CENTER FOR MILITÆRE STUDIER
KØBENHAVNS UNIVERSITET

Cyberwarfares udfordringer af begrebet kritisk infrastruktur

Kristian Cedervall Lauta
Rune Hoffmann
Lars Bangert Struwe

November 2013

Denne rapport er en del af Center for Militære Studiers forskningsbaserede myndighedsbetjening for Forsvarsministeriet. Formålet med rapporten er at analysere kritisk infrastruktur som begreb og afsøge alvorlige sårbarheder og trusler med henblik på at kunne anbefale, hvordan der bedst muligt kan etableres et robust og sikkert samfund i en kontekst af cyberrisici og -trusler .

Center for Militære Studier er et forskningscenter på Institut for Statskundskab på Københavns Universitet. På centret forskes der i sikkerheds- og forsvarspolitik samt militær strategi, og centrets arbejde danner grundlag for forskningsbaseret myndighedsbetjening af Forsvarsministeriet og de politiske partier bag forsvarsforliget.

Denne rapport er et analysearbejde baseret på forskningsmæssig metode. Rapportens konklusioner kan således ikke tolkes som udtryk for holdninger hos den danske regering, det danske forsvar eller andre myndigheder.

Læs mere om centret og dets aktiviteter på: http://cms.polsci.ku.dk/.

Forfattere:
Adjunkt, ph.d. Kristian Cedervall Lauta
Militæranalytiker, major Rune Hoffmann
Forsker, ph.d. Lars Bangert Struwe (redaktør)

ISBN: 978-87-7393-712-9

This report is a part of Centre for Military Studies' policy research service for the Ministry of Defence. Its purpose is to provide an analysis of critical infrastructure as a concept and to explore serious vulnerabilities and threats in order to recommend how best to establish a robust and secure society in the context of cyber risks and threats.

Centre for Military Studies is a research-based centre located at the Department of Political Science at the University of Copenhagen. The centre performs research in connection with security and defence policies and military strategies and this research constitutes the foundation for the policy research services that the centre provides for the Ministry of Defence and the political parties to the Defence Agreement.

This report is an analysis based on research methodology. Its conclusions should therefore not be understood as the reflection of the views and opinions of the Danish Government, the Danish Defence or any other authority.

Read more about the centre and its activities at http://cms.polsci.ku.dk/.

Authors:
Assistant Professor Kristian Cedervall Lauta, PhD
Military Analyst Rune Hoffmann, major
Researcher Lars Bangert Struwe, PhD, editor.

ISBN: 978-87-7393-712-9

English Abstract

There is increasing concern today about cyber warfare and cyber crime because modern society is more complex and vulnerable than ever before. Society relies on the availability of an increasing variety of functions, which are becoming increasingly sophisticated and interdependent. In fact, society is becoming so advanced that it is beginning to interact with itself. This means that it is no longer possible to predict on a one-to-one scale which components of a given society are critical to its overall function. Furthermore, functional differentiation, infrastructure dependencies, and global accessibility contribute to modern society's increasing vulnerability with regard to conventional as well as unconventional security threats.

Generally speaking, there are two competing discourses about possible reactions to the increasing complexity of society. One discourse claims that it is still possible, and necessary, to identify critical infrastructure, while a competing discourse claims that modern society has become too complex to effectively identify critical infrastructure.

Cyberspace in particular presents traditional military strategic thinking with a challenge. This makes it difficult to apply classic military theory that takes its point of departure in the use of conventional weapons, in a straightforward manner. One the one hand, cyberspace makes it possible to secretly erode a country's information infrastructure over a long period of time, and on the other, it offers the opportunity to attack a country at a few seconds' notice and create extensive damage. In the light of these capacities, cyberspace could very well prove to be the most important arena of security policy in the near future – the future first line of defence. For these reasons, among others, Denmark's strategic and operational capacity in cyberspace must be strengthened.

However, it is also relevant to discuss cyber defence without reference to military capacities. The threat of a conflict today that is not directly related to critical infrastructure in the traditional sense makes espionage appear even more relevant. Military and civilian coordination is therefore essential, not least as it is difficult to clearly define the boundaries between civil and military responsibility. An effective defence therefore requires timely and institutionalised coordination and a clear, coherent organisational framework. This aspect in particular could usefully be strengthened through scenario-based, interdisciplinary exercises with the emphasis on issues relating to "command and control" (C2) and a strengthened organisational framework.

The transition from civilian to military responsibility in particular should be revisited and practised, as an escalation could occur at very short notice. Training could take the form of scenarios that involve both civil and military authorities, preferably with the participation of the private sector. These exercises should be carried out at operational and strategic level, and thereby contribute to the establishment and maintenance of an understanding among the involved players.

Dansk resumé

I dag er der en stigende bekymring for cyberwarfare eller cyberkriminalitet. Det skyldes, at det moderne samfund er komplekst og sårbart. Samfundet baserer sig på udbuddet af stadig flere funktioner, som bliver tiltagende avancerede og internt afhængige af hinanden. Systemet bliver herved så avanceret, at det begynder at interagere med sig selv. Dette betyder, at man ikke længere på forhånd præcist kan forudsige, hvilke enkeltstående komponenter i et system der er kritiske. Funktionel differentiering, infrastrukturelle afhængigheder og global tilgængelighed bidrager til, at vi som samfund bliver mere sårbare overfor konventionelle, såvel som ukonventionelle, sikkerhedstrusler.

Overordnet er der to sameksisterende, konkurrerende debatter om den mulige reaktion på samfundets tiltagende kompleksitet. En, hvor man mener, at man kan identificere kritisk infrastruktur, og en anden, der siger, at denne er alt for kompleks til, at det giver mening.

Særligt cyberspace udfordrer klassisk militærstrategisk tænkning. Blandt andet det fundamentalt anderledes tids- og rumperspektiv gør det svært at overføre klassiske ideer om f.eks. eskalationsteorier eller anvendelsen af konventionelle krigsmidler til cyberspace. Krigsskuepladsen giver på den ene side mulighed for at erodere et lands informationsinfrastruktur over lang tid og på den anden side mulighed for med ét slag at tilføre et land store ødelæggelser uden varsel eller forudgående eskalation. Af samme grund bør Danmarks strategiske og operationelle kapacitet i cyberspace styrkes mest muligt. Cyberspace kunne meget vel vise sig at være det vigtigste sikkerhedspolitiske område i den nære fremtid – den første forsvarslinje.

Cyberforsvar er relevant ikke kun i forhold til traditionelle militære trusler om angreb, men i lige så høj grad i forhold til anslag, som ikke vedrører kritisk infrastruktur i traditionel forstand som spionage, og kapaciteter inden for både det civile og militære område. Militær og civil koordination er således af afgørende betydning, da de har hver deres syn på kritisk infrastruktur. Netop fordi det kan være vanskeligt at definere grænsen imellem det civile og militære, fordrer et effektivt forsvar en stor koordinationsindsats og en kohærent organisationsstruktur. Særligt dette aspekt kunne med fordel styrkes igennem scenariebaserede, tværgående øvelser med stor vægtning af forhold vedrørende ”command and control” (C2).

Der er en uklar grænse imellem civilt og militært ansvar. En situation kan ændre sig meget hurtigt ved eskalation af indsatsen. Man bør træne håndtering af sådanne situationer gennem scenarier, der gennemspilles af civile og militære myndigheder og inddrager det private erhvervsliv. Disse øvelser skal gennemføres på såvel operativt som strategisk niveau og etablere en forståelse imellem disse niveauer.

Anbefalinger

Følgende fem anbefalinger opstilles på baggrund af rapportens iagttagelser:

- Forsvaret af Danmark i forhold til cyber network operations-baserede trusler, styrkes gennem tværgående scenariebaserede eskalationsøvelser op til strategisk niveau med henblik på at belyse, hvor grænsen er imellem civile og militære trusler, og hvornår og hvordan militære cyberkapaciteter skal indsættes.

- Koordinationen imellem de forskellige civile og militære aktører, der aktivt arbejder med cyber network operations-trusler, styrkes. Dette sker næppe ved etablering af flere myndigheder.

- Beredskabsmyndighedernes pragmatiske tilgang til forståelsen af kritisk infrastruktur skal fastholdes, imens forsvaret samtidig bibeholder sit fokus på konkret kritisk infrastruktur.

- Man bør overveje hensigtsmæssigheden af begrebet kritisk infrastruktur for så vidt angår GovCERT's betjeningsområde, når retsgrundlaget for tjenesten genovervejes.

- Man skal ophøre med direkte sammenligninger mellem en angelsaksisk diskussion om kritisk infrastruktur og en dansk. En række forskelle i samfundsmodellerne besværliggør en sådan sammenligning, og samlet set er Danmark et langt mere robust samfund end de angelsaksiske.

Indholdsfortegnelse

1. Indledning

Kritisk infrastruktur blev for første gang introduceret på lovniveau i dansk ret, da man oprettede Forsvarets Efterretningstjenestes internetvarslingstjeneste, GovCERT. Her fik virksomheder og organisationer, der beskæftiger sig med kritisk infrastruktur, mulighed for at tilslutte sig tjenesten. Formålet med indførelsen af internetvarslingstjenesten under forsvaret var at forebygge cyberangreb på disse virksomheders og organisationers kritiske infrastruktur.

Da begrebet kritisk infrastruktur er nyt i dansk sammenhæng, er det naturligt at analysere dette i en sikkerhedspolitisk sammenhæng. Den førende forskning i kritisk infrastruktur er angelsaksisk, hvilket i denne forbindelse udgør et problem, da der er meget stor forskel på det danske velfærdssamfunds gennemregulerede samfundsstrukturer og den angelsaksiske verdens langt mindre regulerede samfund. Herved kan angelsaksiske anbefalinger ikke direkte overføres til et dansk velfærdssamfund. Samtidig viser det sig, at der er en væsensforskellig militær og civil diskurs inden for feltet, hvilket besværliggør konkret koordination og mere generelt arbejdet med kritisk infrastruktur i forbindelse med cybertrusler.

I lyset af disse betragtninger, der bliver uddybet herunder, forsøger denne rapport med udgangspunkt i en sikkerhedspolitisk tilgang og loven om GovCERT at identificere, hvad der kan forstås ved kritisk infrastruktur, hvilke særlige udfordringer identifikationen af kritisk infrastruktur i cyberspace medfører, og hvordan disse udfordringer kan adresseres.

Da de relevante retlige fortolkningsbidrag, der knytter sig lovgrundlaget, giver mulighed for en række forskellige fortolkninger, belyser rapporten med udgangspunkt i forskning og eksempler fra policyudvikling i andre lande mulighederne for, og udfordringerne i, at identificere kritisk infrastruktur i nutidens teknologiske samfund. Rapporten søger derved at skabe et overblik over ”state-of-the-art” i forhold til kritisk infrastruktur nationalt og internationalt (kapitel 2). Som en del af begrebets operationalisering oplister rapporten derefter de generelle udfordringer, som identifikationen af kritisk infrastruktur medfører (kapitel 3). Vores samfunds tiltagende teknologiske og funktionelle kompleksitet generelt, og særligt koblingen til computer network operations (CNO’er) i relation til infrastruktur er væsentlige udviklinger, der optager både forskningen og aktørerne inden for feltet. Et cyberangreb på Danmark kan hurtigt igangsætte et eskalationsscenarie, hvor et i udgangspunktet civilt angreb ændres til en militær konfrontation. Derfor formulerer rapporten

afslutningsvis et bud på, hvilke danske myndigheder der kunne arbejde med begrebet (og problemstillingerne) og på hvilken måde (kapitel 4) med henblik på at iværksætte øvelser, der kan forberede det danske samfund på angreb på dets infrastruktur. Rapporten afsluttes med en række anbefalinger, der adresserer udfordringerne med identifikation og håndtering af kritisk infrastruktur.

1.1 Problem og baggrund

I 1950'erne gav kontrollen og beskyttelsen af samfundsvigtige nøglepunkter umiddelbar mening. 2. Verdenskrig gav det danske samfund erfaringer med at dimensionere det danske forsvar i forhold til både menneskeskabte og naturlige trusler. I det industrielle samfund var den infrastruktur, der understøttede essentielle samfundsfunktioner, således under samfundets egen kontrol og samlet set af overvejende fysisk karakter. Det var derfor muligt at imødegå alvorlige anslag imod Danmark ved at bruge ekstra ressourcer på at beskytte særligt kritiske installationer.

Hvad der må betegnes som et samfunds infrastruktur, er altid under udvikling i takt med dette samfunds teknologiske og funktionelle ekspansion.[1] Kort sagt er det i dagens Danmark mindst lige så relevant som i 1950'ernes Danmark at prioritere indsatsen i forhold til beskyttelsen af infrastrukturen, men infrastrukturen er meget vanskeligere både at identificere, at kontrollere og at håndtere. Ligesom kompleksiteten i de systemer, det moderne samfund baserer sig på, inklusive selve infrastrukturen, bliver mere og mere kompleks, bliver de interaktioner og derved sårbarheder, der kan forårsage sammenbrud, tilsvarende mere komplekse.

Sårbarhedsudredningen fra 2004 identificerede fire hovedforhold, som på afgørende vis har ændret og til dels fortsat ændrer risikoscenariet for Danmark:

- Globalisering
- Teknologisk udvikling (informations- og kommunikationsteknologi (IKT))
- Terror
- Bortfald af en direkte militærtrussel med den kolde krigs ophør.

Ikke mindst de to første udviklingstendenser er blevet markant forstærket siden 2004. I dag baserer en del af vores samfunds essentielle funktioner sig således (helt eller delvist) på infrastruktur udenfor vores nationale kontrol.[2] Vi har fødevare- og ressourceforsyning fra Europa, elforsyning fra nabolande, olieforsyning fra Mellemøsten,

kommunikationsinfrastruktur via en myriade af servere placeret forskellige steder på kloden, alle virtuelt tilgængelige uden stedlige begrænsninger, og er dybt afhængige af opretholdelsen af transportveje og -sektorer i andre lande. Da Danmark i 2004 oplevede sin hidtil værste strømafbrydelse, skyldtes det således en fejl på det svenske elnet.[3]

Særligt cyberbaserede trusler imod kritisk infrastruktur i Danmark udfordrer forståelsen og beskyttelsen af kritisk infrastruktur. I en rapport udarbejdet for Energistyrelsen slår det private firma Security Lab således fast, at man ved et angreb på de såkaldte SCADA[4]-systemer i dag kan rette alvorlige anslag imod el-, vand- og varmeforsyningen i Danmark.[5] I den seneste udgave af Nationalt Risikobillede[6] angives såkaldte cyberangreb som ét blandt ti centrale risikoscenarier for Danmark, og for ganske nylig blev et omfattende cyberangreb imod borgernes CPR-numre og andre persondata afsløret.[7] Hertil kommer den mulighed for langsomt at erodere infrastruktur, som cyberspace ligeledes tilvejebringer, f.eks. ved effektivt at infiltrere vores kommunikationsinfrastruktur.[8]

Et centralt problem i forbindelse med cyberangreb er, at IKT både er en del af den kritiske infrastruktur og supporterer den kritiske infrastruktur. Cyberspace er således både en overordnet mængde, der dækker næsten hele den mulige kritiske infrastruktur, og en delmængde af denne og kan således sammenlignes med f.eks. elforsyningen.

Hertil kommer, at de infrastrukturelle anlæg, som vi faktisk har under national kontrol, også er blevet mere sårbare, fordi de er blevet mere avancerede, og fordi deres afhængighed af cyberspace øges. Altså: Ikke alene har vi tiltagende essentielle funktioner, der decideret er udenfor vores kontrol, vi har også stadig sværere ved at kontrollere de anlæg, der fortsat er placeret i Danmark.

Det er indtil nu begrænset, hvor mange anslag vi har set. I 2000 betød et angreb på den australske vandforsyning, at 800.000 liter kloakvand flød ud i parker og floder i Queensland,[9] og computerormen Stuxnet satte angiveligt Irans atomprogram adskillige år tilbage.[10]

Samtidig med denne, overordnet set, øgede kompleksitet synes diskussionen af, hvilke dele af vores samfundsinfrastruktur der skal betragtes som kritiske for samfundet, lige så aktuelle som altid. I Danmark har begrebet i en årrække været mindre aktuelt som styrende for organiseringen af vores beredskab. Ikke mindst den lange, stabile fredstidsperiode, som vi har oplevet efter den kolde krigs afslutning, har undermineret behovet for fuldstændigt at begrebsklassificere risici og sårbarheder.[11] Altså har fraværet af direkte militære trusler imod

Danmark, samt en gennemgående fornuftig civil infrastrukturplanlægning (herunder vedligeholdelse af denne), overflødiggjort at skelne strengt imellem, hvilke dele af samfundets infrastruktur der skal opfattes som kritiske henholdsvis ikkekritiske. Den hårde funktionsklassificering, der skelner skarpt imellem kritiske og ikkekritiske enheder, har således været inkorporeret i den offentlige og den private sektors gennemgående princip om risikobaseret dimensionering, jf. afsnit 2.2 om kritisk infrastruktur i Danmark.

Det aktuelle problem er, at der med den ovennævnte øgede kompleksitet følger nye sårbarheder. Når en 15-årig dreng principielt kan sidde i Pakistan og slukke for strømmen i Danmark, må vi overveje, hvordan vi igen kan prioritere vores beskyttelsesindsatser og samtidig sende klare signaler til fjendtlige elementer og derved skabe klare retningslinjer for, hvornår der er tale om et kritisk anslag.[12, 13]

Selve begrebet kritisk infrastruktur er et moderne begreb, selvom det trækker på en lang forsvars- og beredskabstradition. Imens det på den ene side således har en intuitiv klangbund hos myndigheder, der er beskæftiget med forsvar og beredskab, er det på den anden side vigtigt at holde sig for øje, at det som begreb er ungt. Således er det iboende dilemma, som denne rapport, og i sidste ende alle moderne diskussioner om kritisk infrastruktur, kredser om, at kritisk infrastruktur på den ene side er indlysende centralt for at kunne opretholde et effektivt forsvar og på den anden side bliver mere og mere vanskeligt at operere med som kategori.

1.2 Opgave

Nærværende rapport er et produktionsmål inden for CMS' forskningsbaserede myndighedsbetjening til Forsvarsministeriet i 2013. Der er tale om en analyse af kritisk infrastruktur som begreb og en afsøgning af alvorlige sårbarheder og trusler med henblik på at kunne anbefale, hvordan der bedst muligt kan etableres et robust og sikkert samfund i en kontekst af cyberrisici og -trusler.[14]

1.3 Fremgangsmåde

På grundlag af ovenstående opgavebeskrivelse har CMS afholdt et indledende møde med Forsvarsministeriet med henblik på at afstemme forventninger til rapporten. CMS har på baggrund af en destillation af disse forventninger – sammenholdt med egne interne procedurer for gennemførelse af projekter[15] – valgt nedenstående fremgangsmåde for udmøntning af projektet.

Overordnet førte opgaveanalysen frem til tre trin forud for den endelige konklusion og anbefaling. Første trin afsøger og gennemgår begrebet kritisk infrastruktur med udgangspunkt i forskningslitteraturen såvel som i en national og international kontekst med henblik på at danne forudsætning for analysens andet trin. Andet trin analyserer de udfordringer, der er forbundet med operationalisering af kritisk infrastruktur i henholdsvis en civil og en militær kontekst. Tredje trin behandler kritisk infrastruktur i relation til cybertrusler for derigennem at opstille en eskalationsstige med henblik på at indikere, hvornår imødegåelse af trusler imod infrastruktur er et anliggende for forsvarets kapaciteter. Dette sidste trin blev tilføjet, da begrebet kritisk infrastruktur, som det fremgår af kapitel 2, i sig selv er omdiskuteret. Vi valgte derfor at tilføje et afsnit, der i højere grad betoner de politiske og operationelle muligheder, som begrebet omfatter i en cyberkontekst.

Som et led i den indledende research afholdt rapportens forfattere møder med interessenter og eksperter inden for feltet beredskab og cybertrusler i Danmark. Det skete for at identificere eventuelle nye perspektiver i forhold til det primære fundament i "state-of-the-art" inden for feltets forskningslitteratur og for at kunne inddrage synet på emnet i lande, som vi normalt sammenligner os med. Endvidere fik interessenterne mulighed for at komme med yderligere kommentarer på baggrund af skriftlig information om rapportens tre trin – dette skete med henblik på at sikre yderligere validering forud for udfærdigelse af rapportens konklusion og anbefalinger.

Den endelige kvalitetssikring af rapporten er funderet i CMS' principper, der indebærer en intern reviewproces efter færdiggørelsen af den endelige rapport og en efterfølgende bedømmelse ved en ekstern ekspert (peer-review/fagfællebedømmelse). I den forbindelse ønsker rapportens forfattere at rette en stor tak til interessenter, interne bedømmere og den eksterne fagfællebedømmer. Det skal dog samtidig understreges, at rapportens perspektiver, konklusioner og anbefalinger alene er forfatternes ansvar.

2. Kritisk infrastruktur

At identificere kritisk infrastruktur forudsætter en lang række antagelser af både normativ og faktuel karakter. Kritisk infrastruktur er ikke en naturlig sproglig eller organisatorisk kategori på trods af den intuitive forestilling om det modsatte. Dette kapitel giver et overblik over, hvordan begrebet er forsøgt institutionaliseret i Danmark, hvordan "state-of-the-art" inden for forskningen behandler kritisk infrastruktur, og endelig hvordan begrebet er anvendt i en international kontekst. Formålet med kapitlet er at bidrage til danske myndigheders mulighed for at fortolke begrebet kritisk infrastruktur.

2.1 Uforudsigeligt eller komplekst – to diskurser

Overordnet findes to sameksisterende, konkurrerende diskurser om den mulige reaktion på samfundets tiltagende kompleksitet:

- En gruppe teoretikere og praktikere betragter kompleksitet som uforudsigelighed og mener derfor, at vi ikke bør basere vores respons på gisninger om systemets interaktioner, men i stedet fokusere på at opbygge generel resiliens (robusthed) og redundans.

- En anden gruppe teoretikere og praktikere fastholder, at vi kan, og bør, identificere svage punkter, som kan sætte samfund ud af spil, og at dette gøres ved at lade analysemodellen følge samfundsudviklingen og således øge modellens kompleksitet.

Der er altså tale om to forskellige måder at forstå, håndtere og tale om kritisk infrastruktur på. Med andre ord eksisterer der to meget forskellige måder at forstå vores evne til at systematisere samfundet og dets trusler på – og dette kommer til udtryk i markant forskellige tilgange til kritisk infrastruktur.

Hvis man således på den ene side fastholder, at det er muligt at systematisere kompleksiteten, kommer det til udtryk i en forskningsstrategi, hvor samfundet kan og bør systematiseres, f.eks. igennem komplicerede algoritmer. Dette resulterer i implementeringsfasen i lister over aktiver og oversigter over relevante infrastrukturelle anlæg. I det tilfælde, at uforudsigelige hændelser forekommer, vil dette skulle indregnes i den anvendte model, som derved i sig selv bliver mere og mere kompleks, men, ifølge denne tænkning, også mere og mere præcis. Vi kan med andre ord igennem analyser af tidligere hændelser, ny viden om verden (f.eks. meteorologiske modeller, klimaforskning eller terrorforskning) og forestillinger om fremtiden

blive stadig bedre til at imødegå fremtidige trusler og stadig mere præcist identificere, hvilke dele af vores samfund vi bør beskytte.

Hvis man derimod anlægger det grundsynspunkt, at komplekse systemer ikke kan systematiseres, men er komplekse, netop fordi de interagerer uforudsigeligt, vil man fokusere på samfundets generelle modstandskraft. Det betyder ikke nødvendigvis, at Storstrømsbroen er lige så vigtig som Storebæltsbroen, men at det kan være svært fuldstændigt at forudsige konsekvenserne af Storstrømsbroens sammenbrud (og derved endeligt afgøre, om den er kritisk eller ej). Konsekvensen er altså, at ideen om, at vi på forhånd fuldstændigt kan adskille kritisk fra ikkekritisk, bliver illusorisk. I stedet bør vi sikre kritiske funktioner igennem opbyggelse af redundante systemer med fokus på lokal resiliens og kreativ responskapacitet.

Som det fremgår af det følgende, er disse to forståelsesparadigmer også afspejlet i de institutionelle rammer, som kritisk infrastruktur i dag er indlejret i, også til dels i en dansk kontekst. De to diskurser betyder, at dels en fælles institutionel tilgang og dels en fælles samtale om tilgangen til kritisk infrastruktur er vanskelig, hvis der ikke er en forståelse af andre sektorers udgangspunkt. I det følgende vil de to diskurser træde klarere frem i gennemgangen af begrebet kritisk infrastruktur.

2.2 Kritisk infrastruktur i Danmark

Kritisk infrastruktur er, på trods af sin intuitive relevans, et ungt beredskabsbegreb. Selvom man altid har arbejdet med en ide om kritikalitet i beredskabsplanlægning, og ikke mindst strategiske nøglepunkter i forsvarsplanlægning, optræder en institutionalisering af begrebet kritisk infrastruktur først fra midten af 1990'erne.[16] I forlængelse heraf opstod begrebet kritisk infrastruktur-beskyttelse (Crititical Infrastructure Protection – (CIP)). T*he President's Commission on Critical Infrastructure Protection* analyserede i 1996 beskyttelsen af følgende fem funktioner i en amerikansk kontekst:

1. Information and Communications
2. Banking and Finance
3. Energy, Including Electrical Power, Oil and Gas
4. Physical Distribution
5. Vital Human Services.[17]

Begrebet kritisk infrastruktur blev først introduceret i Danmark efter terroranslaget imod USA 11. september 2001.[18] Centralt for begrebets nuværende implementering er således, at det er opstået, udviklet og implementeret hovedsageligt i forbindelse med terrorbekæmpelse. I Danmark har man aldrig haft en gennemgående institutionel definition af kritisk infrastruktur. I sårbarhedsudredningen fra 2004 valgte kommissionen således at afstå fra definere kritisk infrastruktur.

For at skabe et minimum af begrebsklarhed beskriver sårbarhedsudredningen begrebet som omfattende "de elementer i et overordnet system (samfund), der er så vitale, at forstyrrelse og nedbrud af bare en enkelt af dem ville kunne true selve systemets funktionsduelighed."[19] Denne overordnede definition må siges, for sig selv, at give meget lidt operationel vejledning i tvivlsspørgsmål i forbindelse med identifikation af kritisk infrastruktur.

På trods af udredningens tilbageholdenhed med hensyn til håndfast at definere kritisk infrastruktur indeholder den foreslåede definition nogenlunde de variable led, som definitioner af kritisk infrastruktur generelt kredser omkring. Et beskyttelsesobjekt ("et overordnet system"), en kobling mellem subjekt og funktion ("er så vitale") og en intensitetsbetragtning ("forstyrrelse og nedbrud (…) true selve samfundets funktionsduelighed").

Kritisk infrastruktur indgår i dag i en række retsgrundlag på beredskabsområdet, vigtigst, og for første gang på lovniveau, i lov om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v.[20] Loven regulerer dele af embeds- og funktionsområdet for Forsvarets Efterretningstjenestes enhed GovCERT[21] med det formål "at skabe klar hjemmel for den statslige varslingstjeneste for internettruslers behandling af personoplysninger". Tjenesten, der blev etableret i 2009, har til formål at sikre, "at staten kan reagere koordineret overfor trusler imod informationssikkerheden og hurtigt imødegå konsekvenserne af it-angreb"[22]. Loven er vedtaget med henblik på at balancere dette formål med det gennemgående hensyn til privatlivets fred, herunder retten til beskyttelse af personoplysninger. I lovens § 2 gives kommuner og virksomheder, der er beskæftiget med kritisk infrastruktur, mulighed for at tilslutte sig varslingstjenesten.

Loven forstår i henhold til de almindelige bemærkninger kritisk infrastruktur på følgende vis:

> "Begrebet 'kritisk infrastruktur' omfatter her, i overensstemmelse med begrebets fortolkning på det beredskabsmæssige område, de sektorer, der forestår vitale

> samfundsmæssige interesser, f.eks. finans-, energi- samt it- og telesektoren. Begrebet skal fortolkes dynamisk og vil således udvikle sig over tid i takt med samfundsudviklingen, som kan gøre det relevant at inddrage nye sektorer under begrebet kritisk infrastruktur."[23]

Altså en definition, der fortsat betoner kritisk infrastruktur som et dynamisk begreb, men i modsætning til sårbarhedsudredningen knyttes begrebet ikke til disse vitale funktioners sammenbrud.

Endvidere fastslås det i de almindelige bemærkninger til lovforslaget:

> "Internettet er blevet en del af den kritiske infrastruktur. En række af de funktioner, som udføres af det offentlige, og som er væsentlige for statens virke, afhænger af internettet."[24]

Denne tilgang, hvor kritisk infrastruktur modelleres over sektorer, der synes at forestå vitale funktioner, ligger ganske vist i tråd med den eksisterende sektorbaserede beredskabstænkning i Danmark, men bringer ikke fortolkeren tættere på med sikkerhed at kunne prioritere hverken inden for eller imellem sektorer. Det er sigende, at beredskabsloven ikke indeholder referencer til kritisk infrastruktur[25], ligesom begrebet ikke kan betegnes som strukturerende for beredskabstænkningen i Danmark konkret eller generelt.

Udover "internettet" eksemplificerer lovens almindelige bemærkninger kritisk infrastruktur som "finans-, energi-, samt it- og telesektoren"[26] og fastslår, at dele af denne infrastruktur i dag er i hænderne på private virksomheder, herunder elforsyningen.[27] Derudover optræder kritisk infrastruktur i dansk ret alene *en passant* i forbindelse med varetagelsen af sektoransvaret.[28]

Dette betyder dog ikke, at man i dag ikke differentierer beskyttelsesindsatsen. I stedet for at arbejde med på forhånd opstillede kategorier, der opdeler i kritisk henholdsvis ikkekritisk infrastruktur, og derved med kategorisk forskellige krav til risikodimensioneringen, integrerer man i dag kritikalitet i den risikobaserede dimensionering.[29]

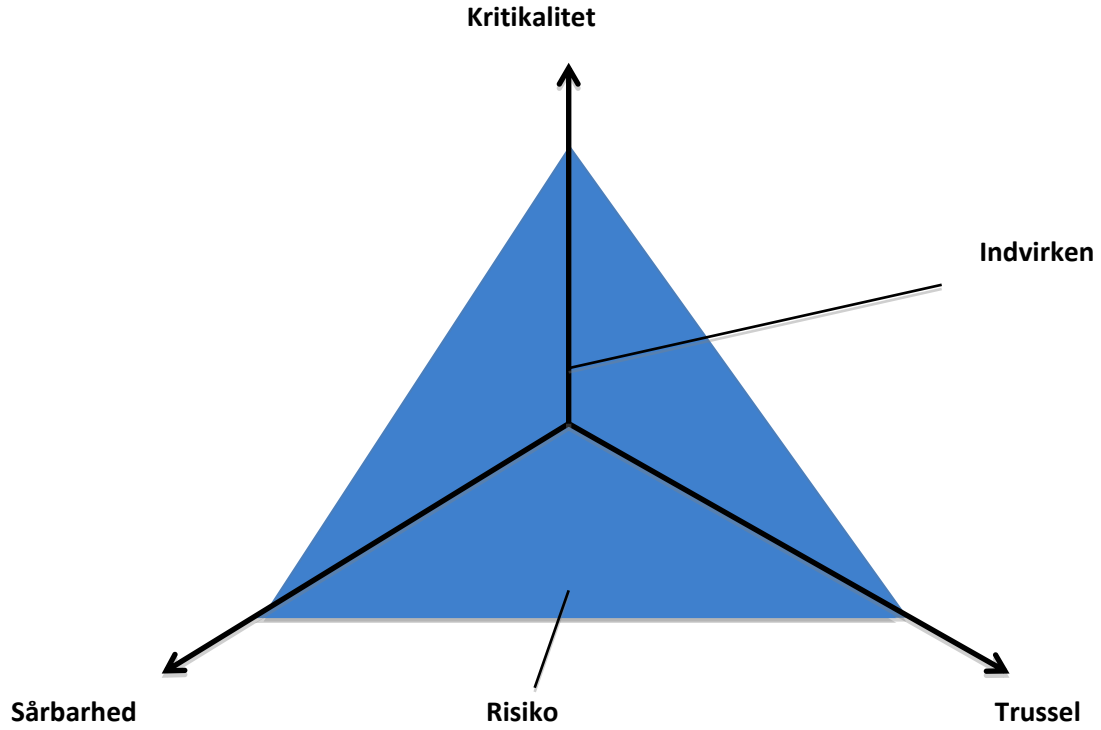
Sandsynligheden, eller risikoen[30], for en given hændelse opgøres i dag, let fortegnet, ved at sammenholde en enheds sårbarhed eller robusthed med det aktuelle trusselsbillede. Dimensioneringen af responssystemet foregår således, ideelt, ved at "øge eller mindske sandsynlighed for, at risici udløses; øge eller mindske konsekvenser, når risici udløses; tilføre

eller fjerne risici – det vil sige tilføre eller fjerne objekter og muligheden for, at der sker ulykker".[31]

Et tredje ben i denne analyse vedrørende kritikalitet kan på den ene side tilgodese den konkrete kompleksitet og på den anden side behovet for systematisk at prioritere indsatsen.

Forholdet mellem kritikalitet, sårbarhed, trussel, risiko og indvirken kan illustreres på følgende vis:

Figur 1: Kritikalitet og risiko



I princippet kan arealet, der optegnes imellem de tre faktorer, siges at udgøre prioriterings-behovet eller, om man vil, beskyttelsesinteressen for Danmark.

I Beredskabsstyrelsens *Håndbog i risikobaseret dimensionering* anbefales det i forbindelse med risikoanalyse at arbejde med en såkaldt risikobaseret matrice, hvor potentielle hændelser opdeles efter hyppighed og konsekvens. En given hændelse vurderes her på en skala 1-5, hvor 5 er "kritisk". Håndbogen giver en række meget håndgribelige eksempler på indikatorer for denne kritikalitet, herunder antallet af berørte individer og omfanget af tab.[32]

Risikobaseret dimensionering løser bestemt ikke alle problemer, men adresserer til dels det vidensproblem, der uløseligt knytter sig til probabilitets- og kausalitetsanalyser. Desværre

betyder det også, at en væsentlig del af analysen af en given enheds kritikalitet er overladt til enheden selv med de fordele og ulemper, det medfører. Eksempelvis er det i denne forstand oplagt at bringe begrebet kritikalitet i anvendelse i forbindelse med ressourcekampe. Synliggørelsen eller ekspliciteringen af dette kriterium i dimensioneringen vil styrke tilsynsmyndighedens mulighed for at påtale åbenlyse fejldimensioneringer og fejl samt magtmisbrug og give indspark til fordel for Danmarks samfundssikkerhed.

Et nyligt fremlagt EU-direktiv om netværks- og informationssikkerhed, det såkaldte NIS-direktiv (Network and Information Security)[33], opererer ligeledes med en sådan sektorbaseret modellering (tilsyneladende valgt på baggrund af Europa-Kommissionens erfaring). Her omfattes "market operators" i artikel 3.8, hvis de styrer kritisk infrastruktur, "that are essential for the maintenance of vital economic and societal services". Med bestemmelsen følger en ikkeendelig liste over sektorer, som Europa-Kommissionen vurderer som kritiske[34], og som omfatter energi-, transport-, bank-, finans- og sundhedssektorerne.

En sektorbaseret modellering tilvejebringer gode indikatorer for kritisk infrastruktur og er således en tiltalende og nem fremgangsmåde, hvor besværet med at fremskrive en præcis definition erstattes af erfaringsbaseret intuition.

2.3 Kritisk infrastruktur som forskningsgenstand

Moderne teorier om håndtering og identifikation af kritisk infrastruktur handler ofte om at afkode, balancere og kontrollere afhængigheder ("dependencies" eller "interdependencies") i et komplekst system af fysiske, virtuelle, kulturelle og geospatiale afhængigheder og forsøge at håndtere den øgede kompleksitet ved hjælp af netværksteori[35], sårbarhedsanalyse[36] eller resiliensovervejelser[37]. I det følgende forsøger rapporten at give et indblik i denne forskning.

Ikke alene hænger infrastruktur i dag sammen igennem IKT, infrastrukturer hænger også i stigende grad fysisk sammen. Dette har medført, at en række teoretikere tager udgangspunkt i disse afhængigheder i identifikationen af kritisk infrastruktur. Koblinger mellem infrastruktur kan opdeles i forskellige typer af afhængigheder (dependencies/interdependendies).[38] Rinaldi, Peerenboom og Kelly definerer fire typer af afhængigheder:

- Fysiske – en fysisk forbindelse, f.eks. en ledning
- Cyberbaserede – informationssystemsudveksling
- Geografiske – hovedsageligt udtrykt som fysisk nærhed

- Logiske – en opsamlingskategori indeholdende kulturelle, samfundsmæssige sammenhænge.[39]

For særligt at gøre de logiske afhængigheder mere operationelle supplerer Pederson et al. taksonomien. Udover fysiske (ledninger), informationsbaserede (f.eks. SCADA) og geospatiale (fysisk nærhed) afhængigheder medtager de således policybaserede (lovgivning eller policy) og samfundsbaserede (øvrige sociale faktorer, f.eks. offentlig mening, frygt eller kultur) afhængigheder.[40] Der findes en række eksempler på stedfundne begivenheder, der understreger, hvordan i hvert fald fysiske, informationsbaserede og geospatiale afhængigheder ofte manifesterer sig i form af svært forudsigelige 2.- og 3.-ordens-effekter.[41]

En måde at arbejde med kritisk infrastruktur på er at identificere og kortlægge infrastruktur via disse afhængigheder. Jo flere afhængigheder på et givent stykke infrastruktur, jo mere kritisk. Dette kan udvides via identifikationen af afhængighedsklasser, som man forsøger i den nationale amerikanske strategi for beskyttelse af kritisk infrastruktur.[42]

Den interessante forandring, der har ændret vores infrastrukturelle behov, er naturligvis den tiltagende afhængighed af cyberspace. Som informationsteknologi og netværksbasering indarbejdes i vores kritiske infrastruktur, bevæger cyberspace sig langsomt nedad i afhængighedshierarkiet og må i dag helt oplagt, som det også er tilfældet i den amerikanske model, skulle placeres i bunden af afhængighedsklasserne.

Ted Lewis fra Department of Homeland Security (DHS) foreslår i sin bog *Critical Infrastructure Protection in Homeland Security* en model, hvor man i analysen af kritisk infrastruktur tager udgangspunkt i infrastrukturelle netværksafhængigheder. Det punkt (”node”) med flest afhængigheder (”links”) er det anlæg (”hub”) med den største beskyttelsesinteresse. Da Nørreport Station har flere afhængigheder til andre dele af infrastrukturen i hovedstaden end Frederikshavn banegård, er beskyttelsesinteressen større, og derved er Nørreport Station mere kritisk. Uanset om man vælger DHS’ meget funktionelle tilgang, er afhængigheder en meget væsentlig del af at forstå og arbejde med kritisk infrastruktur konkret og komplekse systemer generelt.

Disse afhængigheder og deres tætte og uforudsigelige kobling skaber det, man inden for systemteori beskriver som et komplekst system. Komplekse systemer er som udgangspunkt hverken mere sårbare eller mere robuste end ikkekomplekse systemer. Samlet set er vores kontrol over komplekse systemer dog markant mindre – hvilket ofte medfører hændelser af

en anden karakter end tidligere set eller forudset. Kompleksitet øger derfor risikoen for svært forudsigelige kaskadeeffekter imellem forskellige dele af infrastrukturen.[43] Imens det således på den ene side er oplagt, at vi bliver mere sårbare, når vi mister kontrol over infrastrukturen, er der situationer, hvor det styrker, særligt et samfund som det danske.

I sit indflydelsesrige hovedværk, *Normal Accidents*, taler den amerikanske sociolog Charles Perrow om, hvordan der uundgåeligt i sådanne komplekse tætkoblede systemer vil være tilbagevendende hændelser, som vi ikke kan forudsige eller forhindre, såkaldte "normal accidents".[44] Hændelserne skyldes hovedsageligt, at vi har gjort os afhængige af tætkoblede og komplekse systemer, der, udover en øget funktionalitet, danner grundlag for uforudsigelige interaktioner imellem systemets komponenter – og derved forventelige (det vil sige normale), men samtidig fuldstændigt uforudsigelige ulykker. Kompleksitet øger altså risikoen for svært forudsigelige kaskadeeffekter imellem forskellige dele af infrastrukturen.[45]

Kompleksitetsteori bruges i denne sammenhæng ofte til at kritisere forventningen om på forhånd at kunne identificere kritisk infrastruktur som funktionalistisk og probabilistisk tænkning, der aldrig vil kunne afspejle de reelle udfald, systemet vil forårsage. Løsningen for disse kritikere er at styrke decentral organisering, robusthed og almen risk-awareness i stedet for at arbejde med et strengt operationelt begreb om kritisk infrastruktur.

En kombination af en begrænset central responskapacitet og decentral organisering er således, udover muligvis at være en ønskværdig samfundsform, et forsvar imod totale sammenbrud. Den amerikanske økonom og samfundstænker Nassim Taleb, bedst kendt for sin Black Swans-teori, undrer sig i seneste bog *Antifragile* over de nordiske landes (økonomiske) succes. Ifølge Talebs teori burde det øge et givent lands sårbarhed eller fragilitet at centralisere samfundet. Det antifragile samfund er således i stand til decentral selvorganisering. Talebs undren over de nordiske velfærdsstater ophører dog, da det bliver klart for ham, at de nordiske lande jo netop ikke er at sammenligne med angelsaksiske stater. Først og fremmest fordi en stor del af samfundets ressourcer ikke fordeles fra centralt, men fra decentralt hold, igennem kommuner og derved til skoler, børnehaver og alment boligbyggeri, alt sammen i vidt omfang brugerstyret. Selve staten er ifølge Taleb reduceret til "a tax collector".[46] Selvom Taleb måske herved går vel vidt i sin beskrivelse af den nordiske velfærdsmodel, påpeger han effektivt vanskeligheden ved at overføre amerikanske og britiske beredskabs- og forsvarserfaringer direkte til en dansk kontekst og den dobbelthed, der er i at være en stor decentralt organiseret stat.

I modsætning til centraliserede minimalistiske stater som Storbritannien og USA gennemsyrer det offentlige Danmark alle samfundsfunktioner. Imens dette på den ene side besværliggør kontrollen, gør det på den anden side Danmark relativt robust overfor anslag. Det er populært sagt ganske vanskeligt at slå staten Danmark ud ved ét slag, men ganske nemt at ramme den. Man kan således ikke sammenligne angelsaksiske erfaringer direkte med nordiske, særligt ikke i forbindelse med dette emne, der i så høj grad vedrører samfundets grundlæggende struktur.[47]

2.4 Udsyn: Kritisk infrastruktur som policy-begreb

I dette afsnit opridses ganske kort, hvordan kritisk infrastruktur er indlejret i andre systemer end det danske. Dette dels for at give et operationelt udsyn, dels for at vise bredden i forståelsen af, hvad kritisk infrastruktur er. Udsynet kan således bidrage til at udfylde det fortolkningsrum, der i Danmark overlades til myndighederne.

EU's kritisk infrastruktur-program (EPCIP)[48] arbejder ud fra en inklusiv definition, hvor funktioner ikke skal påvirke "selve systemets funktionsduelighed" eller varetage "vitale samfundsinteresser", men alene "i væsentlig grad (…) påvirke en medlemsstat":

> "'kritisk infrastruktur': aktiver, systemer eller dele deraf, der befinder sig i medlemsstaterne, og som er væsentlige for opretholdelsen af vitale samfundsmæssige funktioner og menneskers sundhed, sikkerhed og økonomiske eller sociale velfærd, og hvis afbrydelse eller ødelæggelse i væsentlig grad ville påvirke en medlemsstat som følge af, at disse funktioner ikke kan opretholdes."[49]

I denne definition identificeres kritisk infrastruktur altså ud fra de potentielle konsekvenser af et nedbrud og dettes effekt.

I Sverige fik man i 2001 en sårbarheds- og sikkerhedsudredning ved navn *Säkerhet i en ny tid*. Her fokuserer man på en række specifikke forhold og udpeger særligt kritiske informationssystemer eller sektorer såsom elsektoren og telesektoren.[50]

I dag definerer de svenske kriseberedskabsmyndigheders dog kritisk infrastruktur som: "Fysisk struktur vars funktionaltiet bidrar till att säkerställa upprätthållande av viktiga samhällsfunktioner"[51]. Den svenske definition tager således ikke udgangspunkt i trusselsbilledet og disses potentielle effekter, men derimod direkte i den pågældende enheds funktionalitet for samfundet. Denne tilgang tager altså udgangspunkt i anlæg, der bringer

eller understøtter produktionen af værdi til samfundet, i stedet for anlæg, der truer en sådan værdi.

Også i Norge forstås infrastruktur med udgangspunkt i værdiskabelse, og også her tager man skridtet videre i forhold til at forstå, hvilke funktioner der kunne være tale om:

> ”Kritisk infrastruktur er de anlegg og systemer som er helt nødvendige for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse.”[52]

Justis- og beredskapsdepartementet foreslår ydermere at anskue kritisk infrastruktur med inspiration i en klassisk model for forståelse af cyberspace som delt i tre lag: den faktiske fysiske enhed (f.eks. elektricitetsføringen), samfundsfunktioner (f.eks. el – og funktioner, der forudsætter el), og brugere (f.eks. borgere i Norge). Snarere end en dækkende beskrivelse af, hvad kritisk infrastruktur er, er dette nok mere et (i øvrigt udmærket) processuelt eller metodisk greb til at identificere infrastruktur og derved et tentativt indblik i det værdihierarki, der er nødvendigt for effektivt at arbejde med kritisk infrastruktur. Dette behandles nærmere i kapitel 3. Ydermere tager den norske model højde for, at kritisk infrastruktur i dag er netværksbaseret, hvilket umuliggør en helt ideel (ren) sektorbaseret modellering.

Den britiske definition tager mere nøgternt udgangspunkt i ”the functioning of the country (…) which daily life in the UK depends”:

> ”those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends.”[53]

Sigende for vanskeligheden i på få linjer at indkredse kritisk infrastruktur er det følgende den definition, som den tidligere omtalte præsidentielt nedsatte kommission for kritisk infrastrukturbeskyttelse i USA fremkom med:

> ”Systems and assets, whether physical or virtual, so and vital that the incapacity or destruction of such may have a debilitating impact on national security, national economic security, public health or safety, environment, or any combination of these matters, across any Federal, State, regional, territorial, or local jurisdiction.”[54]

Hvis hovedformålet med at anvende en definition er at opnå sproglig præcision og operationel relevans, synes det næsten at ophæve dette formål at anlægge en så operationel,

men samtidig geografisk-inklusiv definition, som den amerikanske, hvor alt fra en bogbus i Casper, Wyoming, til Air Force One må inkluderes i forståelsen af kritisk infrastruktur. Denne meget inklusive, men samtidig operationelle tilgang, har da også ført til meget lange lister over aktiver (77.000 aktiver i 2009 i USA).

Omvendt kunne man mene, at den norske model med udgangspunkt i en meget teoretisk begrebsliggørelse af tryghedsfølelsen næsten umuliggør en effektiv operationalisering. Disse to positioner kan betegnes som yderpunkter inden for disse definitioner.

3. Analyse: Indkredsning af udfordringer

Kritisk infrastruktur er et vanskeligt begreb at arbejde operationelt med, og, som det fremgår af kapitel 2, også at opstille definitioner af. Problemet ved at opstille en klar, operationel definition består således dels i:

1. *Teoretisk* – herunder definitorisk – at identificere vitale samfundsinteresser eller -funktioner, da dette involverer en række normative og politiske valg.
2. *Praktisk* fuldstændigt at afdække sammenhængen mellem et givent stykke infrastruktur og de føromtalte samfundsinteresser. Både at fastslå, at et sammenbrud faktisk ville forhindre den givne vitale samfundsfunktion i at fungere, altså et spørgsmål om kausalitet, og at identificere fuldstændigt, hvilke kombinationer og koblinger der kunne føre til et sådant sammenbrud, det vil sige de ovenfor omtalte afhængigheder.

I det følgende bliver den første af disse hovedudfordringer underkastet en kort uddybende analyse.

Formålet med kapitlet er, til gavn for læseren, at gøre det klart, hvad en definition af kritisk infrastruktur bør tage højde for, og således at skabe en slags definitionsanatomi af begrebet. For at identificere kritisk infrastruktur skal man således igennem en sluse af beslutninger. Det norske beredskab arbejder, som ovenfor anført, med en heraf afledt tredelt proces: infrastruktur, samfundsinteresse og brugere. I det følgende foreslår vi en femledet proces, der også inddrager strukturerende overvejelser over koblingen mellem samfundsinteresser og infrastruktur og overvejelser over situationsbestemt kritikalitet.

Imens afsnittet om kritisk infrastruktur som forskningsgenstand redegør for de faktuelle udfordringer med kritisk infrastruktur i et samfund med tiltagende teknologisk og funktionel kompleksitet, forsøger vi i det følgende at optegne nogle af de mere normative valg, der er indlejret i begrebet.

3.1 Normative udfordringer: Hvem, hvad, hvornår?

Et effektivt forsøg på at indkredse kritisk infrastruktur medfører, som det fremgår af ovenstående, en lang række normative valg. De normative udfordringer, der er forbundet med at definere kritisk infrastruktur, er i hvert fald treleddede. Imens de to første er abstrakte, involverer det sidste normative valg en situationel konkretisering af begrebet, som muligvis

forudsætter, at det udskilles fra de andre spørgsmål og adresseres konkret. Det følgende afsnit er struktureret ud fra følgende spørgsmål:

- Hvem beskytter vi?
- Hvad er funktionelt vitalt for dem?
- Hvornår er deres kritiske smertegrænse nået?

At definere vitale interesser forudsætter en klart defineret målgruppe, inden for hvilken vi kan klarlægge, hvad der opfattes som vitalt. Det første normative spørgsmål er en indkredsning af kritisk infrastruktur og bør stilles således: ”Hvem er omfattet af Danmarks interesser?” Kernen i, hvem der omfattes, kan nemt besvares med ”staten Danmark”, men dette viser sig hurtigt at være et væsentligt problem i de videre definitionsbestræbelser. Kan og bør der eksempelvis skelnes mellem privat og offentlig, national og regional eller borger og institution? Er regeringen i sig selv et beskyttelsesobjekt eller alene beskyttelsesværdigt i kraft af den funktion, den på vegne af borgere i Danmark udfører? Er beskyttelsesobjektet alene dansk, eller har vi en infrastrukturel interesse i EU, Norge eller Norden? Imens svaret på dette muligvis er, at Sverige ikke umiddelbart er et beskyttelsesobjekt for staten Danmark, betyder det vel ikke, at vi kan være ligeglade med infrastruktur (f.eks. en server placeret i København), der ved sammenbrud ville sætte Sydsverige tre år tilbage i tid?

Hertil kommer det principielle spørgsmål, om ”Danmark” omfatter rent private interesser. Hvis en trussel alene vedrører interesser på private hænder – er det i så fald omfattet af Danmarks beskyttelsesinteresse, eller er det alene de afledte effekter af et anslag imod private, som påkalder sig vores interesse som samfund? Imens det på den side er klart, at det ville være skadeligt for Danmark, hvis Maersks omsætning blev halveret pga. et cyberangreb, ville det vel næppe være noget der, i sig selv, var en vital interesse for staten Danmark?

Det andet spørgsmål, man må stille sig, er tæt forbundet med det første. Hvis vi kan konstatere, at vores beskyttelsesobjekt er ”mennesker og værdi inden for staten Danmarks interessesfære”, hvad opfatter vi så som essentielle funktioner, der skal beskyttes? Mulighed for at kommunikere, adgang til elektricitet, et nogenlunde velfungerende monetært system, fødevareforsyning og -sikkerhed, et tilgængeligt sundhedsvæsen og mulighed for at blive transporteret til og fra arbejde kan vi givet hurtigt blive enige om er centrale funktioner, der understøtter og muliggør hverdags- og arbejdslivet i Danmark.

Langt mere kompliceret bliver det at diskutere, f.eks. i hvilket omfang mere abstrakte funktioner som tryghed, demokrati eller adgang til information er vitalt for borgere i Danmark. I den norske definition af kritisk infrastruktur tilgodeses borgernes tryghed således eksplicit – men hvilke afledte samfundsfunktioner er omfattet heraf? Omfatter dette alene opretholdelsen af politi og retsvæsen eller måske også en mindre konkret følelse af tryghed – f.eks. opretholdelsen af et slagkraftigt forsvar i fredstid eller for den sags skyld gadebelysning om natten?

I sidste ende forbliver dette et spørgsmål, der bør, og skal, overlades til det højest mulige politiske niveau, som det også gøres i forbindelse med dimensionering af det kommunale beredskab.[55]

Uden et sådant klart politisk mandat lader spørgsmålet sig ikke nemt afklare i grænsetilfælde. Mere end noget andet bliver dette altså et spørgsmål om, hvilket generelt serviceniveau staten ønsker at garantere sine borgere i krisetider.

Iboende i begrebet kritisk infrastruktur er altså en generel politisk prioritering, der fastlægger grænsen imellem kritiske og ikkekritiske tab. Udover den ovenfor nævnte funktionelle fastlæggelse af "statsligt serviceniveau" er en konkret skalering af disse servicer dog også nødvendig; sagt med andre ord må selv kritiske funktioner i deres implementering være underlagt en politisk proportionalitet, som forudsætter en fælles forståelse af en smertegrænse for samfundstab (både funktionstab og materielle tab). Der må altså sondres mellem kritikalitet i form af abstrakt funktionalitet og kritikalitet som konkret, situationsbestemt fænomen.

Selvom der næppe kan sættes spørgsmålstegn ved, at elektricitet meget hurtigt ville komme igennem de første normative lag (eksempelvis: beboere i Danmark, der skal understøttes med adgang til elektricitet), betyder dette jo ikke automatisk, at alle afbrydelser af strømmen i Danmark er anslag imod vores kritiske infrastruktur. For at kunne arbejde effektivt med denne sondring forudsætter det altså, at alle involverede myndigheder er udstyret med et begrebsapparat og kendskab til et værdihierarki, der gør dem i stand til konkret at afveje sådanne situationer – og muligvis forudgående diskussioner af, hvornår noget bliver kritisk.

Helt konkret: Er det kritisk, at 10 % af Danmark er uden strøm i en time, eller at dele af Danmark er uden strøm i to dage? I forsøget på, på forhånd, at trække denne usynlig smertegrænse fremkommer nogle virkelig vanskelige politiske prioriteringer. Imens man med

hensyn til at besvare, hvem man beskytter, og hvilke funktioner disse beskyttelsesobjekter skal have adgang til, kan bevare en overordnet afstandstagen til komplicerede politiske og moralske dilemmaer, må man, for at det bliver et effektivt instrument, også have en ide om, hvor langt denne beskyttelse rækker.

Den situationsbestemte kritikalitet kunne tilgås via en række parametre eller indikatorer. Først og fremmest: Hvor mange berøres (eller hvor stor en del af landet) og i hvilket omfang? Internetadgang er en kritisk funktion i Danmark, men fordi en kommune er uden internet i tre dage, bliver det ikke nødvendigvis automatisk kritisk for Danmark. Eller sagt på en anden måde, selv hvis vi konstaterer, at en given funktion er vital for indbyggere i Danmark, er denne vitalitet underlagt en nedre bagatelgrænse eller mere præcist en relationel proportionalitet i forhold til antallet af berørte eller udstrækningen af sammenbruddet. I identifikationen af kritisk infrastruktur arbejder de britiske myndigheder med en såkaldt kritikalitetsskala, der indeholder tre "impact dimensions": levering af essentielle nationale services, økonomisk tab og tab af liv.[56] Sådanne indikatorer bør overvejes og diskuteres på det højest mulige politiske niveau.

Hertil kommer overvejelser over, hvor kritisk eller sårbart et givent stykke infrastruktur er i relation til andre stykker infrastruktur. Imens det således isoleret set kunne være uden den store betydning at være uden strøm en dag, forholder det sig anderledes, hvis dette betyder overbelastning af telefonnet eller transportnet eller medfører sammenbrud af generatorer på hospitaler. Altså vil, som omtalt i afsnit 2.3, et sammenbrud i elnettet ofte have implikationer langt udover selve elnettet.

Endelig, ud fra et sikkerhedspolitisk perspektiv, vil en række trusler i sig selv ikke være kritiske, men indeholde eskalationspotentialer, og må derfor fortsat prioriteres. Dette bekymrer i særdeleshed, når det gælder cyberspace. Det nuværende trusselsbillede giver således umiddelbart anledning til relativt få beredskabssituationer, men langt flere små anslag, som næppe i klassisk forstand kan betragtes som anslag imod vores kritiske infrastruktur. Kritisk infrastruktur kan altså her blive en forhindring for at se en løbende erodering af samfundets sikkerhed. F.eks. igennem systematisk undergravning af vores informationssikkerhedsstruktur. Imens det næppe er et kritisk anslag imod vores infrastruktur, at kinesiske myndigheder skaffer sig adgang til Fødevarestyrelsens forhandlingsmandater forud for en WTO-konference, kan dette få meget store økonomiske og organisatoriske konsekvenser for Danmark på længere sigt.

Samlet set er der en række grundlæggende politiske, og givet ret inopportune, samfundsspørgsmål, der skal være klarlagt, før man succesfuldt kan opstille en operationel model for indkredsningen af kritisk infrastruktur, og jo klarere disse politiske mandater er, des bedre er det for de underliggende beslutninger. Imens en række af disse normative værdier muligvis kan udledes af eksisterende politiske strukturer og -beslutninger, vil særligt grænsetilfælde næppe kunne udledes af andet end eksplicitte politiske prioriteringer.

Dette giver anledning til at genoverveje hensigtsmæssigheden af at anvende begrebet kritisk infrastruktur i fastlæggelsen af GovCERT's arbejdsområde. Begrebet har muligvis for mange variable, og for lille et anvendelsesområde, til at kunne tjene som et hensigtsmæssigt begreb i cybersammenhæng. For mere effektivt at kunne afgøre dette forsøger vi i det følgende afsnit at opliste nogle af de sikkerhedsmæssige udfordringer, der knytter sig til cyberspace – uden dog at behandle de specifikke responsmuligheder, det danske forsvar har, for alene at fokusere på den processuelle håndtering.

4. Eskalationsscenarier og cyberwarfare

Begrebet kritisk infrastruktur bringes ofte i anvendelse som en meget fast kategori identificeret ud fra det sociale system enten ved at etablere et værdihierarki eller ved at kortlægge infrastrukturen. Disse anvendelsesformer er dog som allerede omtalt vanskeliggjort af det moderne samfunds øgede kompleksitet. De to modsatrettede diskurser om kritisk infrastruktur, vi løbende har diskuteret, at den kritiske infrastruktur på en og samme tid bliver henholdsvis mere udsat og mindre udsat, understøttes af de perspektiver, som kritisk infrastruktur kan anskues ud fra.

Følger man en militærstrategisk diskurs, identificeres kritisk infrastruktur altså ud fra muligheder for at skade Danmark og derved øge effektiviteten ved et angreb, er det fortsat muligt at identificere sådanne sårbare nøglepunkter, selvom infrastrukturen bliver tættere koblet og mere kompleks. Hvis man derimod, følgende en civil diskurs, tager udgangspunkt i selve systemets evne til at modstå angreb af en hvilken som helst karakter, bliver forudgående analyser og identifikation enten meget komplicerede eller umulige. Disse diskurser ses også i allerhøjeste grad afspejlet i de forskellige institutionelle sammenhænge, hvor begrebet kritisk infrastruktur bringes i anvendelse. Imens civile beredskabsmyndigheder tager afstand fra begrebet som et énstrenget styringsværktøj, er begrebet fortsat af allerstørste relevans for militære aktører inden for feltet.

Dette gør en koordination af civile og militære myndigheders samarbejde endog meget svært, da de helt basalt set ikke har et fælles udgangspunkt endsige en fælles referenceramme.

Denne rapports udgangspunkt er sikkerhedspolitisk. Derfor udforsker resten af rapporten en måde, man kan arbejde militært med kritisk infrastruktur på ved hjælp af scenariebaseret modellering og øget koordination imellem de forskellige aktører. Med scenariebaseret modellering – eller med et andet ord øvelser – kan man på den ene side tilgodese det militære behov for at tænke strategisk over samfundets forsvar og på den anden side undgå de civile undsigelser. For at kunne gøre dette undersøger vi de særlige udfordringer, der knytter sig til at håndtere cyberbaserede trusler imod kritisk infrastruktur, og ser på de strategiske overvejelser, man bør gøre sig, når en konflikt i cyberspace skal forstås i traditionelle militærstrategiske termer.

I yderste konsekvens, i det militærstrategiske spektrum inden for cyberwarfare[57], er der mulighed for et militært offensivt modsvar på en intervention i cyberspace – enten som nation

eller som en del af en alliance. Cyberangrebet på Estland i 2007, der var en tre uger lang serie af DDOS-angreb (distributed denial of service-angreb) på estisk infrastruktur, angiveligt udført på foranledning af Rusland, demonstrerede potentialet ved sådanne interventioner i cyberspace. Angrebet viste dog også en høj tærskel for, hvornår en intervention medfører anvendelse af modoffensive foranstaltninger, idet hverken Estland eller NATO anså angrebet som hørende under Atlantpagtens artikel 5 ("musketereden").[58] Men under alle omstændigheder peger dette på, at en nation må forberede sig på, at militær respons efter omstændighederne kan komme i spil.

På et mere sandsynligt, og mindre intensivt, trin på eskalationsstigen nødvendiggør forskellige incitamenter en definition af de civil-militære relationer. NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) anfører blandt andet i sin *National Cyber Secyrity Framework Manual*[59] forskellige motivationer for henholdsvis civile politimyndigheder og militære efterretningstjenester. Den civile myndighed vil ofte være tilbøjelig til at eksponere et angreb og en modus med henblik på at forhindre yderligere angreb samt have et fokus på efterforskning til brug i strafferetslig sammenhæng. For den militære efterretningstjeneste kan det efter omstændighederne forholde sig anderledes. Her kan der ofte være behov for en høj grad af hemmeligholdelse for blandt andet at beskytte kilder eller for på et senere tidspunkt at kunne afdække eller angribe mere betydningsfulde bagvedliggende strukturer. Eller mere vidtgående at undlade at eksponere et angreb for senere selv at kunne anvende samme modus offensivt – eksempelvis som en del af et såkaldt aktivt forsvar i erkendelse af, at et komplet og fuldstændigt reaktivt cyberforsvar ikke er muligt. Dette peger således også på nødvendigheden af at definere civil eller militær kontrol.

Helt firkantet kan man sige, at inddæmningen og reparationen af skader – indsatsen, som svarer til brandslukning – kan klares inden for den nuværende beredskabsstruktur med politiet for bordenden, men sagen er ganske anderledes, hvis regeringen beslutter, at der skal udføres et modangreb, eller hvis anslaget i øvrigt har militærstrategisk betydning. Her vil den almindelige krisestruktur skulle fortsætte med bekæmpelsen og udbedringen af skaderne, mens den militære struktur vil forventes at overtage ledelsen. Dette punkt kan være meget svært at definere, hvorfor det skal trænes.

4.1 Eskalationer og cyberspace

En 15-årig dreng kan i princippet sidde fysisk i Pakistan og gennemføre en intervention i dansk infrastruktur – via cyberspace – med endog meget stor effekt. Imens dette scenariums

relevans er tvivlsomt i praksis, er det utvivlsomt med til at øge den diskrepans imellem militære og civile aktører i cyberspace, som vi oplever i disse år.

En række af de anslag, vi faktisk oplever imod Danmark i cyberspace, ligger således i et grænseland imellem kriminelle handlinger, terrorhandlinger og handlinger, der sker på foranledning af en fremmed stat og således er at betragte som fjendtlige handlinger imod staten Danmark. Dette øger kravet om en klar organisationsstruktur og scenariebaseret træning og fordrer en høj grad af C2 på cyberområdet.

Uanset om angrebet retter sig imod en offentlig myndighed eller en privat virksomhed, vil den umiddelbare reaktive imødegåelse af interventionen i cyberspace muligvis være den samme – men der rejser sig alligevel et spørgsmål om, hvem der har ansvaret for inddæmning og håndtering af truslen, og hvilke yderligere responsmuligheder der knytter sig til den enkelte aktør. Disse responsmuligheder kan blandt andet være betinget af, hvor angriberen kan indplaceres i spektret fra almindelig kriminalitet – over spionage og terror – til en de facto militær trussel eller konflikt. Altså en model, der indarbejder proportionel eskalation fra hjemmecomputeren til GovCERT.

4.2 Eskalationsteori

Hermann Kahns eskalationsteori indeholder en model for, hvordan en traditionel konflikt kan udvikle sig, eller hvad vi kunne kalde en taksonomi for en eskalerende konflikt. Ifølge Kahn følger udviklingen af en konflikt ofte en særlig progression. Han beskriver dette igennem scenarier indplaceret på en eskalationsstige, hvor eskalationen kan udvikle sig på mindst tre forskellige måder – her betegnet som x, y og z.[60]

X betegner en måde, hvorpå en konflikt eskaleres, ved at modstanderen øger intensiteten kvantitativt. Traditionelt kan dette være fysisk angreb på logistiske forbindelseslinjer eller overgang til brug af taktiske nukleare våben. Drages en parallel til nutidens cyberspace og kritisk infrastruktur, kan dette eksempelvis være en forøgelse af DDOS-angreb imod et stykke kritisk infrastruktur eller udbredelse af angrebet til flere infrastrukturelle sektorer. I korte træk dækker x altså over, at fjenden intensiverer sit allerede igangværende angreb.

Y forøger konflikten geografisk. Traditionelt kan dette være en udvidelse af det militære operationsområde. I en cyberkontekst kunne konflikten således udbredes fra alene at ramme infrastruktur i hovedstaden til at involvere resten af landet.

Endelig betegner z en såkaldt forbundet eskalation, hvor også alliancepartnere bliver involveret, hvilket traditionelt for Danmark kan omfatte angreb på et andet NATO-land. I cyberspace kan dette være angreb på servere, der er placeret i nabolande, som har betydning for både Danmarks og leverandørlandets infrastruktur.

Figur 2: Eksempler på eskalationsmåder i scenarier

	Traditionelt angreb	**Cyberangreb**
Type x: Kvantitativ øgning af intensiteten	Fysisk angreb på logistiske forbindelseslinjer eller brug af taktiske nukleare våben	Forøgelse af DDOS-angreb på et stykke infrastruktur eller udvidelse til andre sektorer
Type y: Geospatial udvidelse	Progressiv udvidelse af operationsområdet til hele Danmark	Udvidelse af angreb på infrastruktur fra landsdel til hele landet
Type z: Forbundet eskalation	Angreb på et andet NATO-land som en del af angrebet imod Danmark	Angreb på servere i naboland, som er kritisk for Danmark og leverandørland

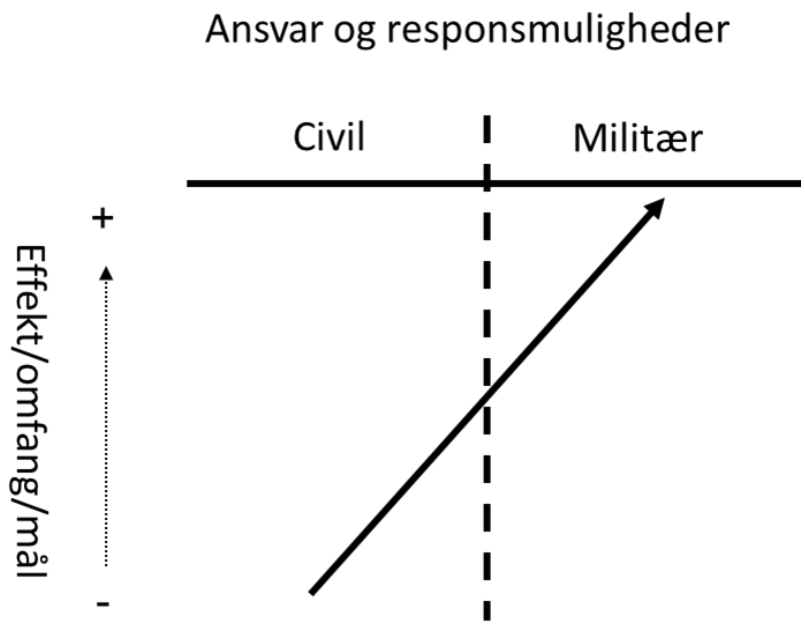
4.3 Overgang mellem civil og militær kontrol

Disse forskellige måder, hvorpå en konflikt kan udvikle sig, vil i princippet kunne føre til en kæde af begivenheder, der scenarieafhængigt kan indplaceres og gradueres på en eskalationsstige – det klassiske eksempel er Cuba-krisen i 1962 – der igen ville give mulighed for identifikation af ansvar og responsmuligheder for henholdsvis private virksomheder, civile myndigheder og militæret.

Et eksempel på et nutidigt eskalerende angreb i cyberspace, der både spredte sig over flere sektorers infrastruktur og skiftede fra civilt til militært mål, blev identificeret i Sydkorea 20. marts 2013.[61] Angrebet, der indledningsvis blev kaldt Dark Seoul, ramte den finansielle sektor hårdt – med sletning af indholdet på titusindvis af computerharddiske til følge. Det, man indledningsvis troede var en kriminel handling imod pengeautomater, viste sig dog at have en helt anden og militær dagsorden. En senere analyse af angrebet – efterfølgende benævnt Operation Troy – viste, at angriberen i virkeligheden havde fremstillet malware, der anvendte søgeord såsom våben, forsvar, artilleri og øvelser på højere niveau m.v., med henblik på at skaffe sig adgang til og informationer fra vigtige militære computere via den civile infrastruktur. Hvad der dermed umiddelbart virkede som en kriminel handling imod den finansielle infrastruktur, havde således i virkeligheden været et forsøg på et angreb i den militære arena, hvilket således også medfører, at ansvaret flyttes fra det civile til det militære domæne. Det forhold, at Operation Troy vurderes at være udført af en hackergruppering

kaldet The New Romtanic Cyber Army Team[62] viser endvidere, at selv tilsyneladende uafhængige hackere kan have endog meget stor effekt på et lands infrastruktur, hvis de har de nødvendige evner og ressourcer.

Figur 3: Eskalation (modus x, y eller z eller kombination)



Figur 3 viser således en eskalation, hvor omfanget, målet eller effekten af en intervention udvider graden af proportionalitet i responsmuligheder. I praksis vil det dog ofte være vanskeligt at definere den præcise grænse eller "red line", hvor egentlige militære optioner kan blive en realitet. Dette forhold er også erkendt i en rapport fra den britiske Defence Committee om cybertrusler imod det britiske militærs it-infrastruktur, hvor professor i international sikkerhed Paul Cornish betegner cybertruslers natur som:

> "blurred between military and civilian, and between the physical and the virtual; power can be exerted by states or non-state actors, or by proxy. Cyberspace has made it possible for non-state actors, commercial organizations and even individuals to acquire the means and motivation for warlike activity. "[63]

Eskalationsteorien[64] giver således ikke et entydigt svar på, hvornår et cyberangreb på infrastruktur er et anliggende for de militære kapaciteter, men peger derimod på udvikling af scenarier, der indeholder forskellige kombinationsmuligheder – til brug for diskussion og udvikling af mekanismer og tærskler – for derigennem at forbedre mulighederne for at navigere i en kommende konflikt.

En sådan dimensionering og diskussion af responsmuligheder kan udvikles igennem scenarie-baseret træning, øget koordination og løbende evaluering på baggrund heraf. Samtidig vil dette give større rutine i forhold vedrørende det vanskelige C2-aspekt, der efter omstændighederne omfatter forskellige myndigheder med forskellig institutionel kultur. Med andre ord skal man gennemføre øvelser baseret på scenarier, hvor samarbejde imellem civile og militære myndigheder og organisationer trænes, og hvor overgang fra civil til militær kontrol belyses og trænes.

I rapporten om terroranslagene i Oslo og på Utøya 22. juli 2011 var nogle af arbejdsgruppens observationer og konklusioner, at der på ledelsesniveau var en manglende evne til at afklare ansvar, en manglende evne til koordination og interaktion samt en for ringe evne til at tage ved lære af de øvelsesaktiviteter, der var gennemført.[65] Helt konkret lyder rapportens anbefalinger:

> ”Tragedien 22/7 avdekker behov for mange slags endringer: i planverk og regler, i disponering av kompetanse og ressurser, i organisasjonskultur, prioriteringer og fokus, ja, til og med i samfunnets holdninger. … Der det sviktet, skyldtes det primært at:
>
> - Evnen til å erkjenne risiko og ta lærdom av øvelser har vært for liten.
> - Evnen til å gjennomføre det man har bestemt seg for, og til å bruke planene man har utviklet, har vært for svak.
> - Evnen til å koordinere og samhandle har vært mangelfull.
> - Potensialet i informasjons- og kommunikasjonsteknologi har ikke vært godt nok utnyttet.
> - Ledelsens evne og vilje til å klargjøre ansvar, etablere mål og treffe tiltak for å oppnå resultater har vært utilstrekkelig.
>
> Etter kommisjonens mening handler disse lærdommene i større grad om ledelse, samhandling, kultur og holdninger – enn mangel på ressurser, behov for ny lovgivning, organisering eller store verdivalg.”[66]

Det betyder, at man i høj grad bør lægge vægt på en såkaldt beredskabskultur, hvor de enkelte organisationer skal bevidstgøre deres egne ansatte om organisationens del af beredskab og/ eller kritisk infrastruktur.

I den førnævnte britiske rapport udtrykkes der ligeledes bekymring for, at det på strategisk niveau er uklart, hvem der har ansvaret, hvis landet kommer under vedvarende cyberangreb, og at dette blandt andet bør adresseres gennem policy.[67] Dette peger således på, at ikke alene skal der gennemføres øvelser, men der skal også være stor tyngde i læringen fra disse øvelser – på både strategisk og operativt niveau. Endvidere indikerer de britiske og norske observationer, at der er et behov for koordinationsfora på disse niveauer.

Som eksemplerne fra cyberspace også viser, er den traditionelle trinbaserede eskalation generelt udfordret. Den traditionelle fysiske verden er begrænset af faktorer såsom mandskab og materiel, der skal dedikeres og bevæges i tid og rum. I cyberspace kan forskydninger i anslagets tyngde derimod ske meget intenst og således trinløst. Dette vanskeliggør også dimensioneringen af forsvaret alene ud fra det aktuelle trusselsbillede, da udviklinger kan ske meget hurtigt. Hvis Kina kan beslutte sig for at ødelægge Danmark, og beslutningen tre timer senere resulterer i en fuldstændig strømafbrydelse i hele landet, forskyder dette ikke kun en række militærstrategiske akser, men også måden, vi kan og bør betragte beskyttelsen af kritiske funktioner i vores samfund på. Til dette skal dog tilføjes, at de bagvedliggende beslutningsprocesser imidlertid ikke kan sættes op i tempo.

Ydermere er eskalationsmodellen udfordret af, at anslag i cyberspace ikke altid medfører en eskalation i traditionel forstand. Der er således i dag mulighed for at udføre statsfjendtlig og undergravende virksomhed som f.eks. mild sabotage, storstilet spionage eller endda alvorlig sabotage, uden at dette medfører en eskalation i egentlig militær forstand. Således åbner cyberspace op for at udføre storstilet statsfjendtlig virksomhed, som ikke i traditionel forstand udgør et angreb, men som har meget store konsekvenser for de berørte stater. Dette kunne f.eks. være ved at skaffe sig adgang til statshemmeligheder, industrielle design eller forestående virksomhedsaftaler. Sabotageoperationer kan også udføres langt mere subtilt i cyberspace i operationer, der gør det vanskeligt at spore sabotøren, eller hvor effekten indtræffer, lang tid efter at sabotøren har været inde i systemet. GovCERT påpeger således, at risikoen for denne type fjendtlige aktioner er langt mere sandsynlig, og allerede forekommende, end såkaldte beredskabssituationer, hvor forsvars- og beredskabskapaciteter umiddelbart bringes i spil.

En vigtig indsigt i at skabe et effektivt forsvar i cyberspace er altså, at hovedparten af de aktiviteter, vi vil forhindre, ikke falder under et militært mandat. Der er såvel civile, private og offentlige som militære operatører.

I forbindelse med det tidligere nævnte hackerangreb imod CPR-registret i Danmark udtalte Politiets Efterretningstjeneste (PET), at man nu vil oprette en særlig cybersektion til håndtering af denne type anslag imod Danmark,[68] som vil blive placeret i PET's operative afdeling.[69] Dette tiltag vil betyde, at endnu en aktør med ansvar for cybersikkerhed introduceres.

Der ligger en betydelig udfordring i at skabe en velfungerende, løbende koordination om ansvarsfordeling mellem myndigheder – i dag ikke mindst PET's nye cybersektion, Rigspolitiets afdeling for efterforskning af IT-kriminalitet og Forsvarets Efterretningstjenestes Center for Cybersikkerhed. Denne udfordring skal på den ene side imødegås ved at øge koordinationen og på den anden side tilgodese den sårbarhed, som alle sådanne C2-aspekter medfører.

Helt i tråd med dette anbefalede IT- og Telestyrelsen allerede i 2007[70] i forbindelse med etableringen af GovCERT følgende:

- Højnelse af den enkelte aktørs beredskab
- Sikring af rettidig information og koordination mod fælles problemer.

Disse anbefalinger baserer sig ikke mindst på styrelsens udredning af de mange forskelligartede aktører, der alle har et medansvar for internetsikkerheden i Danmark. En enstrenget sikkerhedsorganisation er i dag ikke mulig i lyset af cyberspaces fuldstændige integration i vores samfund og således ikke hensigtsmæssig at planlægge efter. I stedet kan scenariebaserede øvelser, der involverer alle relevante aktører, bidrage til løbende afklaring af ansvarsområder imellem disse og dermed styrke vores responskapacitet og derved muligheden for at afværge anslag imod kritiske anlæg. Man kunne i denne sammenhæng også overveje forskellige institutionelle mekanismer til øget koordination, f.eks. tværgående koordinationsenheder eller et fast hierarki i tilfælde af en større krise.

Kort opsummeret betyder ovenstående, at der er vanskeligt at identificere en "red line" for, hvornår et angreb er en intervention i traditionel forstand og derfor et militært ansvar og anliggende, og hvornår det er et civilt anliggende. Kritisk infrastruktur som begreb mindsker bestemt ikke denne vanskelighed. For forsvaret betyder dette, at der bør tages udgangspunkt i trusler i sig selv med henblik på en mere generisk imødegåelse af intervention. Disse trusler bør behandles i scenarier med forskellige eskalationsmåder og gradueringer for at give både operationel og strategisk overblik over tærskler for en militær indgriben og proportionalitet –

for så vidt angår strategisk og operationel anvendelse af hele CNO-spektret – men måske især for computer network attacks (CNA'er). Disse scenarier bør udarbejdes under inddragelse af de relevante sektorer og øvrige aktører. I kraft af usikkerheden af både trusselsbilledet og aktørfeltet, der skal imødekomme disse, bør man løbende øve evnen til at koordinere og forhindre anslag imod Danmarks sikkerhed, uagtet om disse anslag vedrører kritisk infrastruktur, og, hvor det er hensigtsmæssigt, overveje at institutionalisere disse. Man bør i denne sammenhæng være opmærksom på den sårbarhed, som nye koordinationsmekanismer automatisk medfører. Koordinationsmekanismerne kommer således i sig selv til at være sårbare.

Således nødvendiggør vanskeligheden i at trække en definitiv linje et øget samarbejde mellem civile og militære aktører. Dette kunne med fordel ske igennem en klart defineret og kohærent organisationsstruktur og en løbende politisk dialog, hvor prioriteterne for beskyttelse løbende korrigeres.

5. Konklusion

Overordnet er der som belyst to sameksisterende, konkurrerende diskurser om den mulige reaktion på samfundets tiltagende kompleksitet. Samtidig er der en militær og en civil diskurs om kritisk infrastruktur. Samlet medfører dette, at der er to diskurser. En, hvor man mener, at man kan identificere kritisk infrastruktur, og en anden, der siger, at samfundet er alt for komplekst til, at det giver mening. Disse to diskurser krydser også hinanden i spørgsmålet om håndteringen af kritisk infrastruktur i cyberspace, men har hver sin logik og hvert sit organisatoriske mål. Dette gør det nærmest umuligt at forene de to synspunkter. Da disse svært forenelige diskurser også vanskeliggør den konkrete håndtering, f.eks. hvornår man skal gå fra civil til militær kontrol over et cyberangreb, skal der arbejdes intenst på at etablere koordinationsmekanismer og øvelser, der involverer civile og militære myndigheder.

Man bør genoverveje hensigtsmæssigheden af at bruge begrebet kritisk infrastruktur som afgrænsning af myndigheders betjeningsområde, i hvert fald indtil en række normative beslutninger har skabt en yderligere udfyldning af begrebet. Endvidere bør man være påpasselig med en direkte applicering af en angelsaksisk doktrin inden for feltet, idet samfundsstrukturerne ikke er analoge og de anglosaksiske forhold dermed ikke umiddelbart lader sig oversætte til danske forhold.

Et komplekst system betyder, at det er tilsvarende komplekst at opstille en klar taksonomi over infrastruktur. Imens man i et industrielt samfund kunne indplacere infrastruktur på en trappestige, der trinvist førte fra ligegyldigt til kritisk, er dette meget vanskeligt i kommunikationssamfundet. Dette betyder omvendt ikke, at man ikke kan gøre sig forestillinger om, hvad der kan være kritisk infrastruktur. Individer eller grupper, der har til hensigt at skade Danmark, vil stadig forsøge at ramme Danmark hårdest muligt med den mindst mulige indsats.

Når Danmark skal forsvares imod terrortrusler eller konventionelle krigstrusler, er det således ikke nødvendigvis hensigtsmæssigt at udføre komplicerede beregninger af, hvilke dele af vores infrastruktur der må betragtes som kritisk for det samlede system. Tværtimod vil disse beregninger i det moderne kommunikationssamfund kunne udgøre en trussel i sig selv, da de potentielt vil være tilgængelige for de selvsamme fjendtlige elementer, hvis angreb de skulle mildne eller imødegå. I stedet bør man arbejde med en forsvarspolitisk model, der afdækker fjendtlige elementers forestilling om, hvad der er kritisk for Danmarks overlevelse. Altså arbejde klassisk scenariebaseret ud fra de data, der er tilgængelige for enhver. I dette arbejde

vil konsultationer med de relevante beredskabssituationer, tværgående øvelser og scenarier kunne styrke samfundets samlede forsvar. Man bør fremdyrke en generel beredskabskultur, så personer, der ikke altid arbejder med beredskab, bliver mere bevidste om deres andel i det samlede beredskab.

Særligt cyberspace udfordrer klassisk militærstrategisk tænkning. Den oversættes således kun vanskeligt til klassiske eskalationsteorier eller anvendelsen af konventionelle krigsmidler. Krigsskuepladsen giver på den ene side mulighed for at erodere et lands informationsinfrastruktur over lang tid og på den anden side mulighed for med et slag at tilføre et land store ødelæggelser uden varsel eller eskalation. Af samme grund bør Danmarks strategiske og operationelle kapacitet i cyberspace styrkes mest muligt. Cyberspace kunne meget vel vise sig at være et af de vigtigste sikkerhedspolitiske område i den nære fremtid – den første forsvarslinje.

Cyberforsvar er i denne sammenhæng relevant ikke kun med hensyn til traditionelle militære trusler, f.eks. som forberedelse af angreb, men i lige så høj grad med hensyn til anslag, som ikke vedrører kritisk infrastruktur i traditionel forstand, f.eks. spionage, og kapaciteter inden for begge områder. Militær og civil koordination er således af afgørende betydning, da disse områder har hvert sit syn på kritisk infrastruktur. Netop fordi det kan være vanskeligt at finde grænsen imellem det civile og militære, fordrer et effektivt forsvar en stor koordinationsindsats og en kohærent organisationsstruktur. Særligt dette aspekt kunne med fordel styrkes igennem tværgående scenariebaserede øvelser, med stor vægtning af forhold, der vedrører C2. Disse øvelser skal foregå på såvel operativt som strategisk niveau og etablere en forståelse imellem disse niveauer.

Ved et cyberangreb – cyberwarfare – fra en fremmed stat vil man imidlertid skulle overveje mulig gengældelse. Her vil den civile beredskabsindsats skulle ske underordnet en militær aktivitet, der er rettet imod den formodede angriber. Her vil man overgå til militær kontrol, og dette skal øves, da kravene her kan være i modstrid med ønskerne fra det civile beredskab.

Uanset hvordan man arbejder med kritisk infrastruktur, skal man være sig bevidst, at det involverer en række grundlæggende samfundsspørgsmål, der bør fastlægges igennem klare politiske mandater. Imens en række af disse normative valg muligvis kan udledes af eksisterende politiske strukturer og beslutninger, vil grænsetilfælde næppe kunne afgøres på baggrund af andet end eksplicitte politiske prioriteringer. Man må forsøge at forankre disse beslutninger på det højest mulige politiske og institutionelle niveau, da der er mange

grænsetilfælde. Det anbefales således i endnu højere grad end i dag at skabe en national platform, hvorfra disse vanskelige spørgsmål kan adresseres af politikere og sektorer i fællesskab. Dette gælder således for sikkerhedstænkning i almindelighed og kritisk infrastruktur i særdeleshed.

6. Anbefalinger

Følgende fem anbefalinger opstilles på baggrund af rapportens iagttagelser.

- Forsvaret af Danmark i forhold til cyber network operations-baserede trusler, styrkes gennem tværgående scenariebaserede eskalationsøvelser op til strategisk niveau med henblik på at belyse, hvor grænsen er imellem civile og militære trusler, og hvornår og hvordan militære cyberkapaciteter skal indsættes.

- Koordinationen imellem de forskellige civile og militære aktører, der aktivt arbejder med cyber network operations-trusler, styrkes. Dette sker næppe ved etablering af flere myndigheder.

- Beredskabsmyndighedernes pragmatiske tilgang til forståelsen af kritisk infrastruktur skal fastholdes, imens forsvaret samtidig bibeholder sit fokus på konkret kritisk infrastruktur.

- Man bør overveje hensigtsmæssigheden af begrebet kritisk infrastruktur for så vidt angår GovCERT's betjeningsområde, når retsgrundlaget for tjenesten genovervejes.

- Man skal ophøre med direkte sammenligninger mellem en angelsaksisk diskussion om kritisk infrastruktur og en dansk. En række forskelle i samfundsmodellerne besværliggør en sådan sammenligning, og samlet set er Danmark et langt mere robust samfund end de angelsaksiske.

Litteraturliste

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

Beredskabsstyrelsen (2013), *Nationalt Risikobillede* (Birkerød: Beredskabsstyrelsen).

Boin, Arjen og McConnell, Allan (2007), 'Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resillience', *Journal of Contingencies and Crisis Management,* 15 (1), p. 50-59.

Breitenbauch, Henrik Ø. (2012), *Beredskab eller intern sikkerhed? Danmark og den internatinale institutionsudvikling inden for det robuste og sikre samfund* (København: Center for Militære Studier).

Cornish, Paul et al. (2011), *Cyber Security and the UK's Critical National Infrastructure* (London: Chatham House (The Royal Institute of International Affairs)).

Henriksen, Anders (2012), *Cyberkrig. Folkeretten og computer network operations* (København: Center for Militære Studier).

Holst, Sara Helene og Hansen, Ditte Bergholdt (2004), *Håndbog i risikobaseret dimensionering* (Birkerød: Beredskabsstyrelsen).

Kahn, Herman (1965), *On Escalation* (London: The Pall Mall Press Limited).

Lewis, Ted G. (2006), *Critical Infrastructure Protection in Homeland Security. Defending A Networked Nation* (New Jersey: Wiley).

Moteff, John, Copeland, Claudia og Fischer, John (2003), 'Critical Infrastructures: What Makes an Infrastructure Critical', *Report for Congress* (Washington DC: Congressional Research Service, The Library of Congress).

Murray, Alan T. og Grubesic, Tony H. (eds.) (2007a), *Critical Infrastructure. Reliability and Vulnerability* (New York: Springer).

Murray, Alan T. og Grubesic, Tony H. (2007b), 'Overview of Reliability and Vulnerabilty in Critical Infrastructure', in Alan T. Murray and Tony H. Grubesic (eds.), *Critical Infrastructure. Reliability and Vulnerability* (New York: Springer).

Office, Cabinet (2010), 'Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards', in Natural Hazards Team Cabinet Office (ed.) (London).

Pederson, P. et al. (2006), *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and Internatioanl Research* (Idaho: Idaho National Laboratory).

Rinaldi, S.M., Peerenboom, J.P. og Kelly, T.K. (2001), 'Identifying, understanding, and analysing critical interdependencies', *Control Systems, IEEE,* 21 (6).

Schintler, Laurie Anne et al. (2007), ’Moving from Protection to Resilliency: A Path to Securing Critical Infrastructure’, *Critical Infrastructure. Reliability and Vulnerability* (New York: Springer).

Sakerhet i en ny tid (2001), SOU, 201: 41 (Stockholm: Fritzes Offentliga Publikationer).

Sood, Aditya K. og Enbody, Richard J. (2013), ’Crimeware-as-a-service – A survey of commoditized crimeware in the underground market’, *International Journal of Critical Infrastructure Protection*.

Taleb, Nassim Nicholas (2010), *The Black Swan* (London; New York: Penguin Books).

Taleb, Nassim Nicholas (2012), *Antifragile* (New York: Random House).

Bilag: Lov om GovCERT

Lov om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v.

VI MARGRETHE DEN ANDEN, af Guds Nåde Danmarks Dronning, gør vitterligt:

Folketinget har vedtaget og Vi ved Vort samtykke stadfæstet følgende lov:

§ 1. Loven finder anvendelse på IT- og Telestyrelsens behandling af personoplysninger, som er indeholdt i pakke- og trafikdata, ved driften af den statslige varslingstjeneste for internettrusler.

§ 2. Kommuner og regioner samt private virksomheder, som er beskæftiget med kritisk infrastruktur, kan efter anmodning blive tilsluttet den statslige varslingstjeneste for internettrusler.

Stk. 2. Ministeren for videnskab, teknologi og udvikling kan fastsætte nærmere regler for de i stk. 1 nævnte myndigheders og private virksomheders tilslutning til den statslige varslingstjeneste for internettrusler, herunder regler om betaling af gebyr.

§ 3. I denne lov forstås ved:

1) *Pakkedata:* Indholdet af internetbaseret kommunikation.

2) *Trafikdata:* Data, som behandles med henblik på overførsel af pakkedata.

3) *Sikkerhedshændelse:* Hændelse, der påvirker tilgængelighed, integritet eller fortrolighed af information eller tjenester på internettet.

§ 4. Som led i driften af den statslige varslingstjeneste for internettrusler behandler, herunder indsamler, registrerer, analyserer og opbevarer, IT- og Telestyrelsen uden retskendelse tilsluttede myndigheders og private virksomheders ind- og udgående pakke- og trafikdata. Pakkedata må dog kun analyseres ved begrundet mistanke om en stedfunden eller forventet sikkerhedshændelse, og kun i det omfang det er nødvendigt for at gennemføre den pågældende analyse.

Stk. 2. Registrerede pakke- og trafikdata som nævnt i stk. 1 slettes, når formålet med behandlingen er opfyldt.

Stk. 3. Uanset at formålet med behandlingen ikke er opfyldt, kan

1) pakke- og trafikdata, der knytter sig til en sikkerhedshændelse, højst opbevares i 3 år,

2) pakkedata, der ikke knytter sig til en sikkerhedshændelse, højst opbevares i 14 dage og

3) trafikdata, der ikke knytter sig til en sikkerhedshændelse, højst opbevares i 12 måneder.

Stk. 4. Fristerne i stk. 3, nr. 1-3, regnes fra tidspunktet for registreringen af de pågældende data i den statslige varslingstjeneste.

Stk. 5. Ministeren for videnskab, teknologi og udvikling kan fastsætte nærmere regler for den i stk. 1 nævnte behandling af pakke- og trafikdata.

§ 5. § 35 i lov om behandling af personoplysninger finder ikke anvendelse på den statslige varslingstjeneste for internettruslers behandling af personoplysninger.

Stk. 2. Personer, der virker inden for den statslige varslingstjeneste for internettrusler, har tavshedspligt, jf. straffelovens § 152, jf. § 152 a-e, med hensyn til oplysninger, som de gennem deres virksomhed i varslingstjenesten får kendskab til, jf. dog § 6.

§ 6. Data, der behandles som led i den statslige varslingstjenestes aktiviteter, kan kun videregives i følgende tilfælde:

1) Pakke- og trafikdata, der knytter sig til en sikkerhedshændelse, kan videregives til politiet.

2) Pakkedata, der knytter sig til en sikkerhedshændelse, kan videregives til Forsvarets Efterretningstjenestes militære CERT, hvor IT- og Telestyrelsen skønner det nødvendigt for at beskytte nationale digitale infrastrukturer mod sikkerhedsmæssige trusler. Forsvarets Efterretningstjeneste behandler, herunder sletter og opbevarer, disse data i overensstemmelse med bestemmelserne i § 4.

3) Trafikdata kan, hvor dette er nødvendigt i henhold til varslingstjenestens formål og aktiviteter, videregives til danske myndigheder, tilsluttede private virksomheder og tilsvarende varslingstjenester i andre lande.

§ 7. Ministeren for videnskab, teknologi og udvikling nedsætter et uafhængigt tilsyn, der følger den statslige varslingstjeneste for internettruslers virksomhed.

Stk. 2. Tilsynet består af en jurist som formand og 4 sagkyndige medlemmer. Formanden og medlemmerne beskikkes af ministeren for videnskab, teknologi og udvikling. Ministeren for videnskab, teknologi og udvikling skal ved beskikkelsen af medlemmerne lægge vægt på, at tilsynet samlet repræsenterer juridisk, it-revisionsmæssig og sikkerhedsmæssig sagkundskab.

Stk. 3. Formanden og medlemmerne beskikkes for 4 år ad gangen og kan genbeskikkes.

Stk. 4. Ministeren for videnskab, teknologi og udvikling fastsætter nærmere regler for tilsynets virksomhed. Ministeren for videnskab, teknologi og udvikling kan herunder beslutte, at tilsynet skal udarbejde en årsberetning om den statslige varslingstjeneste for internettruslers virksomhed.

Stk. 5. IT- og Telestyrelsen stiller sekretariatsbistand til rådighed for tilsynet.

Stk. 6. Staten afholder alle udgifter ved tilsynets virksomhed.

§ 8. Ministeren for videnskab, teknologi og udvikling kan bemyndige en under ministeriet oprettet statslig myndighed eller efter forhandling med vedkommende minister andre statslige myndigheder til at udøve de beføjelser, der i denne lov er tillagt ministeren for videnskab, teknologi og udvikling.

Stk. 2. Ministeren for videnskab, teknologi og udvikling kan fastsætte regler om adgangen til at påklage afgørelser, der er truffet i henhold til bemyndigelse efter stk. 1, herunder om, at afgørelserne ikke skal kunne påklages.

Stk. 3. Ministeren for videnskab, teknologi og udvikling kan fastsætte regler om udøvelsen af de beføjelser, som en anden statslig myndighed efter forhandling med vedkommende minister bliver bemyndiget til at udøve efter stk. 1.

§ 9. Ministeren for videnskab, teknologi og udvikling skal senest 3 år efter denne lovs ikrafttræden give Folketinget en skriftlig redegørelse på baggrund af en evaluering af den statslige varslingstjeneste for internettrusler og dens virksomhed.

§ 10. Loven træder i kraft den 1. juli 2011.

§ 11. Loven gælder ikke for Færøerne og Grønland.

Givet på Christiansborg Slot, den 14. juni 2011

Under Vor Kongelige Hånd og Segl

MARGRETHE R.

/ Charlotte Sahl-Madsen

Noter

[1] Se således også John Moteff, Claudia Copeland og John Fischer (2003), 'Critical Infrastructures: What Makes an Infrastructure Critical', *Report for Congress* (Washington DC: Congressional Research Service The Library of Congress), p. 11 f. Dette er en gammel sandhed, se f.eks. Nassim Nicholas Taleb (2012) *Antifragile* (New York: Random House) p. 34.

[2] Se sammenlignende Paul Cornish et al. (2011), 'Cyber Security and the Uk's Critical National Infrastructure', (London: Chatham House (The Royal Institute of International Affairs)), p. viii.

[3] Den konkrete årsag er ifølge energinet.dk en "dobbelt samleskinnefejl på en koblingsstation i Sydsverige", se http://energinet.dk/DA/El/Stroemafbrydelse/Tidligere-stroemafbrydelser/Sider/Tidligere-stroemafbrydelser.aspx (sidst besøgt 5. juni – 2013). Til dette eksempel skal dog tilføjes, at Østdanmark allerede i 1915 blev forbundet med Sydsveriges elforsyning, og det således ikke kan siges at være et moderne eksempel på forbundethed. Dog illustrerer det fint, hvad konsekvenserne af at være forbundet udover landets grænser kan være.

[4] Supervisory control and data acquisition (SCADA) er et computersystem til monitering og kontrol af udstyr eller processer i eks. industrien, telekommunikation, vandværker og energisektoren.

[5] Se Jens Holm: 'Rapport: Sådan kan dansk kritisk infrastruktur hackes', Computerworld, 30. oktober 2012, tilgængelig via http://www.computerworld.dk/art/221498/rapport-saadan-kan-dansk-kritisk-infrastruktur-hackes (sidst besøgt 7. juni 2013). Se også Beredskabsstyrelsen (2013), *Nationalt Risikobillede* (Birkerød: Beredskabsstyrelsen), p. 50.

[6] Ibid., p. 49 f.

[7] Se f.eks. Søren Astrup: 'Datatilsynet: Hackerangreb på cpr-register er meget alvorligt', Politiken.dk, d. 6. juni 2013, tilgængelig via http://politiken.dk/tjek/digitalt/internet/ECE1989749/datatilsynet-hackerangreb-paa-cpr-register-er-meget-alvorligt/ (sidst besøgt 7. juni 2013).

[8] Se f.eks. Ewan MacAskill og Julian Borger: 'New NSA leaks show how US is bugging its European allies', The Guardian, 30. juni 2013, tilgængelig via http://www.guardian.co.uk/world/2013/jun/30/nsa-leaks-us-bugging-european-allies (sidst besøgt 25. juli 2013).

[9] Jens Holm: 'Rapport: Sådan kan dansk kritisk infrastruktur hackes', Computerworld, 30. oktober 2012, tilgængelig via http://www.computerworld.dk/art/221498/rapport-saadan-kan-dansk-kritisk-infrastruktur-hackes (sidst besøgt 7. juni 2013).

[10] Se f.eks. T.S.: 'A cyber-missile aimed at Iran? ', The Economist, 24. september 2010, tilgængelig via http://www.economist.com/blogs/babbage/2010/09/stuxnet_worm (sidst besøgt 25. juli 2013).

[11] Se generelt Henrik Ø. Breitenbauch (2012), *Beredskab eller intern sikkerhed? Danmark og den internatinale institutionsudvikling inden for det robuste og sikre samfund* (København: Center for Militære Studier).

[12] Se Anders Henriksen (2012), *Cyberkrig. Folkeretten og computer network operations* (København: Center for Militære Studier), anbefaling 3, p. 5.

[13] Selv uden særlige IT-kundskaber kan et sådant angreb udføres, se således om markedet for crimeware Aditya K. Sood og Richard J. Enbody (2013), 'Crimeware-as-a-service – A survey of commoditized crimeware in the underground market', *International Journal of Critical Infrastructure Protection*.

[14] CMS' resultatkontrakt 2013, projektnummer 13.7: http://cms.polsci.ku.dk/pdf/Produktionsogydelseeskontrakt2013inklBilag.pdf/.

[15] CMS' projektmanual.

[16] Ted Lewis (2006), p. 34.

[17] The President's Commission on Critical Infrastructure Protection (1996). Se http://www.iwar.org.uk/cip/resources/pccip/summary.pdf.

[18] Sårbarhedsudredningen fra 2004 omtaler således kritisk infrastruktur.

[19] Sårbarhedsudredningen, p. 38.

[20] Lov nr. 596 af 14. juni 2011.

[21] Tjenesten er i dag indarbejdet i den såkaldte FE-lov som en del af Forsvarets Efterretningstjenestes opgaver, lov om Forsvarets Efterretningstjeneste, lov nr. 602 af 12. juni 2013, § 2.

[22] Ved kongelig resolution af 3. oktober 2011 blev "ressortansvaret for sager vedrørende beskyttelse af kritisk it-infrastruktur samt statens varslingstjeneste for internettrusler GovCERT" overført til Forsvarsministeriet.

[23] Almindelige bemærkninger, forslag til lov om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v., 2010/1 LSF 197, bemærkninger til § 2. Denne meget løse definition gengives i bekendtgørelse om vilkår for tilslutning til den statslige varslingstjeneste for internettrusler, BEK nr. 1304 af 17. december 2012, § 2.

[24] Almindelig bemærkninger, forslag til lov om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v., 2010/1 LSF 197.

[25] Kritisk infrastruktur bruges dog som begreb i forbindelse med den seneste ændring i beredskabsloven, se forslag til lov om ændring af beredskabsloven, 2008/1 LSF 54.

[26] Ibid., afsnit 4.

[27] Se f.eks. bemærkninger til § 2, forslag til lov om behandling af personoplysninger ved driften af den statslige varslingstjeneste for internettrusler m.v., 2010/1 LSF 197.

[28] Se f.eks. bekendtgørelse om Energistyrelsens opgaver og beføjelser, BEK nr. 436 af 11. maj 2012, § 7, nr. 1.

[29] Se generelt BEK nr. 765 af 3. august 2005 som ændret ved BEK nr. 872 af 6. juli 2007 om risikobaseret kommunalt redningsberedskab.

[30] Rapporten anvender et mere klassik risikobegreb, for et mere moderne og kontroversielt begreb, se ISO 31000 om risikobaseret ledelse, hvor risiko er defineret som "the effect of uncertainty on objectives", jf. ISO 31000 om risikobaseret ledelse.

[31] Sara Helene Holst og Ditte Bergholdt Hansen (2004), *Håndbog i risikobaseret dimensionerin*g (Birkerød: Beredskabsstyrelsen, p. 12.

[32] Ibid., p. 29.

[33] Se *Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union*, COM (2013), 48 final.

[34] Se ibid., Annex II.

[35] Se her f.eks. den meget funktionelt orienterede håndtering af infrastruktur bestående af notes og links foreslået af Ted Lewis, Ted G. Lewis (2006), *Critical Infrastructure Protection in Homeland Security. Defending a Networked Nation* (New Jersey: Wiley). For en litteraturoversigt, der i højere grad betoner disse netværks kompleksitet, se Laurie Anne Schintler et al. (2007), 'Moving from Protection to Resilliency: A Path to Securing Critical Infrastructure', *Critical Infrastructure. Reliability and Vulnerability* (New York: Springer), p. 297 f.

[36] Se i sin helhed Alan.T. Murray og Tony H. Grubesic (2007a), *Critical Infrastructure. Reliability and Vulnerability* (New York: Springer). Antologien indeholder en række bud på, hvordan man ud fra sårbarhedsanalyser kan modellere kritisk infrastruktur i forhold til specifikke sektorer, herunder transport og elforsyning.

[37] Schintler et al. (2007), *Moving from Protection to Resilliency: A Path to Securing Critical Infrastructure* New York: Springer). Se også Arjen Boin and Allan Mcconnell (2007), 'Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resillience', *Journal of Contingencies and Crisis Management,* 15/1, p. 50-59. Her taler de for helt at opgive den traditionelle krisetænkning i forhold til katastrofale nedbrud af infrastrukturen og i stedet understøtte lokal resiliens. Se også den meget indflydelsesrige filosof og økonom Nassim Nicholas Taleb, særligt Nassim Nicholas Taleb (2010), *The Black Swan* (London; New York: Penguin Books).

[38] Se f.eks. S.M. Rinaldi, J.P. Peerenboom og T.K. Kelly (2001), 'Identifying, Understanding, and Analysing Critical Interdependencies', *Control Systems, IEEE,* 21/6. For et nogenlunde forskningsoverblik se P. Pederson et al., *Critical Infrastructure Interdependency Modeling: A Survey of U.S. And Internatioanl Research* (Idaho: Idaho National Laboratory, 2006).

[39] Rinaldi, Peerenboom og Kelly (2010), 'Identifying, Understanding, and Analysing Critical Interdependencies', *Control Systems, IEEE,* 21/6.

[40] Pederson et al (2006)., *Critical Infrastructure Interdependency Modeling: A Survey of U.S. And Internatioanl Research*, p. 7.

[41] Pederson et al. (2006), p. 5.

[42] Se Ted Lewis (2006), p. 49 ff . og p. 56 f., om udmøntningen af dette.

[43] Om kaskader se Alan .T. Murray og Tony H. Grubesic (2007b), 'Overview of Reliability and Vulnerabilty in Critical Infrastructure', in Alan T. Murray og Tony H. Grubesic (eds.), *Critical Infrastructure. Reliability and Vulnerability* (New York: Springer).

[44] (Perrow 1984, 2007)

[45] Om kaskader se Alan T. Murray og Tony H. Grubesic (2007b), 'Overview of Reliability and Vulnerabilty in Critical Infrastructure', in Alan T. Murray og Tony H. Grubesic (eds.), *Critical Infrastructure. Reliability and Vulnerability* (Springer, 2007b).

[46] Taleb (2012), p. 131.

[47] Taleb (2012), p. 131.

[48] Se rådets direktiv 2008/114/EF af 8. december 2008, inkorporeret i dansk ret ved en række bekendtgørelser. BEK nr. 1461 af 14. december 2010 (jernbaneområdet), BEK nr. 1726 af 22. december 2010 (havneområdet), BEK nr. 7 af 6. januar 2011 (vejområdet), BEK nr. 11 af 7. januar 2011 (energiområdet).

[49] Jf. 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.

[50] http://www.regeringen.se/sb/d/536/a/.

[51] Se *Ett fungerande samhälle i en föränderlig värld*, Publ. Nr MSB 266 – dec. 2011, p. 11.

[52] Ullring et al.: *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*, Norges offentlige utredninger 2006: 6. Innstilling fra utvalg oppnevnt ved kongelig resolusjon 29. oktober 2004. Avgitt til Justis- og politidepartementet 5. april 2006.

[53] Se mere på http://www.cpni.gov.uk/about/cni/.

[54] The Presidential Commission on Critical Infrastructure Protection (1997): Final report.

[55] Jf. BEK nr. 765 af 3. august 2005, § 2, stk. 2.

[56] Se generelt Cabinet Office (2010), 'Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards', in Natural Hazards Team Cabinet Office (ed.), (London), p. 8 ff.

[57] Der findes ikke en egentlig universel definition på cyberwarfare. Begrebet omtales ofte i dansk militær sammenhæng som CNO'er (computer network operations). Nærværende rapport anvender den umiddelbart mest citerede amerikanske definition: "operations to disrupt, deny, degrade, or destroy information resident in computer networks, or the computers or networks themselves". Henriksen, Anders, *Cyberkrig*, p. 6, CMS april 2012.

[58] Ibid., p. 26 f.

[59] NATO CCDCOE, *National Cyber Secyrity (Framework Maual)*, p. 87 f., Tallinn 2012, tilgængelig via http://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf.

[60] Kahn, Herman, *On Escalation*, p. 3-9.

[61] Artikel på itwire.com, 8. juli 2013, tilgængelig via http://www.itwire.com/business-it-news/security/60609-south-koreas-dark-seoul-exposed-as-a-military-cyber-attack.

[62] Reuters, 9. juli 2013, tilgængelig via http://www.reuters.com/article/2013/07/09/us-korea-hackers-idUSBRE96714A20130709.

[63] RT.com, 9. januar 2013, tilgængelig via http://rt.com/news/uk-military-cyber-attack-637/.

[64] Kahn, Herman, *On Escalation*, kap. XI.

[65] Kommissionsrapport om terroranslagene i Norge 22. juli 2011, pkt. 19, tilgængelig via http://www.regjeringen.no/nb/dep/smk/dok/nou-er/2012/nou-2012-14/21.html?id=697401.

[66] http://www.regjeringen.no/nb/dep/smk/dok/nou-er/2012/nou-2012-14/3.html?id=697263.

[67] RT.com, 9. januar 2013, tilgængelig via http://rt.com/news/uk-military-cyber-attack-637/.

[68] Nielsen, Jens Beck og Nielsen, Asger Gørup: 'PET tager nyt våben i brug mod hackerne', Berlingske.dk, 1. juli 2013, tilgængelig via http://www.b.dk/nationalt/pet-tager-nyt-vaaben-i-brug-mod-hackerne.

[69] Pressemeddelelse fra PET, 2. juli 2013, tilgængelig via https://www.pet.dk/Nyheder/2013/PET%20styrker%20indsatsen%20i%20forhold%20til%20cybertrusler%20og%20cybersikkerhed.aspx.

[70] *Etablering af en statslig varslingstjeneste for internettrusler*, rapport fra IT- og Telestyrelsen, juni 2007, Dok-id. 424572.