Hjemmeeksamen i RAG 600_1 Terrorsikring og resiliens

Høst 2020

Kandidat nummer: 6009

Utfordringer for å bygge resilient samfunn gjennom risikobasert styring av cyberterrorsimens "wicked problems"

Antall ord: 3593

Antall sider: 15

Innholdsfortegnelse

1. Innledning ... 3

2. Teoretisk rammeverk ... 4

2.1. Terrorisme som "wicked problems" ... 4

2.2. Resiliens ... 5

2.3. Funksjonsbasert risikostyring ... 6

3. Diskusjon ... 7

3.1. Risikobasert styring av cyberterrorismens "wicked problems": muligheter og utfordringer ... 7

Risikobasert styring gir organisasjoner fleksibilitet ... 7

Terrorsikring er blitt "felles" ansvar, men hvem har eierskap til "transboundary" kriser? ... 8

Risikostyringsregimet er ingen praktisk veiledning ... 9

Virksomheter må stadig balansere mellom sikkerhet og produksjonshensyn ... 9

Man blir aldri ferdig med sikkerhetsarbeid ... 10

3.2. Kan samfunnets resiliens oppnås gjennom risikobasert styring av cyberterrorisme? ... 11

4. Konklusjon ... 12

5. Litteraturliste ... 13

1. Innledning

Sikring av cyberspace er en av de viktigste utfordringene i det tjueførste århundret. Økt avhengighet av datasystemer gjør vårt globale samfunn mer sårbart og denne sårbarheten forsterkes av trusselen om cyberterrorisme. Stadig flere aktiviteter som truer nasjonale interesser og kritisk infrastruktur foregår i cyberspace. Vår teknologisk og psykologisk avhengighet av elektroniske systemer har gjort det virtuelle rom til en attraktiv arena for trusselaktører. I den nyere tid har vi tatt vår digital avhengighet på et nytt, fysiologisk nivå, gitt fremskritt i tilknyttet medisinsk utstyr, eksempelvis pacemakere, insulinpumper osv. Dette er gamechanger i diskusjonen om cyberterrorisme. Den utbredte uttalelsen "hvem bryr seg om terrorister på nettet, ettersom de ikke kan drepe mennesker fra cyberspace?" er ikke lenger gyldig. Vi må se dette som signal om at både organisasjoner og staten må lære seg hvordan de nye risikoer kan styres på best mulig måte.

Oppgaveteksten etterspør refleksjoner rundt hvorvidt risikobasert styring[1] er en velegnet metode for å håndtere cyberterrorismens "wicked problem", samtidig som en oppnår målene om et resilient samfunn. For å besvare oppgaven ser jeg nærmere på konseptene problemstillingene består av, herunder terrorisme som "wicked problems", risikobasert styring, og resiliens-begrepet. Videre diskuteres forhold mellom risikobasert styringsregime og "wicked problems" av cybersecurity. Deretter reflekterer jeg rundt hva som fordres for å bygge et resilient samfunn. Jeg konkluderer med at noen aspekter av cyberterrorisme gjør anvendelsen av et risikobasert styringsstyringsregime utfordrende fra både organisatorisk og myndighetenes perspektiv. Konklusjonen underbygges av argumenterer for at integrering av elementer av resiliens-konseptet i risikostyringsmodeller kan bidra til det overordnede målet om resilient samfunn. Med andre ord, bør cyberterrorisme styres ved hjelp av "resiliensbasert" risikostyring.

[1] I denne besvarelsen brukes begrepet "risikobasert styring om "risk-based (functional) regulatory regime"

2. Teoretisk rammeverk

2.1. Terrorisme som "wicked problems"

"Wicked problems" som fenomen har vært kjent siden 1960-tallet. Først i 1973 ble begrepet konseptualisert av Rittel og Webber, som utarbeidet en liste med ti særegenskaper som kjennetegner "wicked problems" (Churchman, 1967; Rittel & Webber, 1973). Forfatterne analyserte en enestående type problemer som utfordrer beslutningstaking innen politisk styring i offentlig sektor. "Wicked problems" beskrives kort som komplekse, preget av usikkerhet og tvetydighet og dermed umulig å finne løsning på.

Jeg velger videre å bruke Fischbacher-Smiths (2016) artikkel som analyserer terrorisme med utgangspunkt i Rittel og Webbers "wicked problem"-modell. Etter min mening er hans rammeverk en grundig empiriskbasert tilnærming som synliggjør felles elementer mellom "wicked problems" og terrorismens egenskaper (Fischbacher-Smith, 2016, s. 402). Jeg bruker derfor hans analyse som en tverrfaglig brobygger for å inspisere forholdet mellom risikobasert styringsregime og cyberterrorisme som fenomen.

Terrorisme er kanskje det mest politiserte begrepet i dag og er svært omstridt på grunn av eksisterende uenigheter rundt definisjonen. For diskusjon rundt terrorisme-begrepet trekker jeg inn Alex Schmid sitt teoretiske bidrag for perspektiver på terrorisme, da det vurderes som svært grundig og omfattende. Schmid (2013) har samlet omkring 250 ulike definisjoner for "terrorisme". Han fremhever *bruk av vold* eller *trussel om vold* med det primære formålet om å generere en *psykologisk innvirkning* utover ofrene med et *politisk motiv* som fellesnevner for alle terrorhandlinger.

Denne definisjonen signaliserer at vi beveger oss bort fra konseptet av terrorisme som direkte voldsutøvelse, mot forståelsen av terrorisme som fryktskapende handlinger. Cyberterrorister er "individer som ikke er motivert av penger, men heller av å fremme en politisk agenda eller ideologi for å forårsake skade og kaos for allmennheten" (Brooks et al., 2018, s. 661). Denne definisjonen faller rett inn i det nye perspektivet på terrorisme.

Også Smith og Brooks (2013) varsler en ganske annen fremtid enn den vi ser i dag ved å bemerke det pågående skiftet i terrorismens årsaker og uttrykksformer som samtidig overlapper med karakteristiske trekk ved "wicked problems". Det skiftende begrepet kan, ifølge Smith og Brooks (2013), omfatte blant annet øko-terrorisme, cyberterrorisme og KI-terrorisme[2]. Uansett hvordan fremtidens terrorisme manifesteres, vil valg av perspektiver på risikostyring være av største betydning for å bygge et resilient samfunn.

2.2. Resiliens

I likhet med "terrorisme"-begrepet kan man identifisere i overkant av 300 forskjellige definisjoner av begrepet "resiliens" (Anholt & Boersma, 2018). Ved å trekke hovedessens ut fra definisjonsmangfoldet, kan resiliens defineres som "samfunnets evne til å tilpasse seg og raskt komme seg fra stress og sjokk forårsaket av påkjenninger som kriser, katastrofer osv.". UNDG[3] spesifiserer at gjenopprettelse av funksjoner skal resultere i "vedvarende, positiv og transformerende endring" (Anholt & Boersma, 2018, s. 3).

I likhet med "terrorisme" gjennomgår "resiliens"-begrepet et ontologisk skifte. Welsh (2014) bemerker dette ved å argumentere for at resiliens skal forstås som en kontinuerlig tilpasnings-prosess istedenfor en statisk tilstand. Også Evans og Reid (2013) utvider denne tankegangen ved å fremstille endring i resiliens-paradigmet, som en bevegelse fra en utopisk tilstand av trygghet mot aksept av at den moderne verden innebærer permanent eksponering for uunngåelige farer.

Globalisering, klimaendringer og endring i globalt trusselbilde er sannsynlige årsaker til økt fokus på resiliens. Den iboende usikkerheten assosiert med tilsiktede hendelser, gjør at den siste tilnærmingen kanskje samsvarer best med terrorrisikoen vi lever med hver dag. Risikobasert styring er et av verktøyene som brukes for å styrke samfunnets resiliens.

---

[2] KI står for kunstlig intelligens (engelsk: AI). Smith og Brooks bruker begrepet "kybernetisk terrorisme"
[3] United Nations Sustainable Development Group

2.3. Funksjonsbasert risikostyring

For diskusjonen rundt risikobasert styringsregimet velger jeg å trekke inn Sissel Jore sitt teoretisk bidrag. Jore er et kjent navn i "sikkerhet vs. security"-debatten og har forsket på terrorisme-diskursen i flere år (Jore, 2012, 2019a, 2019b, 2020).

På 1970-tallet har risikobasert styring stegvis erstattet regelbasert tilnærming, som innebærer overgang fra detaljert myndighetskontroll til et internkontrollregime (Lindøe et al., 2012). Risikobasert styring bygger på forventninger om at organisasjoner har nødvendig kompetanse for å vurdere fremtidige risikoer og trusler, og tilstrekkelige ressurser for å møte myndighetenes mål. Forventningene baseres på antagelsen at organisasjoner har alle forutsetninger for å ta rasjonelle beslutninger og velge blant flere løsningsalternativer (Aven, 2003). Problemet er, skriver Rittel og Webber (1973, s. 164) at det ikke finnes flere løsningsalternativer for "wicked problems".

Jore (2015) knytter terrorangrepene 22. juli 2011 mot Oslo/Utøya og mot oljeanlegget In Amenas i januar 2013 til sterkere fokus på private og offentlige organisasjoners ansvar for risikostyring i Norge. Disse hendelsene og påfølgende massiv mediedekning dannet grunnlag for en allmenn forventning om beskyttelse mot terrorisme i privat og offentlig rom (Jore, 2020). Terrorsikring, som tidligere hadde nasjonal og sektoriell karakter, har blitt et felles ansvar. Dette gjenspeiles i lover og forskrifter publisert i senere år. I 2011 ble det vedtatt ny objektsikringslovgivning basert på risikobasert tankegang og tre nye standarder for terrorsikring ble publisert noen år senere (Jore, 2020). Med utgivelsen av KIKS-rapporten (DSB, 2016) og den nye Sikkerhetsloven (2018) satt myndighetene krav til at hensyn til kritiske samfunnsfunksjoner skal legges til grunn i risikovurderinger.

Ovennevnte dokumenter bygger på et "funksjonelt" reguleringsregime til terrorsikring, der implementeringen av sikkerhetstiltak baseres på risikovurderinger i stedet for forskriftsmessige krav (Jore, 2019b). Et "funksjonelt" regelverk beskriver krav til sikkerhetsnivået som skal oppnås, men ikke spesifiserer hvordan nivået skal oppnås. Altså at konkrete krav og virkemåter utarbeides av hver enkelt organisasjon basert på resultater av risikovurderinger. Tilnærmingen har tradisjonelt vært brukt i industri, hvor ulykker oppstår på grunn av svikt i tekniske, organisatoriske eller menneskelige barrierer (Jore, 2019a).

3. Diskusjon

3.1. Risikobasert styring av cyberterrorismens "wicked problems": muligheter og utfordringer

Moderne organisasjoner må ifølge risikobasert reguleringsregime håndtere både sikkerhets- og security-utfordringer, som kan oppfattes som fundamentalt forskjellige. Mens sikkerhet knyttes til produksjonsrelaterte risikoer, herunder *utilsiktede* hendelser som organisasjonen velger å akseptere, omhandler security trusler organisasjonen er utsatt for (Jore, 2019b). Sikkerhet konseptualiseres derav som et teknisk og kontrollerbart problem, hvor organisasjonen selv er kilde til både problemet og løsningen (Jore, 2019a). Security-problemer er derimot ikke nødvendigvis direkte tilknyttet selskapets aktiviteter og byr derfor på flere utfordringer knyttet til risikostyring.

Risikobasert styring gir organisasjoner fleksibilitet

Tanken bak risikobasert styring er at virksomheter risikoutsettes i ulike grad, avhengig av virksomhetens formål, kritikalitet og lokalisering (NSM, POD, PST, 2015). I security-kontekst fokuserer dette reguleringsregime på kunnskapen organisasjoner har om sine verdier, sårbarheter og trusler (Jore, 2015). Det gir fleksibilitet i hvordan å organisere cybersecurity arbeid og innrette sine digitale systemer mot truslene som anses å være mest kritiske. Dermed har organisasjonen best forutsetninger for å beskytte kritiske verdier, og kan endre og/eller tilpasse sikringstiltak i takt med endringer i trusselbildet. Gitt raskt teknologisk utvikling i cyberspace-kontekst representerer denne egenskapen ved risikobasert styring gode muligheter for cyberterrorsikring.

En utfordring er at med teknologisk fremgang, gjennomgår trusselbilde raskt og kontinuerlig endring. Følgelig må organisasjoner konstant oppdatere sine risiko-/trusselanalyser og barrierer. Ifølge Rittel og Webber (1973, s. 162) resulterer dette i at man aldri blir ferdig med "wicked problems". Med teknologisk fremgang utvikler cyberterrorister kontinuerlig nye angrepsmetoder og finner nye potensielle terrormål, som utfordrer mulighetene for oversikt over alle eksisterende angrepsmetoder og -mål. Fischbacher-Smith (2016) påpeker at også terroristenes krav endres kontinuerlig, som igjen utelukker utvikling av en helhetlig tilnærming. Et stadig endrende trussel-

og risikobilde medfører at hvert "wicked problem" er unikt og genererer flere unike forhold (Fischbacher-Smith, 2016; Rittel og Webber, 1973).

Terrorsikring er blitt "felles" ansvar, men hvem har eierskap til "transboundary" kriser?

Boin (2009) bruker begrepet "transboundary kriser" som har flere felles kjennetegn med "wicked problems". Dette kan sees i sammenheng med standardisering av risikobasert styring som verktøy for å håndtere terrorisme. Standardisering innebærer at ansvaret for terrorsikring ikke lenger er utelukkende statens ansvar, men overføres til private aktører. Boin (2009) argumenterer for at effektiv respons på problemer knyttet til teknologisk utvikling ikke nødvendigvis er sentralisert. Grunnen til utviklingen er en overgang fra verden hvor trussel var "sentralisert" (under den kalde krigen) til en verden hvor trusselbilde er fragmentert. Derav behøves desentralisering av ansvar. Overgangen fra "top-down" til "bottom-up"-tilnærming i internasjonal og rikssikkerhet utfordrer statens rolle som sikkerhetsgarantist (Carr, 2016).

En annen utfordring knyttet til transboundary "wicked problems" er at de ikke er selvstendige problemer, men symptomer på andre underliggende prosesser (Rittel & Webber, 1973, s. 166). Som regel er ikke organisasjonen selv ansvarlig for disse underliggende prosesser. Organisasjonen er heller ikke alltid et mål for politisk og/eller ideologisk motiverte terrorister. Det vil si at underliggende prosesser ofte skjer globalt, og er et resultat av beslutninger tatt på nasjonalt og internasjonalt nivå. Samtidig, påstår Boin (2009) er stater ikke lenger i stand til å håndtere "wicked problems" og "transboundary" kriser på egen hånd. Hvem skal da ha eierskap til kriser forårsaket av disse problemene? Boin (2009, s. 373) påpeker at dette kan resultere i at slike kriser får "multiple owners or no owners at all".

Å styre cyberterrorismens risiko vanskeliggjøres ytterligere, da det ikke finnes en entydig og anerkjent definisjon for fenomenet: ulike land og organisasjoner definerer terrorisme på ulike måter (Rogers, 2019). Valg av definisjon vil være retningsgivende for hvilke strategier en anvender for risikostyring (Jore, 2012; Schmid, 2013). Problemet med cyberterrorisme knyttes og til "usynlighet" av konsekvenser, som utfordrer individets kognitive forbindelse mellom cyberangrep og "vold" og "trussel"-konsepter vi er kjent med i den fysiske verden. Dette byr på utfordringer for

politisk legitimering av mottiltak. Boin og McConnell (2007) fremhever at manglende "frykt"-elementet kan være avgjørende for hvilke midler samfunnet kan bruke for å bekjempe terrorisme.

Risikostyringsregimet er ingen praktisk veiledning

Jore (2015) bemerker at risikobasert styringsregime ikke er en praktisk veiledning. På en side gir det fleksibilitet til organisasjoner som opererer i raskt endrede omgivelser. På andre side vanskeliggjør det styring da det ikke finnes én riktig løsning på cyberterrorismens "wicked problems". Rittel og Webber (1973, s. 162) argumenterer for at løsningene i praksis er subjektive skjønnsvurderinger av varierende kvalitet. Boin og McConnell (2007) foreslår at "trial-and-error"-strategi kan være aktuelt for styring av terrorrisiko med målet om samfunnets resiliens. Rittel og Webber (1973, s. 163) skriver derimot at man ikke har rom for "trial-and-error" i styring av "wicked problems", fordi implementering av tiltak genererer ikke-reversible forhold.

Risikoanalyser forutsetter at man kan definere problemets rammer, som ifølge Rittel og Webber (1973, s. 166) er umulig for "wicked problems". Kombinert med tidligere nevnte egenskaper, medfører dette at de involverte i håndteringen av "wicked problems" har forskjellige perspektiver på fenomener, som resulterer i avvik mellom politikk og praksis (Fischbacher-Smith, 2016). Videre er det vanskelig å forstå helheten av konsekvenser av et cyberangrep på grunn av systemets gjensidige avhengighet.

Jore (2015) problematiserer videre manglende "benchmarking" som skal hjelpe med å forstå når sikkerhetsnivå er "godt nok". Vil en god nok sikkerhet fra organisatorisk perspektiv bety "god nok" med hensyn til samfunnets behov? Hvor mye skal organisasjoner investere i sikkerhetstiltak? Rittel og Webber (1973, s. 162) mener at man sannsynligvis vil avslutte arbeidet med "wicked problems" når man går tom for tid og/eller penger, og ikke når problemet er løst.

Virksomheter må stadig balansere mellom sikkerhet og produksjonshensyn

Jore (2015) mener at organisasjoner har blitt politisk viktige aktører i terrorkampen, mens den dominerende økonomiske logikken som styrer risikotankegangen til privat sektor neppe er forenelig med nasjonale sikkerhetsmål. Ifølge norsk lovgivning må organisasjoner selv betale for

sikkerhetstiltak som kan resultere i at organisasjoner prioriterer økonomiske hensyn fremfor sikkerhetsmål. Tiltak som er tilknyttet utbyttemaksimering er lett å legitimere for stakeholdere. Det er imidlertid ikke så enkelt med terrorsikringstiltak, hvor kostnadene ikke utelukkende til selskapets fordel, men og skal bidra til å beskytte landet. Ifølge Jore (2015) kan det resultere i at mange selskaper senker risikonivået for å spare på terrorsikring.

Hvorvidt dilemmaet sikkerhet vs. produksjon vil være gjeldende i cybersecurity-kontekst er vanskelig å si, fordi skillet mellom cyberterrorangrep og cyberangrep med andre intensjoner er veldig diffus. Organisasjoner investerer gjerne i barrierer som kan hindre økonomisk motivert cyberangrep. De samme barrierene kan med fordel brukes mot cyberterrorangrep. Det er grunn å tro at mange tiltak vil være "overlappende" innen cybersikkerhet, dermed får man anledning til å oppnå både security- og sikkerhetsmål.

Man blir aldri ferdig med sikkerhetsarbeid

Rittel og Webber (1973) mener at på grunn av behovet for konstant tilpasning og kontinuerlig søk etter nye løsninger blir man aldri ferdig med "wicked problems". Denne fellesnevneren for cyberterrorisme og "wicked problems" er også til stede i risikobasert styring. Dette er utfordrende for organisasjoner, fordi det krever at det settes mye arbeid i risikostyringsprosessen (Jore, 2015).

For det første stilles det krav til internkontroll og rapportering til myndigheter. Hensikten er å gjøre det lettere for reguleringsmyndigheten å bedømme om målene med regelverket er oppfylt. Sikkerhet i dette perspektivet er kontinuerlig ressurskrevende arbeid som innebærer at organisasjonene konsekvent må overvåke hvorvidt sikkerhetssystemet er i samsvar med nasjonale trusselvurderinger.

Jore (2015) problematiserer organisasjoners manglende forståelse for trusselsituasjonen og hvilke tiltak som kan/bør iverksettes. Organisasjoner må oppdateres om både nasjonal og internasjonal trusselsituasjon, men markedsglobalisering vanskeliggjør situasjonen ytterligere. Ifølge Aven (2003) få organisasjoner besitter den nødvendige kompetansen til å gjennomføre meningsfulle trusselvurderinger som medfører at de fleste må stole på nasjonale trusselvurderinger, ta i bruk nasjonale standarder eller/og betale konsulentselskaper som utarbeider risikoanalyser.

3.2. Kan samfunnets resiliens oppnås gjennom risikobasert styring av cyberterrorisme?

Jeg har vist at usikkerhet, tvetydighet og kompleksitet som kjennetegner "wicked problems" gjør det praktisk umulig å finne en universell løsning på problemene. I stedet for å bruke alle ressurser på å forsøke å eliminere terror-risiko må vi akseptere den nye normalen og heller fokusere på å bygge opp "risikosamfunnet" sin resiliens. Hollnagel (2011) argumenterer for at samfunnet heller bør fokusere på å designe kritiske systemer med fokus på en robust responsevne. Hvordan gjør man det?

Flere forskere har utarbeidet konkrete forslag til metodiske verktøy som kan brukes for å fremme organisasjonens og samfunnets resiliens (Hollnagel et al., 2011; Steen, 2019). Metodiske verktøy er ikke fokus i denne oppgaven. Jeg ønsket heller å se nærmere på overordnede aspekter av samfunnets resiliens. Jeg har tidligere nevnt at mye tyder på at i cybersecurity-kontekst er staten ikke lenger i stand til å ha full kontroll over risikoer og trusler. Flere forskere argumenterer for at for å fremme samfunnets resiliens skal privat sektor og lokalt samfunn involveres i enda større grad enn i dag (Boin & McConnell, 2007; Carr, 2016).

Ifølge Carr (2016), som forsker på cybersecurity-governance i Storbritannia og USA, er det flere grunner til at cybersikkerhet og spesielt sikring av kritisk infrastruktur, er blitt oppfattet som en utfordring for samarbeid mellom offentlig og privat sektor. Staten er fremdeles ansvarlig for å sørge for nasjonal sikkerhet ved sikring av kritisk infrastruktur. Potensielle konsekvenser av et omfattende cyberterrorangrep på kritisk infrastruktur er så alvorlige at regjeringen vil stilles til ansvar. Imidlertid forvaltes det meste av kritisk infrastruktur i vestlige land av private aktører. Derfor er det behov for et synergi-forhold mellom offentlige og private sektorer for terrorsikring. Forholdet må være koordinert "power sharing", med gjensidig gunstig deling av ansvar, kunnskap og/eller risiko. Videre er det avgjørende at private aktører samarbeider på tvers av sektorer og fremmer aktiv erfaringsdeling. Statens rolle består ikke lenger av tilsyn og veiledning, men av koordinering nettverk og valg av instrumenter som kan brukes til å motivere disse nettverkene (Carr, 2016).

Boin og McConnell (2007) nevner at det kan være vanskelig å fremme resiliens-tankegang i samfunnet med mindre folk føler "frykt". Utfordringen er å oppnå fornuftig nivå av frykt uten å

skape unødvendig angst (Boin & McConnell, 2007). Videre understrekker de viktigheten av kontinuitetsplanlegging i arbeidet med samfunnets resiliens. Også Hollnagel (2011) fremhever improvisasjon som resiliens-strategi, men understreker at kontinuitetsplanlegging i tillegg innebærer en viss fragmentering og desimering av tradisjonelle hierarkiske strukturer og høy grad av situasjonsfleksibilitet. Stor grad av standardisering kan være en effektiv måte å sikre forutsigbarhet i dagligdagse operasjoner, men kan negativt påvirke evnen til å håndtere uventede hendelser som terrorisme (Boin & McConnell, 2007; Jore, 2020).

4. Konklusjon

Gjennom oppgaven har jeg argumentert for at anvendelsen av risikobasert styring i kontekst av cyberterrorisme kan representere noen utfordringer for både private aktører og myndigheter. Dette har sine forklaringer i egenskapene til både cyberrisiko og risikoanalyseverktøy organisasjoner har tilgjengelig. Jeg er enig med Jore (2015) i at moderne organisasjoner ikke er utstyrt for å bære et samfunnsmessig sikkerhetsansvar slik de er pålagt. Dette utfordres ytterligere av at gjeldende terrorbekjempelsesregelverk legger ansvaret på mange forskjellige aktører i samfunnet, og det er vanskelig å utpeke hvem som faktisk er ansvarlig for terrorsikring og potensielle kriser.

I arbeid med cyberterrorsikring vil stater være avhengige av å etablere synergi-forhold med private aktører som forvalter samfunnskritisk infrastruktur. Hvis et slik forhold etableres, vil privat sektor spille en sentral rolle i nasjonal og internasjonal sikkerhet. For å oppnå målet om resilient samfunn må man først identifisere dysfunksjonelle elementer i offentlig-privat samarbeid og deretter utvikle mekanismer for å sikre at forholdet blir basert på gjensidig tillit, felles rolleforståelse og ansvarsbevissthet. Videre kan man begynne å inkorporere cybersikkerhet-strategi i en nasjonal sikkerhetsstrategi.

Risiko og resiliens er overlappende konsepter som søker å minimere alvorligheten av konsekvenser ved uønskede hendelser. Begge er rettet mot å avdekke og redusere systemets sårbarhet. For å bygge et resilient samfunn som vil kunne ha en god responsevne og for å fremme vedvarende, positiv og transformerende endring bør resiliens integreres i risikostyring. Vi bør dermed se på muligheter for å implementere et alternativt "resiliensbasert"-risikoperspektiv.

5. Litteraturliste

Anholt, R., & Boersma, K. (2018). *From Security to Resilience: New Vistas for International Responses to Protracted Crises*. IRGC.

Aven, T. (2003). *Foundations of risk analysis: A knowledge and decision-oriented perspective*. John Wiley & Sons.

Boin, A. (2009). The New World of Crises and Crisis Management: Implications for Policymaking and Research. *Review of Policy Research*, *26*, 367–377. https://doi.org/10.1111/j.1541-1338.2009.00389.x

Boin, A., & McConnell, A. (2007). Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. *Journal of Contingencies and Crisis Management*, *15*(1), 50–59. https://doi.org/10.1111/j.1468-5973.2007.00504.x

Brooks, C. J., Grow, C., Craig, P., & Short, D. (2018). *Cybersecurity: Essentials*. SYBEX, Wiley.

Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, *92*(1), 43–62. https://doi.org/10.1111/1468-2346.12504

Churchman, C. W. (1967). Wicked problems. *Management Science*, *14*(4), B-141-B-146. https://doi.org/10.1287/mnsc.14.4.B141

DSB. (2016). *Samfunnets kritiske funksjoner: Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* (s. 116). https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

Evans, B., & Reid, J. (2013). Dangerously exposed: The life and death of the resilient subject. *Resilience*, *1*(2), 83–98. https://doi.org/10.1080/21693293.2013.770703

Fischbacher-Smith, D. (2016). Framing the UK's counter-terrorism policy within the context of a wicked problem. *Public Money & Management*, *36*(6), 399–408. https://doi.org/10.1080/09540962.2016.1200801

Hollnagel, E., Pariès, J., Woods, D., & Wreathall, J. (Red.). (2011). *Resilience engineering in practice: A guidebook*. Ashgate.

Jore, S. H. (2012). *Counterterrorism as Risk Management Strategies*. https://uis.brage.unit.no/uis-xmlui/handle/11250/182345

Jore, S. H. (2015). Challengers of Building Societal Resilience through Organizational Security Risk Management. *Working on Safety, Portugal*.

Jore, S. H. (2019a). The Conceptual and Scientific Demarcation of Security in Contrast to Safety. *European Journal for Security Research*, *4*(1), 157–174. https://doi.org/10.1007/s41125-017-0021-9

Jore, S. H. (2019b). The Multifaceted Aspect of Uncertainty – the Significance of Addressing Uncertainty in the Management of the Transboundary Wicked Problem of Terrorism. ESREL *Proceedings of the 29th European Safety and Reliability Conference 22-26.09.2019, Hannover, Germany*, 4044–4051.

Jore, S. H. (2020). Standardization of terrorism risk analysis. I O. E. Olsen, K. Juhl, P. H. Lindøe, & O. A. Engen (Red.), *Standardization and risk governance: A multi-disciplinary approach* (s. 150–165). Routledge New Security Studies.

Lindøe, P. H., Kringen, J., & Braut, G. S. (2012). *Risiko og tilsyn risikostyring og rettslig regulering*. Universitetsforlaget.

NSM, POD, PST. (2015). *En veiledning i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger*. https://www.politiet.no/globalassets/03-rad-og-forebygging/beredskap/terrorsikring_en_veileder

Rittel, H. W. J., & Webber, M. M. (1973). Dilemmas in a general theory of planning. *Policy Sciences*, *4*(2), 155–169. https://doi.org/10.1007/BF01405730

Rogers, M. (2019). Cyber Terrorism. I A. Silke (Red.), *Routledge handbook of terrorism and counterterrorism* (s. 253–263). Routledge, Taylor & Francis Group.

Schmid, A. P. (Red.). (2013). *The Routledge handbook of terrorism research*. Routledge, Taylor & Francis Group.

Sikkerhetsloven, Pub. L. No. LOV-2018-06-01-24(2018).

Smith, C. L., & Brooks, D. J. (2013). *Security science: The theory and practice of security*. Elsevier, BH.

Steen, R. (2019). On the Application of the Safety-II Concept in a Security Context. *European Journal for Security Research*, *4*(2),175–200. https://doi.org/10.1007/s41125-019-0004-0

Welsh, M. (2014). Resilience and responsibility: Governing uncertainty in a complex world. *The Geographical journal*, *180*(1), 15–26. https://doi.org/10.1111/geoj.12012