangen en dynamisk, selvregulerende tilgang inspireret af økologien. Den ser samfundet som en kompleks organisme, der kan reparere sig selv (Brassett & Vaughan-Williams, 2015, p. 36; Dahlberg, 2015, p. 546; Duffield, 2012, p. 481).Processerne og den litteratur, de affødte, er beskrevet dybtgående i "Resilience and (in)security: Practices, subjects, temporalities" (Cavelty, Kaufmann, & Kristensen, 2015).

I moderne, komplekse, digitaliserede samfund som de nordiske kan staten altså ikke længere detailstyre via kommandoveje i tilfælde af krise. Det betyder i praksis, at en stor del af opgaverne med at sikre resiliens – også på cyberområdet – må lægges ud i samfundets forskellige sektorer, fordi kun sektorerne har den nødvendige og opdaterede detailviden om deres egen situation. Derfor er sektoransvarsprincippet blevet udgangspunkt for alle de nordiske landes cyberresiliensstrategier. Princippet betyder, at den myndighed, virksomhed eller institution, som til daglig har ansvaret for et område, også har ansvaret for kriseplanlægning og opretholdelse af funktionerne under en krise (Beredskabsstyrelsen, 2006, p. 22). Dunn-Cavelty og Suter argumenterer for, hvordan sektorerne med den rette kombination af organisation og incitamenter kan fungere som selvorganiserende netværk, der kan bidrage til samfundets resiliens. Statens rolle bliver at skabe rammerne for, at alle involverede aktører i det omfattende privat-offentlige samarbejde har forudsætningerne for, og incitament til, at reagere optimalt på kriser (Dunn-Cavelty & Suter, 2009; Jensen, 2018). Fordelen ved sektoransvarsprincippet er altså, at opgaven med beredskab og resiliens skal løses ude i sektorerne, hvor informationsniveauet om lokale forhold er højest. Hvad er ulemperne så?

Ved at decentralisere opgaverne med samfundets resiliens gennem sektoransvarsprincippet bliver det bl.a. uklart

- hvad der er kritisk infrastruktur og derfor skal sikres ekstraordinært
- hvor højt et beredskab der er optimalt

- hvordan omkostninger til resiliens skal fordeles
- hvem der er ansvarlig for, at opgaverne bliver løst.

På det politisk-strategiske niveau kan uklarhederne friste politiske beslutningstagere på valg til at løbe en uhensigtsmæssigt stor risiko ved at nedprioritere ressourcer til beredskabsforanstaltninger, inklusive cyberresiliens. Det er lettere at demonstrere for borgerne, at man træffer beslutninger, som kommer dem til gode, ved at afsætte ressourcer til infrastruktur, velfærd, skattelettelser og andre håndgribelige forhold end ved at afsætte ressourcer til resiliens. De samfundsmæssige gevinster ved resiliens vil først manifestere sig, hvis der opstår en krise – en krise, der måske netop aldrig bliver rigtig alvorlig, hvis det ramte område er blevet tilstrækkeligt resilient på grund af investeringerne (Jensen, 2018). Og hvis det går galt, kan ansvaret placeres ude i sektorerne langt væk fra de politikere, der ikke afsatte tilstrækkelige ressourcer.

Ude i sektorerne er udfordringen, at beredskabsopgaverne ikke er sektorernes eller de individuelle aktørers kerneproduktion. Alt andet lige vil ekstra omkostninger til resiliens skulle tages fra kerneproduktionen eller fra virksomhedens overskud. Dermed vil de have en tendens til at få mindre opmærksomhed og ressourcer, end hvad der er optimalt – især hvis det ikke er en parameter, de ansvarlige chefer bliver målt på. I Danmark evaluerede Digitaliseringsstyrelsen statens implementering af ISO27001 i 2017 og fandt, at selv om myndighederne generelt havde ledelsesmæssigt fokus på området, havde 43% alligevel ikke planer for sikkerhedsaktiviteter, angiveligt fordi området ikke blev prioriteret højt nok til at få ressourcer (Digitaliseringsstyrelsen, 2017, p. 9). Et eksempel fra den private sektor er A. P. Møller-Maersks håndtering af cyberresiliens inden NotPetya-angrebet i 2017, der kostede virksomheden mindst 300.000.000 dollars. Indtil angrebet blev opgaverne med cyberresiliens angiveligt nedprioriteret, fordi de ikke indgik direkte i evalueringen af chefer (Greenberg, 2018).

I det følgende gennemgås de nordiske landes cyberresiliensstrategier med fokus på de udfordringer, som ansvarsplacering under sektoransvarsprincippet giver.

Norge

Den nuværende nationale strategi for informationssikkerhed fra 2019 er Norges tredje (Norwegian Ministry of Justice and Public Security, 2019). Den bygger videre på Norges anden strategi fra december 2012, der blev udarbejdet efter en række omfattende offentliggjorte analyser (f.eks. Ullring et al., 2006) i årene 2000–2012 af informationsteknologis rolle i det norske samfunds sårbarhed. Analyserne foregik på baggrund af erfaringerne fra Norges første strategi, som kom allerede i 2003. I 2003-strategien erkendte regeringen de mange forestående vanskeligheder med at udvikle standarder, placere ansvar etc.

2012-strategien omfattede nogle konkrete tværsektorielle koordinationstiltag, f.eks. etableringen af Udvalget for National Koordinering af Arbejdet med IT-sikkerhed, men var generelt mere en oversigt over identificerede udfordringer

og principper for at overkomme disse. (Regjeringen, 2003, p. 12). I 2012 viste en evaluering af statens implementering af et af de konkrete tiltag, ISO27001, stærkt varierende niveauer, og at mange ledere først reagerede efter udefrakommende kontrol og påtale af de mangelfulde tiltag (DIFI, 2012, p. 39). Den norske rigsrevision påpegede ligeledes svagheder og mangel på systematik i den hidtidige forvaltning, så styrket samordning og fælles situationsforståelse blev i 2012-strategien rykket op som det øverste overordnede mål i de strategiske prioriteter, efterfulgt af styrkelse af den kritiske infrastrukturs resiliens.

I 2012-strategien blev det overordnede ansvar for koordinering og opfølgning pålagt Justits- og Beredskabsministeriet (Departementene, 2012). På trods af den høje prioritet som ledelse, koordination og infrastruktur fik i 2012-strategien, har Norge fortsat udfordringer på området. En rapport fra 2014 konkluderede, at ledere i staten nedprioriterer cyberresiliens, fordi opgaven stjæler tid fra de opgaver, de bliver målt på. Dertil kommer, at fejl og mangler sjældent får konsekvenser (Elgsaas & Schultz Heireng, 2014, pp. 66–68). I 2016 påpegede en analyse, at manglen på overordnet national organisering af cybersikkerhed og en uklar rollefordeling mellem myndighederne internt og mellem offentlige og private aktører fortsat var tydelig, at myndighederne samarbejdede på ad hoc basis, og at cybersikkerheden i de private virksomheder var dimensioneret af interne lønsomhedshensyn (Muller, 2016, pp. 17–18). Samtidig har Nasjonal sikerhetsmyndighet (NSM) i sine årlige evalueringer af cyberrelaterede sikkerhedsforhold løbende påpeget, at ledelsen i for mange offentlige og private virksomheder prioriterer IT-sikkerhed for lavt, og at det har negative konsekvenser for Norges cyberresiliens (f.eks. Nasjonal Sikkerhetsmyndighet, 2018, p. 10).

I den nylancerede 2019-strategi er det fortsat de enkelte sektorers eget ansvar at opnå et tilfredsstillende niveau af cyberresiliens. Justits- og Beredskabsministeriet har ansvar for den overordnede koordination (Norwegian Ministry of Justice and Public Security, 2019, p. 22). Det fremgår ikke tydeligt af strategien, hvilke skridt Norge har taget for at overkomme de erkendte udfordringer med ansvarsplacering i forbindelse med implementeringen.

Finland

Finland lancerede sin cybersikkerhedsstrategi i 2013. I Finland er nationalt beredskab, inklusive cyberresiliens, meget højt prioriteret politisk. Den finske fortolkning af sektoransvarsprincippet kan måske bedst beskrives som "sektoropgaveprincippet": Opgaverne ligger i sektorerne, men ansvaret er centraliseret i regeringens nationale sikkerhedskomité, der på baggrund af løbende vurderinger af trusselsbilledet udarbejder regeringens strategiske mål og derpå fordeler opgaverne med at opfylde dem til de respektive sektorer (Finland Security Committee, 2015; Jensen, 2017d). Alligevel måtte man efter 2013-cyberstrategien erkende, at det på trods af massiv politisk velvilje var vanskeligt at implementere den ensartet og koordineret

på tværs af sektorerne. Sikkerhedskomiteen udviklede derfor i 2017 en fælles liste på 22 punkter, ud fra hvilken de forskellige sektorers fremgang kunne evalueres (Jensen, 2017b; Turvallisuuskomitea, 2017). De centralt formulerede målepunkter gør det lettere for sektorerne at fokusere deres implementering og argumentere for, at cyberresiliens skal prioriteres i forhold til andre (kerne)produktioner. Samtidig gør centraliseringen af ansvaret det muligt for regeringen at fordele implementerings- og driftsomkostningerne mellem sektorerne (Jensen, 2017d). Når det gælder privat-offentligt samarbejde, har Finland en organisatorisk veludbygget model: Det finske Kontor For Forsyningssikkerhed har løbende kontakt med over 1500 private virksomheder, der er udpeget som kritisk infrastruktur. Kommunikationen går begge veje, og virksomhederne holder myndighederne opdateret om tekniske udviklinger og ændringer i forhold, der kan påvirke tværsektorielle afhængigheder (Jensen, 2017c).

Traditionelt har privat-offentligt samarbejde i beredskabssammenhæng i Finland i betydeligt omfang bygget på frivillighed og virksomhedernes patriotisme. Frivillighed er stadig et vigtigt element, men omkostningerne til beredskab bliver mere synlige og er stigende. Mange private aktører er ikke længere nationalt ejede, og både private og offentlige virksomheder opererer på markedsvilkår i konkurrence med internationale aktører. Derfor kan beredskab ikke længere indarbejdes automatisk (og dermed som skjult omkostning), men skal indarbejdes kontraktuelt. Herved træder de reelle omkostninger tydeligere frem. Det forhold har dog ikke ændret på den brede politiske opbakning til at opretholde et højt niveau (Jensen, 2017a).

I Finland fortsætter arbejdet med at udvikle statens rolle i samfundets cyberresiliens. En evaluering af landets cybersikkerhed fra 2017 identificerede potentielle svagheder, som manglende koordination på cyberforsvarsområdet fortsat kan medføre. Rapporten anbefalede blandt andet forbedringer af den strategiske ledelse (Lehto et al., 2017, p. 4). Som eksempel på mulig yderligere centralisering af ansvaret, overvejer regeringen at koncentrere Finlands cyberforsvar under en fælles kommando (O'Dwyer, 2018).

Danmark

Danmark fik sin første nationale cyber- og informationssikkerhedsstrategi i 2014. Strategien indeholdt generelle hensigtserklæringer, men omfattede primært konkrete aktiviteter, såsom etablering af de nødvendige institutioner under Forsvaret og politiet til at imødegå cybertrusler, implementering af informationssikkerhedsstandarden ISO27001 i hele staten samt tiltag til at forbedre beskyttelsen af kritisk infrastruktur, særligt i energi- og telesektoren (Forsvarsministeriet, 2014, p. 15). Strategien blev afløst af en ny og mere omfattende strategi i maj 2018, som det endnu er for tidligt at vurdere effekterne af.

Det er en udfordring, at Danmark endnu mangler en fælles institutionel forståelse og forankring af sektoransvaret samt endnu ikke har et centralt overblik over, hvad der udgør kritisk infrastruktur (Christensen & Lund Petersen, 2017, p. 3). Prioritering af beredskabsopgaver var et problem, allerede inden cyber kom til, og i dag er der stadig forskellige modenhedsniveauer af cyberresiliens i statens forskellige sektorer. Det er sandsynligt, at tværministerielt samarbejde hæmmedes af, at ministerierne prioriterede deres kerneaktiviteter højere end cyberresiliens og at det medvirkede til, at opgaven med at udarbejde en ny strategi først udkom med over et års forsinkelse (Jensen, 2018). Manglende fælles forståelse og prioritering præger også det offentligt-private samarbejde: Ifølge Rådet for Digital Sikkerhed forudser mange private virksomheder en videreførelse på cyberområdet af de svagheder, der historisk har været ved at implementere beredskab gennem sektoransvar. Den private sektor ser endvidere en uafklaret opgave i, hvordan omkostningerne til implementering af cyberresiliens skal fordeles mellem det offentlige og virksomhederne, samt det forhold, at sektorerne – bortset fra Forsvaret, der har fået ca. 200 mio. EUR (Forligspartierne, 2018) – ikke er tildelt ekstra midler til etablering og drift af statens cybersikkerhedsstrategier. Endvidere er der kun begrænset direkte og formaliseret vidensdeling og koordination mellem private aktører og staten på cyberområdet. Finanssektoren er af egen drift gået hurtigere frem på cybersikkerheds- og resiliensområdet end nødvendigt i forhold til lovgivningen, sandsynligvis på baggrund af økonomiske overvejelser om konsekvenserne af manglende cybersikkerhed (Jensen, 2018). Det er dog usandsynligt, at markedsmekanismer af sig selv kan trække cybersikkerheden op på et samfundsmæssigt optimalt niveau hos mange andre private aktører i den kritiske infrastruktur (NISU, 2015, p. 52).

Danmark fik i foråret 2018 en ny strategi, der erkendte problemerne med koordination og implementering og opstillede konkrete modtræk. Bl.a. skulle det tværsektorielle overblik forbedres ved at oprette et døgnbemandet cybersituationscenter og en oversigt over kritisk IT-infrastruktur. Tværsektoriel koordination søgtes forbedret ved at oprette en national styregruppe for cyber- og informationssikkerhed samt sektorenheder for seks udpegede samfundskritiske sektorer og ved at foretage jævnlige tilstandsmålinger på området. De seks sektorer (sundheds-, finans-, tele-, søfarts-, transport- og energisektoren) offentliggjorde i januar 2019 individuelle strategier for at nå de pålagte mål (Forsvarsministeriet, 2019). I det privat-offentlige samarbejde skal kontakten til borgere og virksomheder være lettere, bl.a. forenkles adgangen til at anmelde cyberangreb (Regeringen, 2018, pp. 24, 25, 37, 41, 44). Tiltagene vil alt andet lige forbedre den tværgående kommunikation og det offentligt-private samarbejde. Det er endnu for tidligt at vurdere effekten, men de første uformelle tilbagemeldinger er positive. Henset til de hidtidige erfaringer og det forhold, at kun Forsvaret er blevet tildelt ekstra midler til opgaven, er det dog sandsynligt, at de enkelte sektorer fortsat vil have svært ved at prioritere cyberresiliens i forhold til deres kerneopgaver (Jensen, 2018).

Island

Islands nationale cybersikkerhedsstrategi er fra 2015. Når det gælder statens rolle i beskyttelsen af kritisk infrastruktur, tager strategien udgangspunkt i, at myndighederne har ansvaret for planlægning og indøvelse af beredskab (Altinget, 2008). Strategien lægger dog op til et omfattende offentligt-privat samarbejde. Forud for lanceringen deltog repræsentanter for ca. 60 private og offentlige institutioner i høringsmøder, hvilket er et betydeligt antal, når man tager Islands befolknings størrelse i betragtning (Ministry of the Interior, 2015, p. 4).

Island offentliggjorde i 2017 en omfattende evaluering af implementeringen. Beskyttelsen af kritisk infrastruktur mod cyberhændelser er stadig på et meget lavt niveau, bl.a. på grund af manglende koordination og vidensdeling. F.eks. har politiet udarbejdet en liste over kritisk infrastruktur, men den er ikke sendt ud til de involverede aktører, der derfor savner formaliserede og indøvede kommunikationsveje. Endvidere har de enkelte identificerede aktører i Islands kritiske infrastruktur implementeret varierende grader af cybersikkerhedskapacitet, men der er ingen nationalt fastsatte standarder. Islands finansielle institutioner er dog gået videre, end lovgivningen på området kræver og har selvstændigt opbygget en betydelig resiliens. Islands evne til krisestyring under cyberhændelser vurderes som endnu meget begrænset. Bl.a. fordi de gennemførte øvelser ikke involverer alle relevante deltagere, f.eks. sundhedssektoren. Det var dog i 2017 forventningen, at sundhedssektoren fremover vil blive inddraget (Global Cyber Security Capacity Centre, 2017, pp. 23–25).

Sverige

Arbejdet med at sikre Sveriges cyberresiliens foregår i disse år som et vigtigt element i en større indsats fra regeringen for at genetablere den svenske stats muligheder for at forbedre samfundets beredskab og resiliens. Efter den kolde krig blev mange krise- og beredskabsorganisationer afviklet og nedlagt, og i en årrække blev beredskab lavt prioriteret af politikere og myndigheder. Denne udvikling er efterhånden vendt. Bl.a. på grund af en stigende bekymring for hybride trusler, herunder cyberangreb (Lindgren & Ödlund, 2015), men også ud fra en generel erkendelse af de sårbarheder, som digitaliseringen af samfundet har medført (Forsvarsdepartementet, 2013, p. 36). Myndigheden for Samfundsbeskyttelse og Beredskab (MSB) blev etableret i 2009 ("Myndigheten för samhällsskydd och beredskap – Krisinformation.se," 2009) og spiller en nøglerolle i Sveriges totalforsvar, herunder koordination og evaluering af beredskabet (MSB, 2016, p. 5).

Den svenske regering iværksatte i 2013 et omfattende udredningsarbejde for at identificere kravene til en national strategi for informations- og cybersikkerhed. Udredningen identificerede på bagrund af erkendte mangler inden for kontrol og kvalitet af statslig IT-sikkerhed, at der var behov for en central, tværsektoriel styringsmodel (NISU, 2015, pp. 213, 232–233). På baggrund af arbejdet lancerede

regeringen i 2017 en national strategi for samfundets informations- og cybersikkerhed (Justitiedepartementet, 2017, pp. 4, 20).

Strategien indeholder ikke mange konkrete tiltag, men har til formål at opstille strategiske retningslinjer og mål for fremtidig lovgivning og administration på området. Strategien erkender i sit første kapitel, at Sveriges nuværende cyberresiliens ikke er tilfredsstillende, og placerer en systematisk og samlet indsats som sin øverste prioritet, med et afledt krav om tydelig ansvarsplacering og tilsyn (Justitiedepartementet, 2017, pp. 5, 8, 9, 12).

Den svenske strategi har kun været på plads i et år, og det er derfor for tidligt at vurdere dens effekt. MSB er dog klar i sin beskrivelse af udfordringerne i sin årlige rapport om det nationale beredskab fra 2018: Der savnes tilstrækkelig tydelighed i ansvars- og ledelsesstrukturen for kriseberedskabet, hvilket medfører forskellige modenhedsgrader og gør samfundet mere sårbart. MSB ser endvidere et behov for at styrke tilsynet med cybersikkerhed og betegner det privat-offentlige samarbejde på området som værende "hverken tilstrækkelig vel udviklet eller effektivt" (Myndigheten för samhällsskydd och beredskap (MSB), 2018, pp. 5–6).

Sammenfatning Og Konklusion

Den begrænsede plads i denne artikel levner ikke rum til nuancer og udelader mange væsentlige detaljer. Der er for eksempel ikke gjort forsøg på at måle objektivt og sammenligne, hvor cyberresiliente de nordiske lande er (Hassel, 2016). Alligevel viser den kortfattede oversigt, at de nordiske lande har sammenlignelige erfaringer med udfordringerne i at udvikle statens rolle i opbygningen af samfundenes cyberesiliens og med at fordele opgaverne og placere ansvaret helt konkret, når sektoransvarsprincipperne skal administreres i praksis. Regeringernes problemer forstærkes af, at opgaverne med (og ikke mindst udgifterne til) cyberresiliens konkurrerer med sektorernes primære opgaver, hvad enten aktørerne er private eller offentlige. Sekundære opgaver vil helt naturligt altid have svært ved at opnå høj prioritet, og kun i finanssektoren har markedskræfterne været i stand til at trække cybersikkerhed helt frem i første række.

Siden lanceringen af strategierne har alle landene konstateret, at hvis cyberresiliens skal styrkes, er der behov for dels at tydeliggøre ansvars- og opgaveplacering, dels at implementere styringsmekanismer i form af overvågnings- og rapporteringsmetoder med henblik på, at centrale tværsektorielle institutioner kan evaluere status og niveau for cyberresiliens i de enkelte sektorer. Hensigterne om at tydeliggøre ansvarsfordelingen fremgår af alle strategierne, og alle landene har taget større eller mindre skridt i retning af at forbedre overblik og tværsektorielt samarbejde.

De nordiske landes erkendelser af udfordringerne er dog endnu kun i begrænset omfang blevet omsat til konkret administration og lovgivning. Denne artikel har skitseret mulige teoretiske årsager til de begrænsede fremskridt på både det

politisk-strategiske niveau og for de enkelte beslutningstagere i sektorerne, men en reel afdækning vil kræve yderligere forskning. Men på nuværende tidspunkt er Finland gået markant længere end de øvrige nordiske lande for at skabe klarhed over ansvar og opgaver. Finland har placeret ansvaret helt centralt i en magtfuld organisation, som har direkte indflydelse på sektorernes budgetter og beslutninger, opbygget et omfattende formelt og integreret netværk i den private del af Finlands kritiske infrastruktur og implementeret et konkret styringsredskab i form af et rapporteringssystem ud fra de 22 fælles målepunkter.

Om forfatteren

Mikkel Storm Jensen er major og Cand. Polit. Han har siden 2016 forsket i cyberstrategi på Institut for Strategi ved Forsvarsakademiet og er netop begyndt på et PhD projekt om småstater, alliancer og cybervåben.

Referencer

Altinget. 82/2008: Lög um almannavarnir | Lög | Alþingi, Pub. L. No. 2008 nr. 82 12. júní (2008). Altinget. Retrieved from https://www.althingi.is/lagas/nuna/2008082.html

Arvidsson, B., Cedergren, A., Falkheimer, J., Guldåker, N., Hassel, H., Johansson, J., … Tehler, H. (2016). Att skydda samhällsviktig verksamhet. *CenCIP Professional Papers*, *1*, 1–6. Retrieved from https://www.cencip.lu.se/sites/cencip.lu.se/files/nr1_-_att_skydda_samhallsviktig_verksamhet.pdf

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

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. 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

Cavelty, M. D., Kaufmann, M., & Kristensen, K. S. (2015). Resilience and (in)security: Practices, subjects, temporalities. *Security Dialogue*, *46*(1), 3–14. https://doi.org/10.1177/0967010614559637

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

Dahlberg, R. (2015). Resilience and Complexity. *Culture Unbound*, *7*, 541–557. https://doi.org/10.3384/cu.2000.1525.1573

Departementene. (2012). *Nasjonal strategi for informasjonssikkerhet*. Oslo. Retrieved from https://www.regjeringen.no/globalassets/upload/fad/vedlegg/ikt-politikk/nasjonal_strategi_infosikkerhet.pdf

DIFI. (2012). *Styringssystem for informasjonssikkerhet*. Oslo. Retrieved from https://www.uninett.no/sites/default/files/webfm/difi-rapport-2012-15-styringssystem-for-informasjonssikkerhet_1.pdf

Digitaliseringsstyrelsen. (2017). *Resultatet af undersøgelse af status på implementering af ISO27001-principper i staten*. København. Retrieved from https://digst.dk/media/16012/resultat-for-staten-2017.pdf

DSB. (2016). *Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* Retrieved from https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

Duffield, M. (2012). Challenging environments: Danger, resilience and the aid industry. *Security Dialogue*, *43*(5), 475–492. 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. https://doi.org/10.1016/j.ijcip.2009.08.006

Elgsaas, I. M., & Schultz Heireng, H. (2014). *Norges sikkerhetstilstand-en årsaksanalyse av mangelfull forebyggende sikkerhet*. Retrieved from https://www.ffi.no/no/Rapporter/14-00948.pdf

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

Forligspartierne. AFTALE PÅ FORSVARSOMRÅDET 2018–2023 (2018). København: Folketinget. Retrieved from http://www.fmn.dk/temaer/forsvarsforlig/Documents/Forsvarsforlig-2018-2023.pdf

Forsvarsdepartementet. (2013). *Vägval i en globaliserad värld*. Stockholm. Retrieved from https://data.riksdagen.se/fil/D0CA1290-9BA0-4DA2-BA2F-C2088DC4FE99

Forsvarsministeriet. (2014). *National strategi for cyber- og informationssikkerhed*. København.

Forsvarsministeriet. (2019). Nye sektorstrategier skal ruste samfundet mod cyberangreb. Retrieved January 14, 2019, from http://www.fmn.dk/nyheder/Pages/Nye-sektorstrategier-skal-ruste-samfundet-mod-cyberangreb.aspx

Global Cyber Security Capacity Centre. (2017). *CYBERSECURITY CAPACITY REVIEW Republic of Iceland*. Oxford. Retrieved from https://www.stjornarradid.is/lisalib/getfile.aspx?itemid=f3bb2c35-4c76-11e8-942b-005056bc530c

Greenberg, A. (2018). The Untold Story of NotPetya, the Most Devastating Cyberattack in History | WIRED. Retrieved September 26, 2018, from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Hassel, H. (2016). Att mäta samhällelig resiliens. *CenCIP Professional Papers*, *2*, 1–7. Retrieved from https://www.cencip.lu.se/sites/cencip.lu.se/files/nr2_-_att_mata_samhallelig_resiliens_0.pdf

Jensen, M. S. (2017a). Interview med Janne Kuusela 2/11 2017. København.

Jensen, M. S. (2017b). Interview with Mika Kertunnan 7/11 2017. Helsinki.

Jensen, M. S. (2017c). Interview with Sauli Savisalo 7/11 2017. Helsinki.

Jensen, M. S. (2017d). Interviews with Vesa Virtanen 11/9 2017 and Vesa Valtonen 8/11 2017. Helsinki.

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), 1–18. https://doi.org/10.31374/sjms.3

Justitiedepartementet. (2017). *Nationell strategi för samhällets informations-och cybersäkerhet*. Stockholm. Retrieved from https://www.regeringen.se/49f22c/contentassets/3f89e3c77ad74163909c092b1beae15e/nationell-strategi-for-samhallets-informations--och-cybersakerhet-skr.-201617213

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J., Rusi, T., & Salminen, M. (2017). *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi*. Helsinki. Retrieved from https://tietokayttoon.fi/documents/10616/3866814/30_Suomen+kyberturvallisuuden+nykytila%2C+tavoitetila+ja+tarvittavat+toimenpiteet+tavoitetilan+saavuttamiseksi_.pdf/372d2fd4-5d11-4991-862c-c9ebfc2b3213?version=1.0

Lindgren, F., & Ödlund, A. (2015). *Utmaningar i återuppbyggnaden av Sveriges civila försvar*. Retrieved from www.foi.se/strategiskutblick

Ministry of the Interior. (2015). *Icelandic National Cyber Security Strategy 2015–2026. Plan of action 2015–2018*. Retrieved from https://www.government.is/media/innanrikisraduneyti-media/media/frettir-2015/Icelandic_National_Cyber_Security_Summary_loka.pdf

MSB. (2016). *Sverige kommer att möta utmaningarna, FM2016-13584:3*. Stockholm. Retrieved from https://www.msb.se/Upload/Insats_och_beredskap/160610 FM2016_13584_3 Rapport MSB och FM.pdf

Muller, L. P. (2016). Makt og avmakt i cyberspace: hvordan styre det digitale rom? *Internasjonal Politikk*, *74*(4). https://doi.org/10.17585/ip.v74.428

Myndigheten för samhällsskydd och beredskap – Krisinformation.se. (2009). Retrieved August 20, 2018, from https://www.krisinformation.se/detta-gor-samhallet/samhallets-ansvar/myndigheter-med-sarskilt-ansvar/msb

Myndigheten för samhällsskydd och beredskap (MSB). (2018). *Nationell risk- och förmågebedömning 2018*. Stockholm. Retrieved from https://www.msb.se/RibData/Filer/pdf/28470.pdf

Nasjonal Sikkerhetsmyndighet. (2018). *RISIKO 2018*. Sandvik. Retrieved from https://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2018_web.pdf

NISU. (2015). *Informations- och cybersäkerhet i Sverige SOU 2015:23*. Stockholm. Retrieved from https://www.regeringen.se/49bb84/contentassets/8ae8ef6d5d3f45058c981cbab4e297de/informations--och-cybersakerhet-i-sverige.-strategi-och-atgarder-for-saker-information-i-staten-sou-201523

Norwegian Ministry of Justice and Public Security. (2019). National Cyber Security Strategy for Norway. Oslo: Norwegian Ministry of Justice and Public Security. Retrieved from https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf

O'Dwyer, G. (2018). Finland government examines centralised cyber defence. Retrieved August 15, 2018, from https://www.computerweekly.com/news/252441613/Finland-government-examines-centralised-cyber-defence

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. (2018). National strategi for cyber-og informationssikkerhed Finansministeriet. København: Finansministeriet. Retrieved from http://www.fmn.dk/nyheder/Documents/National-strategi-for-cyber-og-informationssikkerhed-2018.pdf

Regjeringen. (2003). Nasjonal strategi for informasjonssikkerhet Utfordringer, prioriteringer og tiltak. Oslo. Retrieved from https://www.regjeringen.no/globalassets/upload/kilde/mod/red/2000/0002/ddd/pdfv/249054-nasjonal_strategi_for_informasjonssikkerhet.pdf

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

Ullring, S., Bjørhovde, G., Ellingsen, E., Hagen, K. P., Hofshagen, T., Høiland, G., … Tørmo, B. (2006). *Norges offentlige utredninger 2006:6 – Når sikkerheten er viktigst*. Retrieved from https://www.regjeringen.no/contentassets/c8b710be1a284bab8aea8fd955b39fa0/no/pdfs/nou200620060006000dddpdfs.pdf

Abstract in English

Since 2003, the governments of Norway, Denmark, Sweden, Finland and Iceland have developed and implemented national strategies for cyber and information security. The strategies include several topics such as organisational and human resource capacity building, defence policy, international cooperation, etc. This article gives a thumbnail sketch of the countries' strategies for the state's role in societal cyber resiliens (the ability to resist and overcome negative effects of events emanating from the cyber domain). It then shortly describes the experienced challenges with distribution of tasks and responsibilities, and how the implementation of the strategies reflect attempts to overcome them. It concludes that the Finnish government has gone furthest by placing responsibility for implementation centrally in an influential organisation and giving it a centrally developed common matrix for assessing progress and a well-established formal network within the private segment of Finland's critical infrastructure.

Keywords: cyber · resiliens · cyber defence · public-private partnership · governance · sector responsibility principle