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 dimensionering* (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.