Internasjonal POLITIKK Årgang 71 | Nr. 2 | 2013 | 274–283 | ISSN 0020-577X

FOKUS: CYBERSPACE

Cyber-resiliens i EU

MAREILE KAUFMANN
MA, doktorgradsstudent, PRIO
markau@prio.no

Ifølge Rådet for Den europeiske union utgjør nå informasjons- og kommunikasjonsteknologier ryggraden i EUs økonomi og samfunnsliv (Den europeiske unions råd 2009b). Transaksjoner innen finans og handel, transport, helsevesen og energi er avhengige av at nettverksforbindelsene fungerer. Hvis disse nettverkstilkoblingene bryter sammen, vil de økonomiske og samfunnsmessige konsekvensene raskt begynne å påvirke vårt hverdagsliv. Dette kan dreie seg om alt fra stengte minibanker, forstyrrelser i offentlig transport og økte oljepriser til avbrudd i tilgangen på grunnleggende samfunnsgoder som vann og strøm. Å vedlikeholde samfunnssektorer og informasjonsflyten mellom disse er derfor blitt en sentral sikkerhetsoppgave for EU.

Resiliens har i løpet av de siste fem årene blitt en sentral strategi i krisehåndtering. Begrepet beskriver evnen til å gjenopprette en normaltilstand etter en forstyrrelse. I dette bidraget benyttes resiliens som et analytisk begrep, som innebærer en mulighet for å *re-definere normalitet* – i motsetning til at man vender tilbake til det bestående. Begrepet er derfor mer anvendbart enn andre oversettelser av det engelske «resilience», slik som «robusthet» eller «motstandsdyktighet». Bidraget belyser EUs nåværende metoder for cyber-resiliens og hvordan disse metodene utfordrer og omdefinerer vår forståelse av sikkerhet.

De resiliente egenskapene fremmes på ulike måter i ulike transnasjonale nettverk, fra tekniske løsninger til diskursive prosedyrer. Det siste tiåret har EU etablert flere strategier for cyber-resiliens, fremfor alt gjennom dannelsen av Det europeiske byrået for nettverks- og informasjonssikkerhet (ENISA) og utgivelsen av Digital Agenda 2010. Som overnasjonalt organ søker EU å fremme regulering på tvers av landegrensene. Denne tilnærmingen er særlig relevant fordi digitale nettverk av natur er grenseoverskridende. En analyse av EUs tilnærming og de ulike strategienes interne dynamikk åpner også for noen generelle perspektiver på regulering.

Bidragets første del ser på forholdet mellom resiliens og risiko i et nettverkssamfunn. Deretter diskuteres de tekniske og politiske dimensjonene ved cyber-resiliens, før bidraget identifiserer noen svakheter i EUs tilnærming. Det argumenteres for at EUs forsøk på å utvikle cyber-resiliens mekanismer bidrar til å omforme vår forståelse av sikkerhet fra en oppfatning av sikkerhet som «beskyttelse mot fare» til en forståelse av sikkerhet som en form for «disruption management». Videre pekes det på at resiliens nødvendiggjør tett koordinering av ulike administrative nivåer og regulative regimer, noe som innebærer store styringsutfordringer.

Risiko og resiliens i nettverk

Både antall nettbrukere og det som i dagligtalen kalles «tingenes internett» er i eksplosiv vekst. International Data Corporation (IDC) anslår at bare i 2012 ble mer enn 100 milliarder sensorer og trådløst identifiserbare brikker, og 11,5 milliarder kommuniserende gjenstander koblet til internett (Europakommisjonen 2012: 29). Selv om nettverkstilkoblinger er ulikt geografisk fordelt (Graham 2011), knyttes gjenstander, brukere og brukerinstitusjoner verden over stadig tettere til hverandre.

Å sikre disse komplekse sammenkoblingene er en utfordrende oppgave. Ikke bare vanskeliggjøres arbeidet med å sikre internett av mange parter med ulike tilnærminger til cyber-sikkerhet, men nettverkskonstruksjonen utfordrer også vår tradisjonelle forståelse av «sikkerhet» som beskyttelse mot fare. Fra et teoretisk perspektiv er både sikkerhet og usikkerhet iboende aspekt ved nettverksstrukturer (Luhmann 1984; Castells 1996). Kompleksitet øker sannsynligheten for en systembetinget ustabilitet og dermed for en utvisking av grensene mellom tilsiktede og utilsiktede forstyrrelser. Samtidig vil lokale hendelser enkelt kunne spre seg gjennom et nettverkssystem og føre til trusler og forstyrrelser som er *større* enn summen av den enkelte hendelse. Faren for en slik dominoeffekt er blitt ett av hovedargumentene for EUs beredskapsprinsipper i cybersektoren, som fokuserer på å sikre «det svakeste leddet i kjeden» (Den europeiske unions råd 2009a). I teorien forstås nettverk samtidig som fleksible og tilpasningsdyktige, og i stand til å tilby alternative ruter hvis én forbindelse er brutt. Siden kompleksitet og tilkoblingsegenskaper synes å øke «overraskelsespotensialet» i et system (Demchak 2012), er vi i ferd med å nå grensen for vår evne til å beregne risikoer og forebygge trusler. Strategier for å oppnå resiliens er et svar på disse utfordringene, fordi de tar høyde for at vi ikke vet hvordan fremtidige forstyrrelser vil arte seg, og de vektlegger evnen til å respondere på trusler som ikke kan avverges i tide. Dette resulterer i resiliens-strategier som tar utgangspunkt i at en viss grad av risiko må aksepteres.

Resiliens-begrepet i sikkerhetsstudier er adoptert fra økologien (Holling 1973) og psykologien (Garmezy 1973) og brukes som betegnelse på handlinger som reetablerer en forstyrret likevekt eller øker evnen til å takle belastninger og stress. Innen sikkerhetsstudier har det utviklet seg et bredt spekter av definisjoner av resiliens, noe som igjen har medført en utvidet forståelse av begrepet. På den ene siden kan resiliens tolkes som en prosess eller egenskap som har som mål å opprettholde et status quo og motstå forstyrrelse. Det vil gjerne være stabile, velregulerte systemer og fellesskap som absorberer forstyrrelser ved hjelp av systematiske redundanser (flerdobbelt dekning). Denne elastisiteten har likevel sine grenser. Hvis forstyrrelsen vedvarer, må man forsøke å *gjenopprette* eller *gjenoppta* normal funksjon og utvikle nye normalmodi. De sistnevnte praksisene krever imidlertid ofte en evne til å tilpasse seg som man i større grad finner hos åpne men ustabile fellesskap og systemer (Kaufmann 2012).

Mens resiliens i «internettets økosystem av sammenkoblinger» (ENISA 2011b) refererer til en sikker, stabil tilstand, vil brukerne ikke oppleve forstyrrelser når nettverket gjenoppretter en stabil tilstand over tid. Resiliente nettverk kjennetegnes her ved at de leverer og opprettholder et akseptabelt tjenestenivå også når det inntreffer driftsfeil. Hovedmålet med resiliens er at driftsfeil forblir usynlige for brukeren (ENISA 2009: 8). Resiliensen til et cybersystem kommer til uttrykk i systemets tilgjengelighet, pålitelighet og potensial for vedlikehold (ENISA 2011a: 22). På bakgrunn av en analyse av sentrale EU-dokumenter og sekundærlitteratur, vil det følgende avsnittet diskutere et sett ulike strategier for cyber-resiliens og peke på noen utfordringer.

Cyber-resiliens: Den tekniske dimensjonen

Tekniske prosedyrer for å skape resiliens følger prinsipper om redundans, såkalt flerdobbelt dekning, og fleksibilitet. Fra et teknisk ståsted er internettet et nettverk av objekter og tjenester, som ledninger, kabler, servere og programvare. På samme måte som et transportnettverk muliggjør forskjellige ruter fra ett punkt til et annet, skaper tekniske redundanser i hver av nettverkets deler muligheter for å velge alternative metoder og ruter, som igjen muliggjør veksling mellom diverse dataoverføringsmedier og lokal lagring av informasjon. Veksling og lagring gjør at driften kan fortsette selv om nettverksfunksjoner på et høyere nivå svikter (ENISA 2009: 17). Redundans og designbetinget fleksibilitet krever dermed flere komponenter og former for drift med egenskaper som avviker fra hverandre. Planene for utforming av resiliente nettverk vektlegger visse sentrale egenskaper, som for eksempel *drift med flere komponenter*, der mange komponenter dekker ett aspekt av funksjonaliteten, *alternativ ruting*, evnen til å

velge og veksle mellom separate kretser, og *tjenestemangfold*, som gjør det mulig å lede kommunikasjon over på alternative tjenester (ENISA 2009: 17f). Disse planene vektlegger og tilrettelegger for en kvantitativ tilnærming til resiliens. Resiliens kan da måles ved hjelp av tidsfunksjoner som uttrykker hvorvidt et system er tilgjengelig innen et gitt tidsrom og hvor lang tid det tar å reparere skader (ENISA 2009: 24).

Disse strategiene for resilient utforming innebærer at forventningen om at ukjente hendelser kan inntreffe allerede er teknisk integrert på infrastrukturnivå. Fremtidig usikkerhet forankres dermed i den tekniske utformingen, ikke bare i form av ustabilitet fremkalt av kompleksitet, men også som en bevisst strategi for å skape infrastruktur som tar høyde for forstyrrelser. Mens det generelt strider mot prinsipper for kost/nytte-effektivitet å ha flere og avvikende versjoner av den samme tjenesten, er denne flerdobbeltheten kjernen i redundans-begrepet.

Etter hvert som nettverksstrukturen blir stadig mer sammenvevd og mangfoldig, vil denne flerdobbelte dekningen, hvor de ulike komponentene og tjenestene eies av ulike leverandører, også øke kompleksiteten. I mars 2011 rommet internett allerede rundt 37 000 autonome systemer, eksempelvis nettleverandører (ISP-er) (ENISA 2011b: 8). Selv om enkelte globale aktører kan levere de fleste tjenester, utgjør dette mangfoldet av interessenter en utfordring for resilient utforming. «De fleste tingene som ISP-er kan gjøre for å øke resiliensen til internett, kommer andre ISP-er mer til nytte enn selskapet som betaler for dem. Dette innebærer en potensiell 'allmenningens tragedie'. Resiliensmekanismer blir ikke implementert, fordi ingen har funnet en måte å rulle dem ut på som gir tilstrekkelig lokal nytte» (ENISA 2011b: 4). For effektivt å kunne regulere en så differensiert gruppe interessenter som det her er snakk om, kreves dessuten universelle driftsstandarder. Likevel er resilient teknologi bare ett aspekt av det å administrere og vedlikeholde sammenkoblinger. Cyber-resiliens har også en tydelig politisk og rettslig dimensjon som preges av forsøk på å definere og implementere «universelle driftsstandarder», i samspill med en rekke ulike interessenter med ulike perspektiver på sikkerhet.

Cyber-resiliens: Den politiske dimensjonen

På politisk nivå hersker en tendens til å delegere ansvaret for katastrofe-resiliens til en rekke lokale aktører som har en direkte innflytelse på sitt definerte område. I tråd med subsidiaritetsprinsippet er dette også tilfellet for EU hvor Europakommisjonens meddelelser om beskyttelse av kritisk informasjonsinfrastruktur (CII) understreker at EUs medlemsland har det endelige ansvaret for å definere CII-relaterte strategier (Europakommi-

sjonen 2009: 5). Dette betyr at politiske beslutninger treffes av den minst sentraliserte myndigheten som kan håndtere problemet effektivt. Prinsippet om desentralisert ansvar tilsvarer den konvensjonelle tilnærmingen til katastrofe-resiliens hvor problemer håndteres på lokalt nivå. I EU er det derfor anerkjent at katastrofehåndteringsstrategier nødvendiggjør en tydelig arbeidsdeling mellom nasjonale, undernasjonale og overnasjonale aktører og aktiviteter, noe som også kommer til uttrykk i juridiske tekster og harmoniseres i henhold til delte standarder. Subsidiaritetsprinisppet ville dermed gitt EU en tilrettelegger-rolle med ansvar for å fremme samarbeid og koordinere bidrag for å skape cyber-resiliens (Boin & Rhinard 2008: 9f).

Samtidig som det eksisterer et gap mellom løfter om å utvide EUs rolle og den faktiske overføringen av myndighet til Brussel (Boin & Rhinard 2008: 19), gjør forskjeller i ekspertise og beredskap at medlemslandene også har ulike strategier for CII-beskyttelse (Den europeiske unions råd 2009b: 3).

En god illustrasjon på dette er fellesøvelse «Cyber Europe». En del av handlingsplanen i meddelelse 149 består i å harmonisere de ulike strategiene for cyber-resiliens og å delegere og øve på ansvarsområder ved hjelp av «Cyber Europe»-øvelsene. Slike øvelser går langt utover de tekniske aspektene ved en potensiell cyber-katastrofe, og inkluderer også scenarioer for sammenbrudd av sentrale samfunnssystemer koblet til internett, som banksystemer, trafikk, telekommunikasjon og helsetjenester. Slike fellesøvelser ble gjennomført i 2010 og 2012. Mens disse øvelsene er sentralt organisert, re-introduserer subsidiaritetsprinsippet en idé om desentralisering i øvelsesstrategiene. Medlemslandene oppfordres til å gjennomføre regelmessige nasjonale øvelser og utarbeide nasjonale beredskapsplaner for nettverkssikkerhet og katastrofehåndtering (Europakommisjonen 2009: 12; Digital Agenda Action 39). Også organisasjoner og institusjoner på lavere nivå, som NGO-er, borgere og enkeltmennesker, oppfordres til å definere og registrere regelbrudd og problemer for å bidra til økt ansvarlighet (Bendiek 2012).

Slik delegering utøves imidlertid alltid med det formål å bidra til organisasjonen som helhet: Siden «intet medlemsland er en øy», understreker EUs strategier stadig at det enkelte medlemsland bare har begrenset mulighet til å styre og sikre global nettverkskommunikasjon. Internetts globale natur krever en helhetlig og systemisk tilnærmingsmåte til nettverk, informasjonssikkerhet og resiliens på tvers av grensene (Den europeiske unions råd 2009a; Den europeiske unions råd 2009b: 3; ENISA 2011c: 15). Når forskjeller i nasjonale strategier gjør tiltak mot cyber-angrep mindre effektive (Digital Agenda Action 39), blir universelle etiske standarder og systematisk samarbeid over landegrensene en nødvendighet. Strategier for cyber-resiliens svinger derfor mellom delegering av ansvar

til medlemslandene (inkludert infrastruktureierne) og standardisering og universelle regler på et overordnet plan.

Ett av EUs første tiltak for å harmonisere avvikende strategier og cyber-resiliens-aktiviteter var å definere et felles språk. ENISA har utarbeidet et sett med felles ideer om og ordforråd for resiliens som kan brukes av alle, såkalte ontologier og taksonomier for resiliens (ENISA 2011a). Neste steg var å definere teknologiske avvik i standardisering relatert til cyber-resiliens. Dette strakte seg fra protokoller og domenenavnsystemer til filformater. Å implementere en slik standardisering ligger imidlertid langt utenfor EUs kapasitet. Blant de viktige organene kan vi nevne Den europeiske standardiseringskomiteen (CEN), samt NGO-er som Den internasjonale standardiseringsorganisasjonen (ISO) og nonprofit-organisasjonen Internet Corporation for Assigned Names and Numbers (ICANN), som for eksempel koordinerer adressene til nettdomener (ENISA 2009).

Felles språk og felles definisjon av standarder fører ikke i seg selv til effektive overnasjonale tiltak. I noen dokumenter pekes det på klare mangler i koordinering av strategier for cyber-resiliens. Dette medfører behov for et minimum av samarbeidsavtaler og mekanismer for informasjonsutveksling (ENISA 2011c: 17f). På EU-nivå kan slike avtaler forholde seg til EMSA, FRONTEX og ENISA. På nasjonalt nivå fremmes harmonisering av strategier for cyber-resiliens ved hjelp av veiledninger for beste praksis og samarbeidsavtaler mellom medlemsland. Et eksempel på sistnevnte er gjensidige bistandsavtaler. Slike avtaler inngås mellom to eller flere parter og omfatter assistanse på tvers av landegrenser i en nødssituasjon. Disse formaliserte avtalene institusjonaliserer samarbeid som strekker seg lenger enn *ad hoc*-samarbeid bygd på personlige relasjoner. Siden et formål med disse avtalene er å overvinne hindringer som følge av regelverk, lover og konkurranseforhold, er de sentrale for beredskap og cyber-resiliens (ENISA 2011d: 6ff).

Et spørsmål om makt og lederskap

Å definere standardene for cyber-resiliens handler også om myndighet og makt. Mens de mest profilerte strategiene for katastrofe-resiliens gjerne stammer fra sentrale politisk organ som delegerer ansvar og kunnskap til mindre og mer lokale enheter, er kunnskap og myndighet i cyberspace *allerede* fordelt på et mangfold av interessenter. Fordi denne fordelingen har vokst frem organisk, er det nå svært utfordrende å avgjøre hvilket sentralt organ som skal definere og overvåke felles verdier og mål. I EU mangler strategier for cyber-resiliens en ledende aktør med ansvar for innholdet i dem. Dette skaper problemer med hensyn til transparens og ansvarsforhold (Bendiek 2012).

EU anerkjenner selv at mangelen på koordinering og systematisk samarbeid betraktelig reduserer effekten av nasjonale mottiltak. Innad i EU brukes imidlertid dette som et argument for den *positive* virkningen av en sterk EU-koordinering (Den europeiske unions råd 2009b: 3). Samtidig som det vil være vanskelig å innføre styringsmodeller for hele EU, argumenteres det i flere EU-dokumenter med at et sentralstyrt EU-initiativ ville gi store muligheter for å samle inn og bearbeide både informasjon om nasjonale svakheter, sårbarhetsfaktorer, sikkerhetshull, styringsroller og ansvarsforhold, noe som vil kunne få umiddelbar positiv effekt (Den europeiske unions råd 2009a; ENISA 2011d). En slik sentral koordinering og tilrettelegging ville økt verdien av de nasjonale programmene for beskyttelse av kritisk infrastruktur (Den europeiske unions råd 2009a: 15f).

Det er her viktig å påpeke at implementeringen av felles standarder i første omgang ville ha berørt den private sektoren, som eier størstedelen av den tekniske infrastrukturen. Dette innebærer flere utfordringer i koordineringen, siden verken markedskreftene eller standardiseringsforsøkene fra offentlige organer (som EU eller medlemslandenes regjeringer), har gitt tilstrekkelige insentiver til at privat sektor har investert i resiliensen til kritisk informasjonsinfrastruktur (Den europeiske unions råd 2009b: 3). Offentlig–private partnerskap fremstår som en åpenbar måte å fordele ansvar på, men selv om slike partnerskap har oppstått i enkelte land, har de ikke fått fotfeste på europeisk nivå (Den europeiske unions råd 2009b: 4f).

Et koordinerende EU-organ for cyber-resiliens vil derfor trolig ikke vokse frem av seg selv. Bendiek observerer at kunnskap er en svak ressurs på myndighetsnivå, og at EU-organer har ikke kompetanse til å bestemme dagsordener og forme prosesser. Hun påpeker at det er ekspertkunnskapen til private interessenter som er avgjørende hvis man skal bygge konsensus i en struktur preget av flere nivåer og mange interessenter. Strategiene for cyber-resiliens blir da avhengig både av informasjon fra privat sektor og av effektiv implementering av standarder i privat sektor, noe som er politisk problematisk. Det er viktig å diskutere om det er ønskelig at eksperter fra private selskaper skal kunne påvirke sikkerhetspolitikken og hvilke effekter dette kan få. Bendiek påpeker at den samme prosessen på den andre siden kan tolkes positivt, som en form for demokratisering av sikkerhetspolitikk (Bendiek 2012: 24).

Andre kommentatorer påpeker at Europakommisjonen med utgangspunkt i subsidiaritetsprinsippet vil fortsette å bygge opp kompetanse selv om det ikke foreligger noe klart mandat, samtidig som medlemslandene fortsatt vil komme med entusiastiske uttalelser om samarbeid mens de delegerer *ad hoc*, uten en helhetlig strategi. Reguleringen vil da fremdeles være spontan og vokse gradvis frem og ikke være resultat av en detaljert plan (Boin et al. 2007; Boin & Rhinard 2008: 19; Bendiek 2012). Ikke

desto mindre har EU, særlig med ENISAs pågående aktiviteter, vist at unionen anerkjenner cyber-resiliens som et felt med mange interessenter. Samtidig som ENISA de siste par årene har vektlagt en systematisk utvikling av felles standarder for cyber-resiliens og sikkerhet, vil det å balansere universell standardisering med delegert styring i et miljø med mange interessenter forbli en stor utfordring.

Konklusjoner – resiliens som nettverksbasert sikkerhet

Dette bidraget har analysert cyber-resiliens som en styringsstrategi. Koblingen mellom kritisk infrastruktur og internett har gjort sikkerhetsstyring mer komplekst og medført at presis risikoberegning ikke lenger er mulig. Dette har påvirket forholdet mellom sikkerhet og samfunn.

Sikkerhetstenkning beveger seg nå bort fra tanken om å beskytte samfunnet: De resiliens-strategiene som vokser frem, reflekterer en antagelse om at forstyrrelser er uunngåelige i en kompleks, nettverksbasert verden og at en viss grad av risiko må aksepteres. Forventningen om forstyrrelser inkorporeres i informasjonsinfrastrukturen i form av redundanser og teknisk resiliens. Resiliens-strategier forandrer dermed forståelsen av sikkerhet. I en nettverksbasert verden redefineres sikkerhet som samfunnets evne til å takle kriser.

I motsetning til standardiseringsteknikkene for risikoberegning, som bygger på sannsynligheten av gjennomsnitt, introduserer «sikkerhet som resiliens» en idé om mangfold. *Tekniske* strategier for cyber-resiliens svinger for eksempel mellom sikkerhet gjennom mangfoldighet og standardisering. Kort sagt bygger resilient utforming på et mangfold av komponenter og tjenester som sikrer redundans, men som *samtidig* har behov for standardisering. Å formulere og implementere standarder forblir imidlertid i like stor grad et spørsmål om teknisk ekspertise som om internasjonal politisk myndighet.

Den politiske dimensjonen av cyber-resiliens omfatter også en administrativ balansegang mellom private og offentlige interessenter. En konsekvens av dette er at resiliens-strategier også allokerer ansvar til nye samfunnsaktører. Strategiene for cyber-resiliens spenner fra vektlegging av lokalt ansvar til global standardisering. På den ene siden består de av delegert regulering som vokser organisk frem, slik det for eksempel kommer til uttrykk i gjensidige bistandsavtaler eller praktiseres i cyber-resiliensøvelser. På den andre siden tar strategier for cyber-resiliens sikte på å definere universelle standarder for datakommunikasjon og infrastrukturutforming, en strategi som må styres av overnasjonale organer. EU kan fungere som tilrettelegger for en slik standardiseringsprosess, men har ikke nødvendigvis den autoriteten som skal til; samtidig som kunnskapen

om utformingen av strategier ligger i privat sektor (Bendiek 2012). Frem- og tilbakegangen mellom delegert regulering og universelle standarder og det uklare ansvarsforholdet mellom offentlige og private interessenter kan føre til mangel på lederskap i utviklingen av cyber-resiliens. For å motvirke dette har EU satt i gang en dialog med private tjenesteleverandører. Det arbeides også med å definere smutthull i lovverket, samt å utforme et felles teknisk-politisk språk.

På et mer generelt plan har dette bidraget forsøkt å vise hvordan nettverkskommunikasjonen forandrer måten vi forstår og praktiserer sikkerhet som resiliens på. Tekniske og politiske strategier for cyber-resiliens gir rom for nye aktører (lokale, nasjonale, private, EU) og nye maktforhold dem imellom. Utviklingen av cyber-resiliens i EU utgjør et stort og interessant felt for videre forskning.

Om artikkelen

Denne artikkelen er resultatet av forskningsprosjektet «Mastering the Value Function of Security Measures» (ValueSec), finansiert gjennom EUs sjuende rammeverkprogram (bevilgningsavtalenr.: 261742). Artikkelen er oversatt av Eivind Lilleskjæret og redigert av Kristin Bergtora Sandvik.

Litteratur

Bendiek, Annegret (2012) Die Mehrebenen- und Multistakeholder-Struktur der Cybersicherheitspolitik. *Europäische Cybersicherheitspolitik*, SWP Studie S 15: 12–18. Tilgjengelig på www.swp-berlin.org/fileadmin/contents/products/studien/2012_S15_bdk.pdf

Boin, Arjen, Magnus Ekengren, Antonio Missiroli, Mark Rhinard & Bengt Sundelius (2007) *Building societal security in Europe: The EU's role in managing emergencies*. EPC Working Paper no.27.

Boin, Arjen & Mark Rhinard (2008) Managing Transboundary Crises: What Role for the European Union? *International Studies Review* 10: 1–26.

Castells, Manuel (1996) *The Rise of the Network Society*. Oxford: Blackwell.

Demchak, Chris C. (2012) Resilience and Cyberspace: Recognizing the Challenges of the Global Socio-Cyber-Infrastructure (GSCI). *Journal of Comparative Policy Analysis: Research and Practice* 14 (3): 254–269.

Digital Agenda for Europe (2010) Action 39: Member States to carry our cyber attack simulations. Tilgjengelig på http://ec.europa.eu/digital-agenda/en/pillar-iii-trust-security/action-39-member-states-carry-out-cyber-attack-simulations. Lest 30.11.2012.

Den europeiske unions råd (2009a) Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. Impact Assessment (Part 1), 8375/09, Accompanying Document, ADD1. Tilgjengelig på

http://register.consilium.europa.eu/pdf/en/09/st08/st08375-ad01.en09.pdf. Lest 30.11.2012.

Den europeiske unions råd (2009b) Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. Impact Assessment (Part 1), 8375/09, Accompanying Document, ADD4. Tilgjengelig på http://register.consilium.europa.eu/pdf/en/09/st08/st08375-ad04.en09.pdf. Lest 30.11.2012.

ENISA (2009) Gaps in Standardization related to resilience of communication networks. Tilgjengelig på www.enisa.europa.eu/publications/archive/gapsstd. Lest 29.10.2012.

ENISA (2011a) Ontology and taxonomies of resilience. Tilgjengelig på www.enisa.europa.eu/activities/identity-and-trust/technology-for-resilience/ontology. Lest 24.10.2012.

ENISA (2011b) Inter-X: Resilience of the Internet Interconnection Ecosystem. Tilgjengelig på www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/inter-x/interx/report/interx-report. Lest 30.10.2012.

ENISA (2011c) Analysis of Cyber Security Aspects in the Maritime Sector. Tilgjengelig på www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/dependencies-of-maritime-transport-to-icts/cyber-security-aspects-in-the-maritime-sector-1. Lest 24.10.2012.

ENISA (2011d): Mutual Aid for Electronic Infrastructure in Europe. Key Observations Report. Finnes på: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/mutual-aid-assistance/mutual-aid-agreements, hentet 24.10.2012

Europakommisjonen (2009) Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience. COM 149 final. Tilgjengelig på: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF. Lest 30.11.2012.

Europakommisjonen (2012) Towards a competitive European Internet industry. A socio-economic analysis of the European Internet industry and the Future Internet Public-Private Partnership. Tilgjengelig på http://ec.europa.eu/information_society/activities/foi/lead/socioeconomics/Comp%20Internet%20Industry%20Report.pdf. Lest 31.10.2012.

Garmezy, Norman (1973) Competence and adaptation in adult schizophrenic patients and children at risk. I S.R. Dean (red.) *Schizophrenia: The first ten Dean Award Lectures* (163–204). New York: MSS Information Corp.

Graham, Mark (2011) Time machines and virtual portals: The spatialities of the digital divide. *Progress in Development Studies* 11 (3): 211–27.

Holling, C. S. (1973) Resilience and Stability of Ecological Systems. *Annual Review of Ecology and Systematics*, (4): 1–23

Kaufmann, Mareile (2012) Resilience: A Stock-Taking. Key Characteristics and Implications for Human and Societal Security Policy. *PRIO Policy Brief*, 12. Oslo: PRIO.

Luhmann, Niklas (1984) *Soziale Systeme. Grundriss einer allgemeinen Theorie*. Frankfurt am Main: Suhrkamp.