VITEN

FORSKNINGSFAGLIG RAPPORT 1. 2016 FORSVARETS FORSKNINGSINSTITUTT

BESKYTTELSE AV SAMFUNNET I EN NY TID

PROSJEKT
Forståelse og forebygging av radikalisering i Skandinavia
side 21

UTVIKLING
Totalforsvaret i dag
side 12-13

SUKSESSKRITERIER
Håndtering av askeskykrisen
side 28-29

FFI-RAPPORT 15/02472

FFIs nyhetsbrev kommer jevnlig

Les mer og abonner
ffi.no\nyhetsbrev

FFI Forsvarets forskningsinstitutt

OM VITEN

VITEN er en ny type rapport fra Forsvarets forskningsinstitutt (FFI). Den er rettet mot et bredere publikum og er laget i et oversiktlig tidsskriftformat. VITEN kommer i første omgang ut fire ganger i året, og er et ledd i FFIs satsing på god forskningsformidling og -kommunikasjon.

Med VITEN ønsker vi å bidra til en mer opplyst offentlig debatt, med mer forskningsbasert kompetanse, kunnskap og nettopp viten. Temaer for disse rapportene kommer fra hele bredden av FFIs forskning – fra militærtekniske forhold til forsvarsplanlegging, sikkerhetspolitikk og samfunnssikkerhet. I særlig grad vil vi belyse temaer som har betydning for de utfordringene Forsvaret og sivilsamfunnet står overfor. Vi håper at VITEN vil bidra til å vekke interesse for FFIs mange forskningsområder, og vise at forskningen vår bidrar til et bedre forsvar og et tryggere samfunn.

En elektronisk utgave av VITEN ligger på ffi.no, ofte sammen med utfyllende rapporter og annet materiale.

Har du spørsmål om VITEN? Ta kontakt med oss: VITEN@ffi.no

Sikkerhet i en ny tid

Norsk beredskap og krisehåndtering er basert på en omfattende nasjonal dugnad mellom en rekke aktører — sivile og militære, offentlige og private. Samfunnet er i stadig endring og utvikling, og trusler, verdier og sårbarheter som til sammen kan si noe om hvilke risikoer samfunnet er utsatt for, endres også. Forskningsmiljøene har en viktig rolle i å etablere et godt kunnskapsgrunnlag for utvikling av norsk krisehåndtering og beredskap, for å belyse dilemmaer, foreslå tiltak og endringer og bidra til politikkutforming. Forskning bidrar med oppdatert, realistisk, kritisk og nyansert kunnskap om hvordan norsk samfunnssikkerhet og beredskap fungerer.

Formålet med denne rapporten er å presentere FFIs samfunnssikkerhetsforskning og utvalgte sentrale forskningsresultater fra prosjektserien Beskyttelse av samfunnet (BAS). FFIs forskning på sivil beredskap i starten av prosjektserien BAS brøt ny mark i det som senere kom til å omtales som forskning innen samfunnssikkerhet. Forskningen på dette feltet er i vekst ved en rekke universiteter, høyskoler og institutter i Norge i dag, og samfunnssikkerhet er etablert som en egen studieretning ved flere utdanningsinstitusjoner. Det er et viktig område for FFI å satse på.

Det langsiktige målet med BAS er å bidra til et gjennomarbeidet konsept for beskyttelse av befolkningen og samfunnet for øvrig samt å støtte opp under en løpende prioritering av beskyttelsestiltak. Kjernen av dagens BAS-forskning er å se på de store, alvorlige hendelsene som kan ramme Norge, og som krever beredskapsplanlegging og krisehåndtering på tvers av sektorer og nivåer, og der det er behov for sivilt-militært og offentlig-privat samarbeid. Vi ønsker å bidra med kunnskap på en god måte og sørge for å formidle mest mulig av våre resultater til offentligheten. Fordi forskningen bidrar til å belyse sårbarheter og har et kritisk blikk på vår krisehåndteringsevne, er det likevel nødvendig å skjerme deler av forskningsresultatene.

Forskningsgruppen for prosjektprogrammet BAS er tverrfaglig sammensatt av forskere fra statsvitenskap, sosialantropologi, kjemi, fysikk, informatikk og ingeniørfag. Gruppen samarbeider med en rekke andre forskningsgrupper ved FFI, blant annet innen langtidsplanlegging for Forsvaret, terrorismeforskning, cybersikkerhet og beskyttelse mot eksplosiver, kjemiske, biologiske, radiologiske og nukleære trusler.

Dagens BAS-forskning med tilhørende prosjekter og forskningsoppdrag finansieres av blant annet Forsvarsdepartementet, Justis- og beredskapsdepartementet, Nærings- og fiskeridepartementet, Direktoratet for samfunnssikkerhet og beredskap, Nasjonal sikkerhetsmyndighet, Norges forskningsråd, EUs 7. rammeprogram, Forsvarsbygg, Kystverket og Jernbaneverket.

Monica Endregard

Forskningsleder,
BAS-prosjektene

Utgiver:
Forsvarets forskningsinstitutt

Forside/illustrasjon:
FFI/Shutterstock

Redaktør:
Wenche Gerhardsen

Design:
Isabel A. Nordang

viten@ffi.no

Bidragsytere:
Monica Endregard
Kjersti Brattekås
Kjell Olav Nystuen
Therese Sandrup
Wenche Gerhardsen

Foto/illustrasjon:
Forsvaret , NTB Scanpix,
Shutterstock, FFI

Trykk:
Fladby as

Opplag:
1500

P: ISBN 978-82-464-2622-8
E: ISBN 978-82-464-2623-5

Abonner på vårt nyhetsbrev:
ffi.no/nyhetsbrev

Følg oss på:
Facebook
Instagram
ffi.no

Forsvarets forskningsinstitutt
Besøksadresse:
Instituttveien 20
2027 KJELLER

Postadresse:
Postboks 25
2027 KJELLER

Telefon:
63807130

MILJØMERKET
07 AURSKOG - 241 378

BESKYTTELSE AV SAMFUNNET I EN NY TID

SIVIL BEREDSKAP

ETTER DEN KALDE KRIGEN

Hvordan samfunnets militære og sivile deler forstår hverandre og samarbeider om samfunnssikkerhet har endret seg mye siden slutten av 1980-tallet. Det har også forskningen på feltet gjort. FFI har med prosjektserien Beskyttelse av samfunnet (BAS) tatt del i dette forskningsfeltet fra det var helt ferskt. Behovet for mer forskning på feltet startet med Berlinmurens og jernteppets fall. Da endret samfunnets oppfatning av trusler seg dramatisk i løpet av kort tid.

Frykt for atomkrig og tredje verdenskrig gikk over i en langt mer avslappet holdning til trusler mot Norge. Samtidig ble det globale internettet og utviklingen innen informasjonsteknologi en stadig mer sentral faktor i informasjonsflyten i samfunnet. På kort tid ga internett oss en helt annen tilgang til informasjon. Forholdet mellom offentlige virksomheters og næringslivets rolle i samfunnet ble også utfordret på denne tiden. Tidligere tunge statlige virksomheter innen sektorer som telekommunikasjon og kraft ble avmonopolisert og splittet i nye selskaper, som en blanding av statsvirksomheter og private selskaper. Det var mange som ikke lenger så behovet for den gamle måten å gjøre ting på. Som en konsekvens av denne utviklingen begynte i realiteten en nedbygging av det gamle totalforsvaret, selv om dette ikke var basert på noen beslutning hverken politisk eller i forvaltningen. Totalforsvarets opprinnelse og hensikt var en viktig bakgrunn for BAS-prosjektene.

En annen viktig bakgrunn for at FFI mot midten av 1990-tallet gikk i gang med BAS-prosjektene, var den sivile siden av samfunnsutviklingen. Den formelle bakgrunnen for prosjektserien BAS finnes i Stortingsmelding 24 (1992-93) og Stortingsmelding

Foto: NTB Scanpix

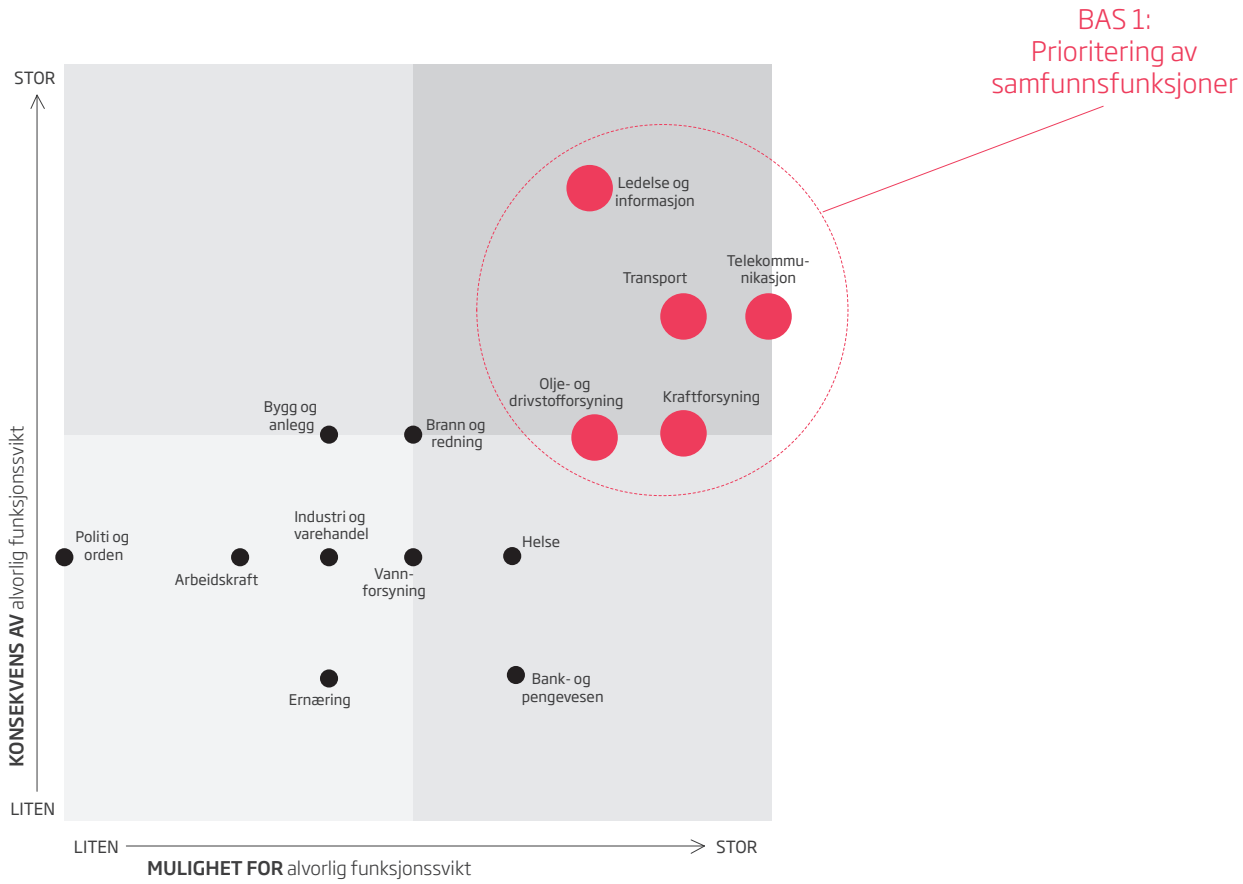
48 (1993-94), som sier at den sivile beredskapen skal omstilles etter et endret risikobilde for bedre å utnytte ressurser i fredstid. I tillegg ble behovet for en revurdering av sivil beredskap forsterket med privatiseringen av offentlige selskaper, som deler av NSB, Telenor og kraftsektoren. Ny eierform ga nye muligheter for samarbeid mellom offentlige, private og utenlandske aktører, og det la nye premisser for beredskapen. Et samarbeid mellom daværende Direktoratet for sivilt beredskap og FFI startet i 1994, for å planlegge for omstilling av den sivile beredskapen på lang sikt. Dermed var det første BAS-prosjektet i gang.

Grunnlaget for et robust samfunn

Den første delen av prosjektrekken, BAS 1, var ferdig i mars 1997. BAS 1 slo blant annet fast at det hadde blitt viktigere enn tidligere å ha beredskapstiltak som sikret behovene under noen innledende uker eller måneder av en eventuell væpnet konflikt. Det ble enda viktigere å se sammenhengen mellom beredskapen i fredstid og i væpnet konflikt, og beskytte individer indirekte gjennom å beskytte viktige samfunnsfunksjoner. Et verktøy for å forberede samfunnet på mulige hendelser er bruk av scenarioer. Scenarioer er beskrivelser av mulige hendelsesforløp som skal belyse konsekvenser av ulike handlingsalternativer. Scenarioer er en hjelp til å identifisere mangler og utfordringer i sivil beredskap og definere mål. BAS 1 brukte både freds- og krigsscenarioer for å få fram hvilke situasjoner et beredskapsapparat skal kunne håndtere. Krigsscenarioene inkluderte blant annet invasjonsangrep mot Finnmark og Nord-Norge, raid og strategiske overfall. Fredsscenarioene var naturskader, trafikkulykker, branner, skogbranner, oljeforurensning, transport av farlig gods, industriulykker, forsyningskriser, atomforurensing, flyktningestrømmer og terrorisme.

De viktigste samfunnsfunksjonene som bør opprettholdes både i væpnet konflikt og i fredstid ble definert i BAS 1. Prosjektet så også på trekk ved militærteknologisk utvikling og krigføring i framtiden, og prosjektet analyserte erfaringsdata fra Gulfkrigen i 1991 for å se hvordan koalisjonen angrep strategiske mål og hvilken effekt angrepene hadde. I tillegg vurderte prosjektet hvordan og hvor det var behov for bedre luftvarsling og tilfluktsrom.

På samme tid som BAS 1 foregikk, fikk temaene «det sårbare samfunn» og «kritiske infrastrukturer» stadig mer oppmerksomhet internasjonalt. I USA ga the President's Commision on Critical Infrastructure Protection ut sin rapport i 1997. I denne rapporten ble det i stor grad lagt vekt på de samme forholdene som BAS-prosjektet på FFI hadde utforsket. Dette var med på å øke oppmerksomheten rundt sårbarhetene i det moderne sam-



funnet i Norge. Den amerikanske rapporten pekte på sentrale utviklingstrekk, som raskt økende kompleksitet og at utviklingen i seg selv var så rask at det var en utfordring å følge den.

Analysene i BAS 1 la et grunnlag for å prioritere hvilke områder som burde undersøkes nærmere: telekommunikasjon, kraftforsyning, transport, olje- og drivstofforsyning, ledelse og informasjon. De tre første av disse områdene ble fulgt opp i de påfølgende BAS-prosjektene.

Telekommunikasjon i fred og konflikt

Det andre i rekken av BAS-prosjektene tok mellom 1997 og 1999 et dypdykk i sårbarheter i offentlig telekommunikasjon. Prosjektet konkluderte med at telekommunikasjonsproblemer vil skape stor friksjon i samfunnet, selv om de inntreffer under normale fredstidsforhold. Mer spesifikt vil samfunnet og den sivile beredskapen ikke være i stand til å yte tilstrekkelig støtte til Forsvaret uten tilgjengelig telekommunikasjon.

BAS 2 pekte på konkrete sårbare områder i det offentlige telenettet, synliggjorde konsekvensene av alvorlig svikt i dette nettet og foreslo strategier og tiltak for å beskytte telenettet på best måte ved ulike utfordringer. Blant annet ble det i sluttrapporten til BAS 2 foreslått å snu på antakelsen om at god sikring mot hendelser i fred også vil gi god krigsbeskyttelse, og heller si at «et telenett som er godt beskyttet mot menneskeskapte trusler vil også være godt egnet til å motstå normale fredsutfordringer».

Nettverkene for telekommunikasjon som BAS 2 så på var det offentlige telenettet, Forsvarets nett og mobil kommunikasjon. Prosjektet anbefalte til slutt at Norge bør satse på å sikre det offentlige telenettet i utstrakt grad framfor å satse på tjenester fra de to alternative nettverkene, blant annet ved å bruke mangfoldet mellom ulike teleoperatører for å redusere sårbarhet. Prosjektet pekte også på en ny utvikling mot slutten av forrige årtusen: «I fremtiden vil en se en konvergens mellom fastnettjenester og mobile teletjenester. Det er derfor viktig at også mobile nett blir gitt tilstrekkelig robusthet». I dag er dette et kjent tema.

BAS 2-prosjektet ble til tross for sin beskjedne størrelse gjenstand for betydelig oppmerksomhet. Samferdselsdepartementet etablerte prosjektet Teleberedskap i et fritt konkurransemarked (TIFKOM) som skulle bearbeide resultatene og sørge for en konkretisering av tiltak. Dette prosjektet støttet i stor grad BAS-prosjektets vurderinger. Senere kom Stortingsmelding 47 (2000-2001), som ble et fundament for videre regime innen telesikkerhet og beredskap i Norge. Et av de første tiltakene som ble iverksatt etter at stortingsmeldingen var behandlet i Stortinget, var å opprette en beredskaps- og sikkerhetsfunksjon i daværende Post- og teletilsynet. FFI var involvert i alle disse prosessene, og fikk umiddelbart positive reaksjoner på forskningsresultatene. Likevel ble temaet i mindre grad fulgt opp. En antatt viktig årsak til dette var flyttingen av Post- og teletilsynet, etterfulgt av en stor gjennomtrekk av eksperter.

Vår avhengighet av elektrisitet

BAS 3 undersøkte i perioden 1999 til 2001 det norske samfunnets avhengighet av elektrisitet. Betydningen av sårbarhet i telenettet og informasjonssikkerhet generelt ble klart tegnet i BAS 2. BAS 3 tok for seg tiltak for å redusere sårbarhet i kraftforsyningen, som er sårbar både overfor fysiske påkjenninger og anslag mot informasjonssystemene. BAS 3 vurderte i hovedsak hendelser som oppstår i gråsonen mellom fredstid og erklært krigstilstand mellom Norge og en annen stat.

Sårbarheten vil i framtiden øke, konkluderte BAS 3. Sammen med et usikkert trusselbilde førte det til at FFI blant annet anbefalte å sikre systemer av informasjons- og kommunikasjonsteknologi (IKT), å satse på personell og kompetanse, å bedre reetablerings- og reparasjonsmuligheter og å sikre viktige funksjoner i infrastrukturen. På lang sikt anbefalte FFI å sikre kraftforsyningen på et høyt nivå.

Tilnærmet all produksjon av elektrisk kraft i Norge er vannkraft, som overføres via kabler i luft, vann og jord. Flere kraftlinjer legges i samme trasé for å spare natur og penger. Det gir økt sårbarhet, blant annet ved at kraftinfrastrukturen blir vanskelig å overvåke og beskytte. Det var begrenset vilje til å iverksette beredskapstiltak blant aktørene i kraftmarkedet, og derfor mente FFI at offentlige ressurser til kraftberedskap burde økes betydelig. Myndighetene har et tungt ansvar, men den enkelte forbruker av strøm har også muligheter til å redusere sin egen sårbarhet ved å ha systemer for alternativ oppvarming og nødstrøm.

Kraftsektoren hadde fremdeles et fungerende sikkerhets- og beredskapsregime på begynnelsen av 2000-tallet, i motsetning til telesektoren, der mye av dette hadde forvitret. Kort tid etter at BAS 3 hadde kommet med sine anbefalinger, ble sikkerhets- og beredskapsregimet i kraftsektoren ytterligere utviklet.

I 2000 kom Sårbarhetsutvalget, ledet av Kåre Willoch, med sin utredning. BAS-miljøet ga flere bidrag til utvalgets arbeid, og til andre utvalg etter Sårbarhetsutvalget.

Transport mot mer sårbare tider

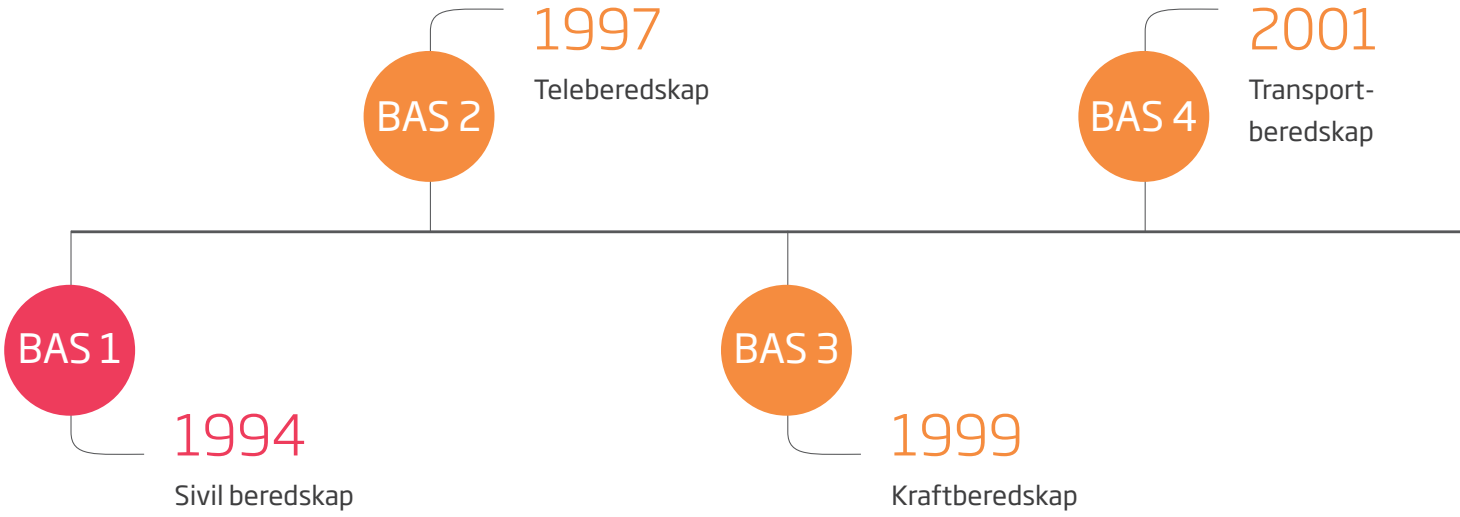
Transportsektoren var tema for BAS 4-prosjektet, som varte fra 2001 til 2003. Oppdraget for BAS 4 kom fra Direktoratet for samfunnssikkerhet og beredskap (DSB), daværende Justisdepartementet og Samferdselsdepartementet, som ville ha svar på spørsmålene: Hvor sårbar er transportsektoren, og hvilke tiltak kan bidra til å gjøre den mer robust?

Vurderingene i dette prosjektet ga innsikt i enkeltsystemene i luftfart, jernbane, veitransport og sjøtransport. Analysene viste at det skal mange samtidige terror- eller krigsanslag til for å svekke transportkapasiteten på nasjonalt eller regionalt nivå. Likevel fant BAS 4 at noen delsystemer i transportsektoren var mer sårbare enn andre, blant annet informasjons- og kommunikasjonssystemer i logistikkstyring og trafikkstyring, personansamlinger på terminaler og transportmidler og transport av farlig gods. En annen svakhet var Transportberedskapsorganisasjonen (TBO), som hadde særlig mangel på koordinering i krisesituasjoner. BAS 4 anbefalte at Samferdselsdepartementet tok over dette ansvaret ved å etablere et transportberedskapsforum. TBO ble i 2005 lagt ned, og ansvaret for å koordinere beredskapen på regionalt nivå ble da overført til fylkeskommunene.

BAS 4 konkluderte med at selv om transportsektoren er rimelig robust, er den, og spesielt jernbanen, kritisk avhengig av andre sektorer som telekommunikasjon, drivstoff- og kraftfor-

BESKYTTELSE AV SAMFUNNET

BAS-prosjektene



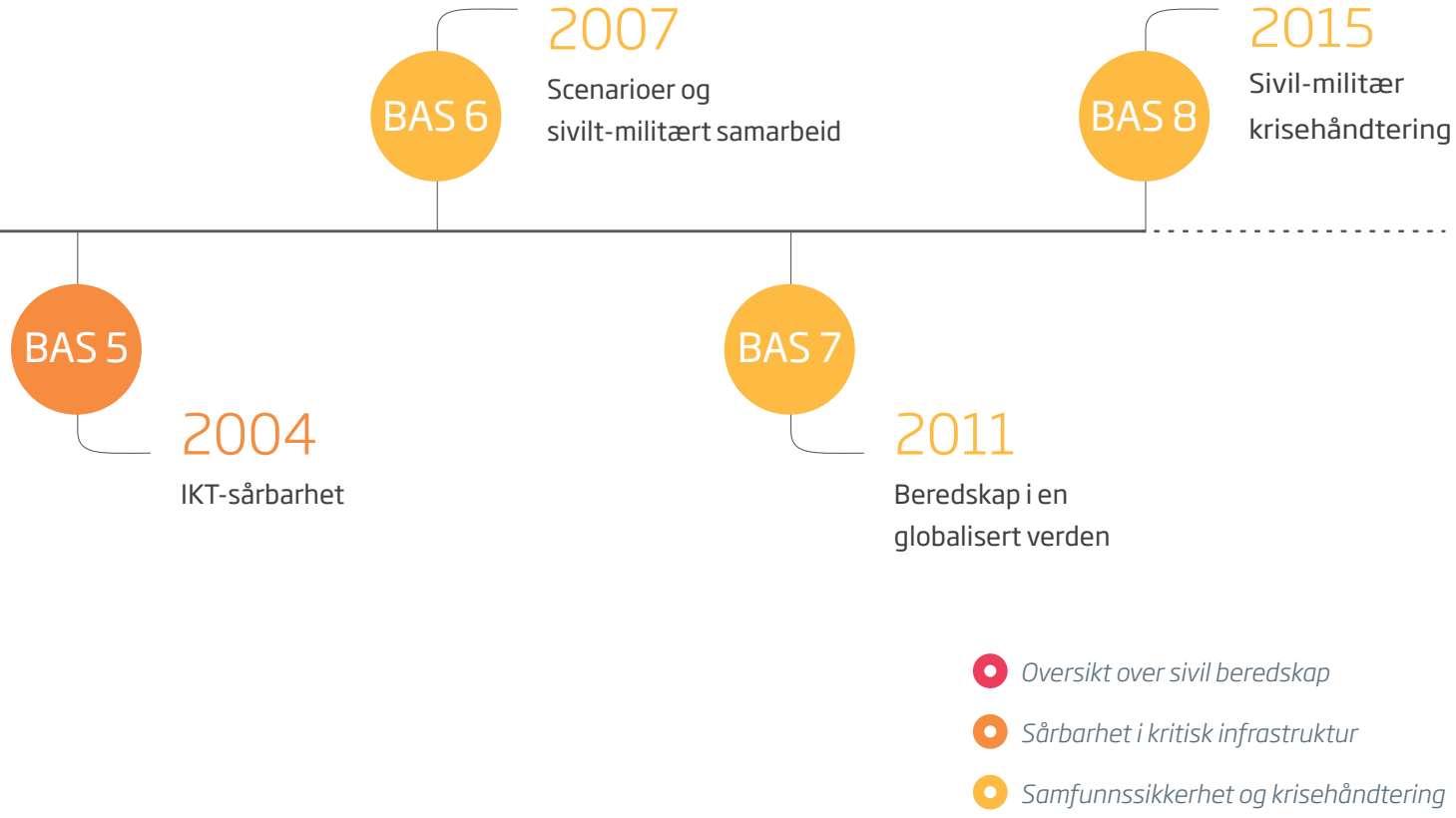
syning. En utvikling mot mer avhengighet av IKT vil dessuten endre premissene for beredskap innen transportsektoren. Krav til økt effektivitet bidrar til å øke bruken av IKT både innen persontransport og godstransport. Det gir igjen mer sårbarhet, og mindre personell som vil kunne operere manuelt under krise. BAS 4 foreslo derfor å innføre ett av tre sikkerhetsnivåer, avhengig av sikkerhetssituasjonen i Norge, med en grunnsikkerhet i bunn (det rimeligste alternativet), deretter beskyttelse mot terrorisme (dyrere) og til slutt et høyeste (og dyreste) nivå for beskyttelse mot væpnet konflikt.

BAS 4 framhevet hvor avhengige vi er av IKT-tjenester og IKT-infrastruktur, og hvor mye dette betyr for samfunnssårbarheten. Prosjektet viste at det ligger en utfordring i å bruke gode metoder i sektorvise risikoanalyser der IKT-systemer blir viktigere for den totale sårbarheten. Neste BAS-prosjekt utforsket derfor metoder for helhetlige analyser som inkluderer integrerte IKT-systemers sårbarhet.

Bedre metoder reduserer risiko

Det femte BAS-prosjektet var et samarbeid mellom flere forskningsinstitusjoner, akademia, myndigheter og offentlige og private virksomheter. Tidligere BAS-prosjekter la fram konkrete forslag til kostnadseffektiviserende tiltak som reduserte sårbarheter i systemene de studerte. Da BAS 5 startet høsten 2004, ble det raskt klart at denne gangen var selve metodene bak tiltakene mer relevante. Grunnen til dette skiftet var den raske utviklingen innen IKT samt teknologi og marked for øvrig, som gjør at konkrete tiltak ofte er foreldet før de blir realisert. Derfor gikk BAS 5 inn for å finne fram til metoder for å vurdere risiko og sårbarhet (ROS) for alle kritiske samfunnsfunksjoner, ikke bare innen IKT.

En ROS-analyse er et virkemiddel for å håndtere risiko. Der blir uønskede hendelser identifisert og rangert ut fra risikoen for at de inntreffer og får alvorlige konsekvenser. Det er første skritt på veien til å redusere risiko, blant annet ved å bidra til at de viktigste systemene og mest effektive tiltakene blir prioritert i sikkerhetsarbeidet. I nasjonal strategi for informasjonssikkerhet fra 2003 står det at «risiko- og sårbarhetsanalyser skal ligge til grunn for alle tiltak myntet på informasjonssikkerhet». Som casestudier gjennomførte BAS 5 fire ROS-analyser av eksisterende IKT-systemer ved et stort sykehus, et stort finansforetak, en stor aktør innen kraftforsyningen og en stor aktør



i petroleumsbransjen. I disse analysene foretok prosjektet en egen studie av sårbarheter i internett. Andre studier i prosjektet undersøkte framtidig utvikling innen nanoteknologi, grafteori og myndighetenes rolle i informasjonssikkerhet som forebygger og kriseleder.

Da prosjektet ble avsluttet i 2007, hadde det utviklet metodikk som kunne brukes til å identifisere og rangere kritiske samfunnsfunksjoner og IKT-systemer, gjøre risikoanalyse av samfunnskritiske IKT-systemer og vurdere effektivitet av tiltak som kan redusere sårbarheter i IKT-systemer. Metodene svarer på spørsmålene: Hva er de mest samfunnskritiske virksomhetene og IKT-systemene? Hvordan kan risiko og sårbarheter i de kritiske IKT-systemene analyseres? Hvordan kan vi velge blant ulike tiltak for å øke sikkerheten i IKT-systemene? Prioriteringer gir imidlertid mest mening for problemstillinger som er mest mulig konkrete. Det kan være svar på spørsmål som: Hvem bør ha prioritert tilgang til kommunikasjonstjenester i en krisesituasjon? Eller: Hvor lønner det seg å investere for å forebygge kriser?

Det er mange utfordringer med gode risikoanalyser av IKT-systemer. Derfor dokumenterte BAS 5 sine erfaringer i en overordnet veileder for risikoanalyse av samfunnskritisk IKT. Risikoanalyser er for øvrig ett av flere virkemidler som er aktuelle for å øke IKT-sikkerhet. Generelle krav om å gjennomføre ROS-analyser som et ledd i det nasjonale sikkerhetsarbeidet er derfor lite hensiktsmessig med mindre virksomhetene ikke samtidig ser hvorfor de bør gjøre det og hvordan de best bør gjøre det. Erfaringene fra BAS 5 ga viktige innspill til dette. BAS 5 etterspurte og anbefalte også rammebetingelser for arbeidet med nasjonal informasjonssikkerhet med et konkret ambisjonsnivå for arbeidet, en avklaring av aktørers roller og oppgaver og gode metoder i bunn.

I BAS 5 ble en rekke faglige temaer i grenselandet mellom IKT og risikoanalyse behandlet. Dette var nybrottsarbeid, og det var naturlig å involvere universiteter og høgskoler. Prosjektet ga økt innsikt i svært komplekse forhold, samtidig som det også ble demonstrert hvordan en tilsynelatende felles problemstilling kan fortone seg i ulike forskningsmiljøer. ■

01

TOTALFORSVARET I DAG

Den gjensidige avhengigheten mellom Forsvaret og det sivile samfunnet øker. Med dette øker også behovet for samarbeid om samfunnssikkerhet i dagens totalforsvar.

Tanken om at Norge skulle ha et totalforsvar ble utviklet av den norske eksilregjeringen i London under den andre verdenskrig. Forsvaret av Norge skulle bygge både på et militært forsvar og en bred sivil beredskap. Dette skulle verne om Norges territorium, selvstendighet og nasjonale verdier og om sivilbefolkningen. Totalforsvaret var opprinnelig skreddersydd for å møte en invasjon, men blir stadig videreutviklet for å møte flere utfordringer i vår tids trusselbilde.

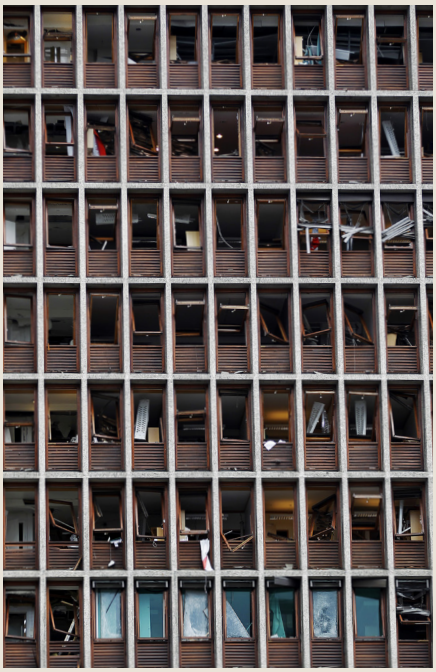
Det moderniserte totalforsvarskonseptet er fortsatt basert på at det norske samfunnet skal utnytte sine begrensede ressurser på best mulig måte når en krise rammer. Gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunnet er grunnleggende for å ivareta samfunnssikkerhet og statssikkerhet, i hele spekteret fra fred via sikkerhetspolitisk krise til væpnet konflikt.

Behov for gjensidig støtte

Stortinget har presisert at de totale ressursene som er tilgjengelige i væpnet konflikt, også skal kunne brukes ved krisehendelser i fredstid. Forsvaret skal derfor i større grad enn tidligere vektlegge støtte til det sivile samfunnet ved fredstidskriser. Det er en av Forsvarets eksplisitte oppgaver å bidra til å ivareta samfunnssikkerhet og andre sentrale samfunnsoppgaver.

Terrorhandlingene 22. juli 2011 synliggjorde behovet for at Forsvaret er klar for å yte bistand til det sivile samfunnet på kort varsel. Forsvaret skal etter anmodning kunne bistå ved ulykker, naturkatastrofer, alvorlig kriminalitet og andre fredstidskriser, og beskytte landet mot alvorlige anslag, inkludert terroranslag. Det er imidlertid nødvendig å vurdere støtte på andre måter også. Et eksempel er samfunnets behov for støtte til å opprettholde et robust sivilt og militært cyberdomene.

I motsatt ende skal den sivile støtten til Forsvaret helst baseres på kommersielle ordninger og samarbeid med sivile aktører gjennom leveranse- og beredskapsavtaler. Her har Forsvaret blitt mer avhengig av at sivile bedrifter leverer infrastruktur, varer, tjenester og teknologi. Slik avhengighet vil kunne gjøre Forsvaret mindre effektivt i ulike scenarioer. Med kortere varslingstid og langvarige konflikter blir dette spesielt



02

03

04

01 Masseskadeøvelse i Narvik. Forsvaret og sivile beredskapsetater øver sammen.
02 Høyblokka i regjeringskvartalet ble helt utbombet 22. juli 2011.
03 Vaktholdet rundt regjeringskvartalet var høyt etter bomben i Oslo.
04 Folk lurer. En soldat på vakt i Oslo etter 22. juli må svare.
05 Blomster og lys på gata.
Foto: Forsvaret

05

synlig. Omfattende pliktmessig sivil støtte til Forsvaret i alvorlige krisesituasjoner vil imidlertid fortsatt kreve at beredskapslovgivningen anvendes. Dette er ikke lenger nødvendig når Forsvaret skal støtte sivilsamfunnet.

Komplekse, nye sårbarheter

De siste 20 årene har totalforsvaret gjennomgått store endringer. Dette er en konsekvens av flere faktorer: den nye sikkerhetspolitiske situasjonen etter den kalde krigen, Forsvarets utvikling, nye rammefaktorer innen sivil beredskap og den generelle samfunnsutviklingen. Med dette kommer økt privatisering, globalisering og teknologiutvikling – ikke minst innen informasjonsteknologi. For eksempel er det gjort avtaler med private aktører om bruk av sivile fiberforbindelser til bruk i Forsvarets egne IKT-systemer. Denne utviklingen, med mer komplekse systemer og eierskapsforhold, fører med seg nye sårbarheter. I fred, krise og væpnet konflikt vil fremmede makter og andre aktører for eksempel kunne rette strategiske angrep mot både Forsvaret og samfunnet for øvrig gjennom avanserte informasjonsoperasjoner, som også kan kombineres med andre konvensjonelle virkemidler.

Utviklingen av totalforsvarskonseptet henger sammen med endringene i sikkerhetsbehovene og hvordan vi oppfatter den nasjonale beredskapens formål. Vi legger i dag mer vekt på samfunnssikkerhet i tillegg til statssikkerhet. Trusselbildet har blitt mer sammensatt, ikke minst ved at nye aktører som utøver terrorisme vokser fram. De nye truslene er gjerne mer dynamiske og mangler grenser. De vil ofte kunne inntreffe raskt og være en kombinasjon av ulike virkemidler. Det er vanskeligere enn tidligere å forstå hvor truslene kommer fra og hva de konkret består av. I dette nye trusselbildet blir nettopp samarbeidet i totalforsvaret ekstra viktig for å kunne beskytte samfunnet på best mulig måte.

HVA GJØR VI HVIS...?

Fra det første BAS-prosjektet startet i 1994 til det sjette prosjektet startet i 2007 hadde det nasjonale arbeidet med samfunnssikkerhet gjennomgått store endringer. Ikke minst gjaldt dette hvilke utfordringer Norge og norske interesser sto overfor. Ved inngangen til 1990-tallet var trusselbildet relativt oversiktlig, og et vanlig scenario var et militært angrep mot Norge, utført av Sovjetunionen. Et totalforsvarskonsept hadde over lengre tid blitt utviklet for å håndtere denne trusselen. I dag er bildet av ulike farer og trusler som Norge står overfor langt mindre oversiktlig, og det er en rekke hendelser som kan tenkes å utgjøre en trussel mot Norge og norske interesser. Dette gjør dagens arbeid med samfunnssikkerhet komplisert, av flere årsaker:

- Det finnes ingen konkrete dimensjonerende utfordringer å måle beredskaps- og krisehåndteringsevnen mot, spesielt på nasjonalt nivå. Det er vanskelig å utvikle arbeidsprosesser som er sporbare og som kobler målsettinger og tiltak i tilstrekkelig grad. Hvordan kan vi da avgjøre hva som er et tilstrekkelig nivå for arbeidet med samfunnssikkerhet?
- Det kan bygge seg opp lokale særtolkninger av hva som er de viktigste utfordringene, og beredskapsarbeidet innen ulike sektorer og på ulike nivåer blir ikke samkjørt godt nok.
- Arbeidet blir reaktivt i stedet for forebyggende. Hendelser som faktisk inntreffer får stor oppmerksomhet i etterkant, mens hendelser som ennå ikke har skjedd ikke når opp på prioriteringslisten.

I likhet med BAS 1 utviklet og brukte BAS 6 scenarioer for å konkretisere hvilke typer utfordringer Norge og norske interesser kan bli utsatt for i framtiden. Ut fra dette blir det mulig å utlede hvilke kapasiteter som er nødvendige for å håndtere situasjonene. Deretter kan det som finnes av kapasiteter i dag måles opp mot dette behovet, slik at det er mulig å beskrive om dagens situasjon er tilfredsstillende, og eventuelt hvilke kapasiteter som mangler — og mulige konsekvenser av dette.

Dekker dagens arbeid med sikkerhet og beredskap hele spekteret av potensielle uønskede hendelser? Hvilke typer hendelser blir i tilfelle ikke omfattet av dagens beredskapsplanlegging? Øver vi på de riktige hendelsestypene? For å bidra til å svare på disse spørsmålene, etablerte BAS 6-prosjektet en typologi over alle uønskede hendelser som kan true vår sikkerhet. Basert på denne typologien utviklet FFI et sett av scenarioer for arbeidet med samfunnssikkerhet.

Scenarioer for samfunnssikkerhet

Prosjektet etablerte et sett med 20 scenarioer som beskriver komplekse hendelsesforløp som kan ha omfattende konsekvenser. Hensikten med scenarioer er å lage et grunnlag for samtale og utvide det mentale kartet for aktørene i totalforsvaret. Scenarioene kan danne utgangspunkt for debatter, skrivebordøvelser og beredskapsanalyser hos sivile og militære aktører. Scenarioene skal dekke sentrale aspekter som krisekommunikasjon, sivil-militære utfordringer, den internasjonale dimensjonen og næringslivets rolle gjennom privat-offentlig samarbeid.

FFIs scenarioer ble utviklet parallelt med DSBs nasjonale risikobilde i 2011, og FFI og DSB hadde og har en god dialog i arbeidet med å utvikle scenarioer. Mens DSBs scenarioer er utviklet med bakgrunn i en risikovurdering med vekt på sann-


HARGELSAKER

synlighet og konsekvens, har FFI tilstrebet å bre ut hele utfordringsspekteret for store konsekvenser for også å dekke scenarioer som på kort sikt virker lite sannsynlige. De utviklede scenarioene skal:

- være relevante for å teste ut sivilt-militært samarbeid
- beskrive hendelser med store konsekvenser
- beskrive hendelser som kan ramme norske interesser primært i Norge
- tilrettelegge for at både store og små kommuner kjenner seg igjen i noen av problemstillingene
- ta med noen relevante scenarioer for kjemikalieberedskap, da dette er valgt som et av områdene for analyse av nasjonal beredskap

Scenariobeskrivelsene har fire faser av hendelsesforløpet: oppbygningsfasen, akuttfasen, redningsfasen og normaliseringsfasen. Det er også utviklet en spørsmålsbank med generelle spørsmål til scenarioene som grunnlag for diskusjon og videre analyse. I tillegg har vi under hvert scenario inkludert spørsmål som kan være til hjelp for å sette i gang en diskusjon rundt beredskap. Scenarioene er derfor også et verktøy som kan hjelpe aktører innen totalforsvaret til å arrangere skrivebordøvelser og gruppediskusjoner om beredskapsevne og rolleforståelse. Forutsetningen er at scenarioene brukes riktig. De må videreutvikles og tilpasses formålet. Et utvalg av scenarioene i BAS 6 ble benyttet til å analysere nasjonal beredskap og krisehåndtering.

Hva skjer ved et væpnet angrep?

Scenarioet «væpnet angrep» ble brukt som grunnlag for en analyse av nasjonal kriseledelse og sivilt-militært samarbeid. Scenarioet beskriver en situasjon der en annen stat bruker militære maktmidler mot Norge for å presse gjennom rettigheter i nordområdene. Hensikten med analysen var å studere i hvilken grad totalforsvaret var i stand til å understøtte både Forsvarets og samfunnets behov i en slik situasjon.

Omstillingen i Forsvaret og sivil beredskap etter den kalde krigen førte til at sivil side konsentrerte seg om fredstidskriser, mens Forsvaret var mest opptatt av operasjoner i utlandet. Før og under BAS 6 gikk oppmerksomheten mot nordområdene og forsvar av norsk territorium. Det var derfor relevant å undersøke hvilke følger disse skiftene fikk. Viktige spørsmål var:

- Hvem har overordnet ansvar på nasjonalt nivå, og blir ansvar og roller oppfattet som klare?
- Er det samsvar mellom sivile og militære behov for samordning og faktisk samordning?
- Er det samsvar mellom sivile og militære behov for ressurser (både personell og materiell) og reell tilgang til ressurser?
- Er aktuelle nasjonale kriseplaner oppdatert og øvd innenfor relevante områder?

Under et væpnet angrep er Forsvaret avhengig av støtte fra det sivile samfunnet blant annet til forsyning av mat og drivstoff, tungtransport, flytting av styrker og verkstedkapasitet. Samfunnet blir utfordret med økt etterspørsel og redusert bemanning i et slikt krisesamarbeid med Forsvaret. Det offentlige og det private må også samarbeide mye mer enn vanlig for blant annet å transportere skadde mennesker og reparere ødelagt infrastruktur. Analysen viste at nødvendige avtaler ikke var på plass for slikt samarbeid. Myndighetene hadde heller ikke planlagt godt nok for å ta imot Nato-styrker.

Analysen viste samarbeidsutfordringer mellom sivile myndigheter og Forsvaret både for å etablere og vedlikeholde et felles og oppdatert situasjonsbilde, og i ansvaret for sivilbefolkningens sikkerhet. Det er betydelige avvik mellom behovene for sivile og militære ressurser og hva som vil være tilgjengelig i en slik krise. Viktige funn var:

- Uavklarte ansvarsforhold mellom ulike sivile aktører.
- Avvik mellom behov for sivil-militær samordning og faktisk samordning.
- Selv om det eksisterer oppdaterte nasjonale kriseplaner, er de ikke alltid kjent i departementene og heller ikke øvd på.
- Sivile myndigheter har ofte ikke tilgang til graderte datanett. Det vanskeliggjør og forsinker utveksling av gradert informasjon.
- Sivile avtaler og beredskapsordninger for å dekke Forsvarets behov for varer og tjenester i en slik situasjon har ikke vært prioritert.

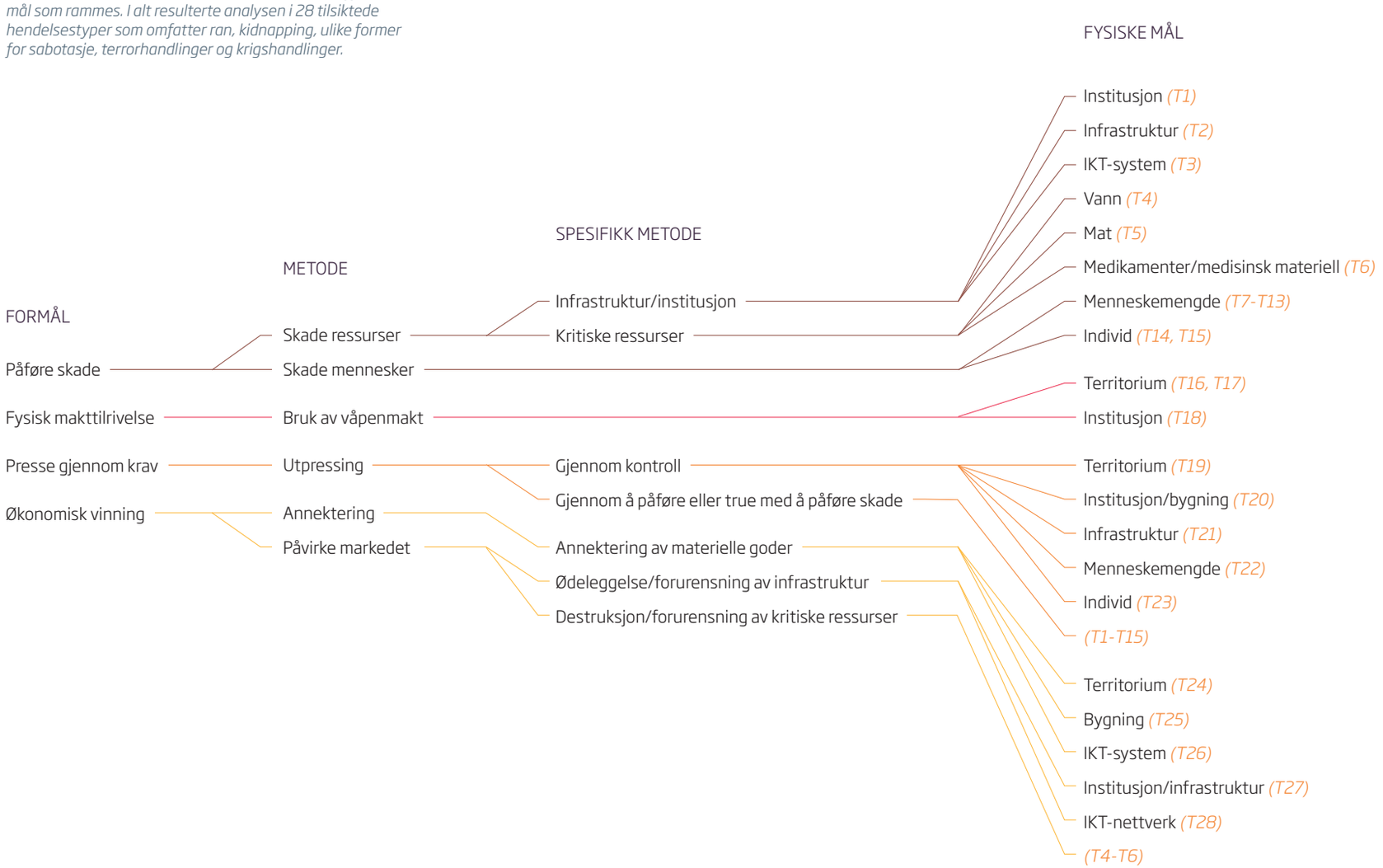
Disse problemstillingene for totalforsvaret i et liknende scenario ble fulgt opp i BAS 7-prosjektet. ■

Typologi over
77 UØNSKEDE HENDELSER

Totalt presenterer typologien 77 uønskede hendelsestyper, fordelt på tilsiktede og utilsiktede hendelser. Innenfor hver hendelsestype er variasjonsmulighetene store, og i tillegg er det mulig å koble sammen kjeder av hendelser. Typologien gir derfor et godt bilde av prinsipielle uønskede hendelser som kan true norsk sivil og militær sikkerhet. Vi skiller mellom to hovedtyper: tilsiktede handlinger og utilsiktede hendelser.

FFI Forsvarets forskningsinstitutt

TILSIKTEDE HANDLINGER *er uønskede hendelser der en aktør bevisst forårsaker hendelsen. Disse hendelsestypene er grovt inndelt etter aktørens kortsiktige formål, som kan være å påføre skade, fysisk tilrive seg makt, presse gjennom krav eller oppnå økonomisk vinning. Hendelsestypene er videre delt inn i aktørens metode og hvilke fysiske mål som rammes. I alt resulterte analysen i 28 tilsiktede hendelsestyper som omfatter ran, kidnapping, ulike former for sabotasje, terrorhandlinger og krigshandlinger.*



TILSIKTET HANDLING (T)
Sabotasje mot institusjon (T1)
Sabotasje mot infrastruktur (T2)
Logisk angrep mot institusjon/infrastruktur (T3)
Forurensning av drikkevann (T4)
Forurensning av mat (T5)
Sabotasje av medisindepot/ medisinsk materiell (T6)
Konvensjonelt massedrapsangrep (T7)
Nukleært angrep (T8)
Radiologisk angrep (T9)
Kjemisk angrep (T10)
Biologisk angrep (T11)
Berserkerepisode (massedrap utført av en gjerningsperson) (T12)
Pogrom (systematisk vold mot gruppe) (T13)
Attentat mot offentlig representant (T14)
Hatkriminalitet (T15)
Invasjon (T16)
Separatistisk maktbruk (T17)
Kupp (T18)
Utpressing gjennom territoriell kontroll (T19)
Utpressing gjennom kontroll over kritisk institusjon (T20)
Utpressing gjennom kontroll over kritisk infrastruktur (T21)
Gisseltaking (T22)
Bortføring/kidnapping (T23)
Okkupasjonsutbytting (T24)
Større ran (T25)
Logisk angrep for å tilrive seg goder (T26)
Sabotasje mot institusjon/ infrastruktur (T27)
Logisk angrep mot institusjon/ infrastruktur (T28)

UTILSIKTET HENDELSE (U)
Storm (U1)
Flom (U2)
Stort snøfall (U3)
Kraftig regnvær (U4)
Tørke (U5)
Ekstrem varme (U6)
Ekstrem kulde (U7)
Jordskjelv (U8)
Vulkanutbrudd (U9)
Flodbølge (U10)
Fjellskred (U11)
Jordskred (U12)
Snøskred (U13)
Kollisjon/nedfall (U14)
Stråling (U15)

UTILSIKTEDE HENDELSER *er delt i fire hovedkategorier av totalt 49 hendelsestyper: naturhendelser, svikt, akutt sykdom/skadedyrsutbredelse og aggregerte individuelle handlinger. Sammenlignet med tilsvarende arbeider har denne typologien to nye egenskaper. Den inkluderer en ny klasse uønskede hendelser, aggregerte individuelle handlinger. I tillegg gjør den det enkelt å kombinere flere hendelsestyper i et scenario. Hoveddimensjonene i typologien er årsak og primærkonsekvens, men typologien har også flere underdimensjoner.*

Radioaktivt utslipp (U16)
Biologisk utslipp (U17)
Kjemisk utslipp (U18)
Eksplosjon/brann i bygg (U19)
Skogbrann (U20)
Strukturell kollaps (U21)
Transportulykke (U22)
Svikt i kraftforsyning (U23)
Svikt i elektronisk kommunikasjon (U24)
Svikt i vanntilførsel (U25)
Svikt i avløp (U26)
Svikt i transport (U27)
Svikt i olje- og gassforsyning (U28)

Svikt i bank- og finanssystemer (U29)
Svikt i matforsyning (U30)
Svikt i helsetjenester (U31)
Svikt i sosial- og trygdetjenester (U32)
Svikt i evnen til å håndheve lov og orden (U33)
Svikt i nød- og redningstjenesten (U34)
Svikt i kriseledelse (U35)
Svikt i evnen til å forsvare landet (U36)
Svikt i evnen til å detektere hendelser som truer livsmiljøet (U37)
Svikt i renovasjon (U38)
Menneskebåren epidemi (U39)
Insektbåren epidemi (U40)

Næringsmiddelbåren epidemi (U41)
Dyrebåren epidemi (U42)
Epidemisk dyresykdom (U43)
Epidemisk plantesykdom (U44)
Akutt skadedyrsutbredelse (U45)
Mangel på livsnødvendige varer og tjenester (U46)
Akutt mangel på arbeidskraft og kompetanse (U47)
Mangel på innkvartering (U48)
Mangel på grensekontroll (U49)

FORSTÅELSE OG FOREBYGGING AV RADIKALISERING I SKANDINAVIA

I forskningsprosjektet *Searching the unknown: discourses and effects of preventing radicalization in Scandinavia* (RADISKAN) stiller forskerne spørsmål om hvilke forståelser og oppfatninger som underbygger forebyggende arbeid mot radikalisering og voldelig ekstremisme.

Definisjoner i RADISKAN

RADIKALISERING: en prosess der en person i økende grad aksepterer bruk av vold for å nå politiske, ideologiske eller religiøse mål.

VOLDELIG EKSTREMISME: aktiviteten til personer og grupperinger som er villige til å bruke vold for å nå sine politiske, ideologiske eller religiøse mål.

Politiets sikkerhetstjeneste (PST) har i sine trusselvurderinger de siste årene vært bekymret for radikaliserte individer og grupper som er villige til å bruke vold for å oppnå politiske mål. Internasjonale forhold og konflikter utenfor Norge har fått stor betydning for den nasjonale trusselsituasjonen, spesielt med tanke på såkalte fremmedkrigere.

I de skandinaviske landene foregår det i dag mobilisering og rekruttering til ulike grupper som er villige til å bruke vold for å oppnå politiske, ideologiske eller religiøse mål. Landene har alle utviklet egne handlingsplaner rettet mot radikalisering og voldelig ekstremisme. Felles for Skandinavia er at sivilsamfunnet har ansvar for å utpeke grupper som er sårbare for radikalisering og voldelig ekstremisme. Lokalsamfunn og kommuner har også et hovedansvar for å implementere forebyggende tiltak.

Forskerne i RADISKAN vil finne ut mer om hva som faktisk skjer på bakkenivå som følge av at myndighetene har blitt mer opptatte av radikalisering. Hvordan forholder lokalsamfunn seg til utfordringene med å iverksette forebyggende tiltak? RADISKAN ser også nærmere på hvordan forhandlingene rundt potensielt sårbare individer og grupper foregår, og på hvordan definisjoner av radikalisering virker inn på tillit både mellom grupper og innenfor grupper.

Ingen enkel profil

Regjeringens handlingsplan mot radikalisering og voldelig ekstremisme fra 2014 legger opp til en bred forebyggende innsats basert på tidligere erfaringer med generelt kriminalitetsforebyggende arbeid og arbeid med høyreekstreme. Et underliggende premiss er en slags merket løype fra sosial eksklusjon – definert som manglende tilhørighet til det norske samfunnet – til radikalisering og videre voldelig ekstremisme og terrorisme.

Årsakssammenhengen som handlingsplanen trekker fram, mangler vi imidlertid kunnskap om. Studier av personer som blir radikalisert og rekruttert inn i voldelig ekstremisme viser at det ikke finnes en enkel profil, og at å forebygge radikaliseringsprosesser dermed vil kreve ulike virkemidler. Det er et uttrykt behov for mer forskning som kan gi innsikt i hvilke prosesser som ligger til grunn for ulike typer av radikalisering og ekstremisme, både på gruppe- og individnivå. Per i dag mangler vi rett og slett et godt nok empirisk fundament til å kunne utvikle målrettede forebyggende tiltak.

Etnografisk feltarbeid

Studien er hovedsakelig finansiert gjennom Forskningsrådets Program for samfunnssikkerhet 2013-2018 (SAMRISK II). Prosjektet ledes fra FFI, og er et samarbeidsprosjekt med Universitet i Aarhus og Fafo, Institutt for anvendte internasjonale studier. Prosjektet hadde oppstart høsten 2014 og vil løpe til høsten 2018. Gjennom RADISKANs ulike delprosjekter vil det bli utført etnografiske feltarbeid i Danmark, Sverige og Norge. Ett mål er at prosjektet skal bidra til mer kunnskap om utfordringer ved å forebygge radikaliseringsprosesser.


Byens drikkeva
Det er forbudt å bade, vas
fiske eller på annen måte
Mari vannet.
likeledes forbudt å
ned ved vannet.
Vannverksjefen

HELHETLIG SIKKERHET

UTEN MYTER

I BAS 7-prosjektet ble det gjennomført analyser av nasjonal beredskap primært i den øvre delen av krisespekteret. Analysene bygget videre på tidligere scenarioarbeid og allerede gjennomførte analyser i BAS-prosjektene. I dette prosjektet ble det blant annet forsket på teknologiens påvirkninger på samfunnssikkerheten, og noen betraktninger omkring dette temaet er tatt med her.

Den teknologiske utviklingen bidrar til å endre sårbarheten i det moderne samfunnet med rask takt. Ofte fordi vi blir mer avhengige av komplekse strukturer der vi i tilsvarende mindre grad har oversikt over den faktiske sårbarheten. Samtidig får vi nye hjelpemidler til å drive effektiv krisehåndtering i form av kommunikasjonshjelpemidler og beslutningsstøttesystemer. Stilt overfor en så rask utvikling opplever vi usikkerhet til hvordan dette påvirker vår sårbarhet og vår evne til å håndtere kriser. En betydelig utfordring ved denne usikkerheten er at det oppstår et mangfold av myter. Dette er myter som kan virke dramatisk for utviklingen av helhetlig sikkerhet i samfunnet — dersom de ikke møtes med tilstrekkelig kunnskap. FFI er svært opptatt av å bidra til denne helhetlige sikkerhetsforståelsen.

Elektronisk kommunikasjon (EKOM)

- Teknologiutviklingen bidrar til å effektivisere samfunnet, men samtidig blir hver enkelt av de kritiske samfunnsfunksjonene mer kompleks og uoversiktlig.
- Samtidig ser vi at EKOM brukes til flere funksjoner i samfunnet og i flere virksomheter. Kompleksiteten og omfanget øker.
- Dette fører igjen til at færre vet hvor omfattende og kompleks EKOM egentlig er, og vi får en kunnskapsmangel hos dem som bruker denne avanserte teknologien.

Krisehåndtering i et digitalisert samfunn

Hvordan påvirker den teknologiske utviklingen sårbarheten i samfunnet? FFI har studert og analysert sammenhengen mellom økt avhengighet av elektronisk kommunikasjon (EKOM) og vår evne til krisehåndtering og ledelse i alvorlige kriser.

Samfunnet er helt avhengig av EKOM for at alt skal fungere i det daglige. Vi har i stadig raskere takt tatt i bruk og gjort oss avhengige av nye måter å kommunisere på, både i yrkeslivet og privat. Alle har mobiltelefon, flere og flere bruker til dels avanserte applikasjoner, og vi henter og deler informasjon på internettbaserte tjenester. Bortfall av mobiltelefoni og internett skjer med jevne mellomrom. Det fører til ulemper og utfordringer for oss, både som individer og virksomheter, men stort sett klarer vi å håndtere dette uten alvorlige konsekvenser for liv og helse. I normalsituasjoner, uten at det samtidig skjer andre alvorlige hendelser, tåler stort sett samfunnet dette.

Totalforsvaret, nasjonal kriseledelse og sivil beredskap har gjort seg svært avhengig av EKOM-tjenester for å løse nasjonale og internasjonale kriser. Samtidig vet vi at EKOM-tjenestene for eksempel er helt avhengige av fungerende krafttilførsel for å fungere. Avhengigheten av svært sammensatte tjenester som EKOM og kraft har fått utvikle seg uten at de utfordringene dette gir gjennom økt sårbarhet har vært særlig påaktet. Denne sårbarheten har blitt synlig gjennom hendelser som Lærdalsbrannen og uværet Dagmar.

Vi har brukt en scenariobasert analyse til å skaffe innsikt i dette. Analysen viser hvilke EKOM-tjenester vi er avhengige av i en konkret, svært alvorlig utfordring for landet i en krise som følge av en ytre trussel. Grunntemaet har vært beskyttelse av sivilbefolkningen og hvilke sårbarheter EKOM-tjenester påfører vår evne til krisehåndtering. Det scenarioet vi har brukt som utgangspunkt for datainnsamlingen, er en tenkt, alvorlig sikkerhetspolitisk krise med fare for et nært forestående væpnet angrep helt nord i landet.

Basert på scenarioet har vi, ved en framgangsmåte i fem trinn, identifisert relevante krisehåndteringsaktører på lokalt, regionalt og sentralt nivå, og hvordan disse er organisert. Videre har vi kartlagt innbyrdes relasjoner dem imellom og det behovet for kommunikasjon som oppstår for å løse viktige oppgaver. Det omfatter også hvilke kommunikasjonsmidler som er tilgjengelige og som brukes av disse aktørene. Dette gjorde vi ved å spille ut scenarioets ulike faser for utvalgte aktører i to kommuner og på fylkeskommunalt nivå. I tillegg intervjuet vi aktører på strategisk nivå. Informasjonen systematiserte vi i komplekse aktørkart for kommunikasjon mellom aktører på lokalt, regionalt og strategisk nivå. Kartene viser hvilke kommunikasjonsmedier de bruker i ulike faser av den tenkte situasjonens utviklingsforløp.

De tjenesteplattformene som er tilgjengelig er telefoni (både mobil og fast), internett, militær EKOM og andre mobile nett. Kartleggingen synliggjorde hvor behovet for og belastningen på EKOM ble størst på ulike tidspunkter i krisen. Den geografiske avstanden mellom aktører som må samhandle mer eller mindre kontinuerlig i denne krisen, er så stor at EKOM er den eneste muligheten for å kommunisere, og dermed nødvendig for evnen til å løse krisen. Studien viste at mobiltelefonen er den desidert viktigste kommunikasjonstjenesten selv i de mest alvorlige situasjonene Norge kan bli stilt overfor. Andre alternativ, som det nylig innførte Nødnettet og militære kommunikasjonstjenester, vil i en slik setting ha begrenset betydning blant annet fordi brukergruppen er for snever.

Sentrale aktører i denne og andre tilsvarende alvorlige kriser er politimesteren, Fylkesmannen og andre aktører i Fylkesberedskapsrådet. For å oppnå effektiv samhandling og ledelse av kriser må aktørene ha tilgang til kommunikasjonstjenester som er både sikre og robuste. I en tid der ulike former for mobilteknologi og sosiale medier blir et viktigere supplement til tradisjonelle kringkastingstjenester, blir det også stadig viktigere å utvikle sikre og robuste informasjonskanaler som kan nå ut til ulike deler av befolkningen. Den aller viktigste konklusjonen fra denne kartleggingen er at offentlig mobiltelefoni er det eneste felles kommunikasjonsmiddelet for totalforsvarsaktørene innen nasjonal kriseledelse, Fylkesmannen, kommunenes kriseledelse, nødetater, helseforetak og Forsvaret.

Ved en slik grunnleggende tilnærming viser det seg at reserveløsninger, som satellittelefon og andre former for dedikerte radionett, ofte blir en sovepute og gir en illusjon av redundans. I praksis vil det være vanskelig å ta i bruk slike reserveløsninger i konkrete situasjoner fordi de vanligvis ikke brukes i øvelser, det vil være vanskelig å finne kontaktinformasjon til de andre aktørene, og mange andre aktører har ikke tilsvarende muligheter. Dette er et eksempel på et område der det utvikles myter som i ytterste konsekvens kan være svært alvorlige for sikkerheten i samfunnet. Denne utviklingen vil forsterkes over tid dersom vi ikke er årvåkne og har evne til å tilegne oss hensiktsmessig kunnskap.

FFIs studie illustrerer hvordan teknologiutviklingen og nye måter å bruke teknologien på fører med seg nye sårbarheter. En økende avstand mellom brukerne og deres forståelse av den teknologien de blir stadig mer avhengige av, er en viktig del av utfordringen. Fordi de teknologiske tjenestene etter hvert er så komplekse, samtidig som brukergrensesnittet er så velutviklet, har den jevne bruker liten forståelse for den underliggende infrastrukturen og teknologien bak tjenestene. Denne manglende teknologiske kunnskapen fører til manglende kunnskap og forståelse for sårbarhet og sammenheng mellom tjenester.

Vi må se systemer i sammenheng

Hvordan kan vi måle evne til krisehåndtering? Dette kan være utfordrende sett i lys av det norske sektoransvaret, det vil si ansvaret som ligger under de respektive fagdepartementene. Hvordan kan vi sikre en helhetlig tilnærming til samfunnssikkerhet og beredskap?

IKT inngår med mer vitale tjenester i alle typer beslutningsstøtteprosesser innen beredskap og krisehåndtering, og infrastrukturer som vannforsyning, el-forsyning og transporttjenester. Både beredskapsfunksjoner og infrastrukturer kan rammes mer effektivt gjennom angrep mot data- og kommunikasjonssystemer. Hvilke muligheter for å trenge inn i disse systemene foreligger, og hvilke alvorlige konsekvenser kan dette ha for selve leveransene som infrastrukturen gir — enten det er vann, kraft, transporttjenester, eller noe annet?

For å forstå hvilken sårbarhet og reell risikoutfordring dette medfører for samfunnet, er det avgjørende å forstå hvordan de

fysiske systemene og IKT-systemene er satt sammen med økende kompleksitet. Et konkret eksempel illustrerer mulige utfordringer knyttet til en helhetlig sikkerhetstilnærming, og hvilke utfordringer det gir dersom en avgrenset revisjon brukes som mål på sikkerhet. Eksempelet er fra infrastrukturen i vann- og avløpstjenester i en stor norsk by. Vannforsyningsinfrastruktur består av fysisk infrastruktur, det vil si vannreservoar, renseanlegg, høydebasseng, rørsystemer, pumper og annet. Den fysiske infrastrukturen er i stor utstrekning, men ikke fullstendig, styrt av IKT-systemer. Vanntrykket i det aktuelle systemet blir i hovedsak til gjennom høydeforskjeller og gravitasjon, og ikke gjennom IKT-styrte pumper.

En revisjon av systemets IKT-sikkerhet har funnet at en del av disse systemene har betydelige mangler og ikke har god nok sikring mot inntrengning. Det betyr i prinsippet at en skadevolder kan bryte seg inn i IKT-systemet. Dette kan potensielt være alvorlig. IKT-revisjonen trakk den konklusjonen at dette var en metode angripere kunne bruke for å påvirke leveransene av vann til befolkningen, men uten å gå nærmere inn på systemet i sin helhet.

På tross av revisjonens konklusjoner fant vi at det ikke er vesentlig sannsynlig at en angriper, utover korte tidsintervaller, vil kunne skade evnen til å levere sikker vannforsyning og sørge for sikker avløpshåndtering gjennom angrep mot IKT-systemene. Tilstanden i IKT-systemene er helt klart ikke tilfredsstillende, men totalsystemet har i hovedsak likevel tilstrekkelig med «mekanismer» for å hindre alvorlige konsekvenser for fysisk infrastruktur. Svak IKT-sikkerhet kan likevel være et problem for en så vidt tillitskrevende tjeneste som vannforsyning. Frykt kan med andre ord være en større utfordring enn teknisk brudd i vannforsyningen.

FFIs arbeid viste at fysisk sikring er svært viktig, både med hensyn til IKT-angrep og forgiftningsforsøk. Ensidig fokus på å rette opp systemtekniske mangler innen IKT-sikkerhet, og ikke se sikkerhet under ett, vil dermed kunne falle uheldig ut for brukerne av vann- og avløpstjenesten. Også i dette tilfellet ser vi at myter om sårbarheter og sikkerhet påvirker sikkerhetsarbeidet. IKT-baserte infrastrukturer er et svært komplekst område som også er utilgjengelig for mange, og grobunnen for myteutvikling er stor.

En viktig konklusjon er at det er helt sentralt å forstå samspillet mellom en avansert fysisk infrastruktur og en IKT-infrastruktur for å vurdere samlet sikkerhet. De som vurderer sikkerhet og sårbarheter i systemer, må være i stand til å tilegne seg tilstrekkelig dybde- og breddekunnskap om virksomheten eller infrastruktursystemet. De viktigste verdiene i systemet som helhet må identifiseres. I motsatt fall risikerer vi å feiltolke vår egen risiko og å prioritere ressurser feil. Dette eksempelet fra vannsektoren viser hva manglende helhetsforståelse kan føre til når vi skal vurdere sikkerhet og evne til krisehåndtering.

I gamle dager var det enklere

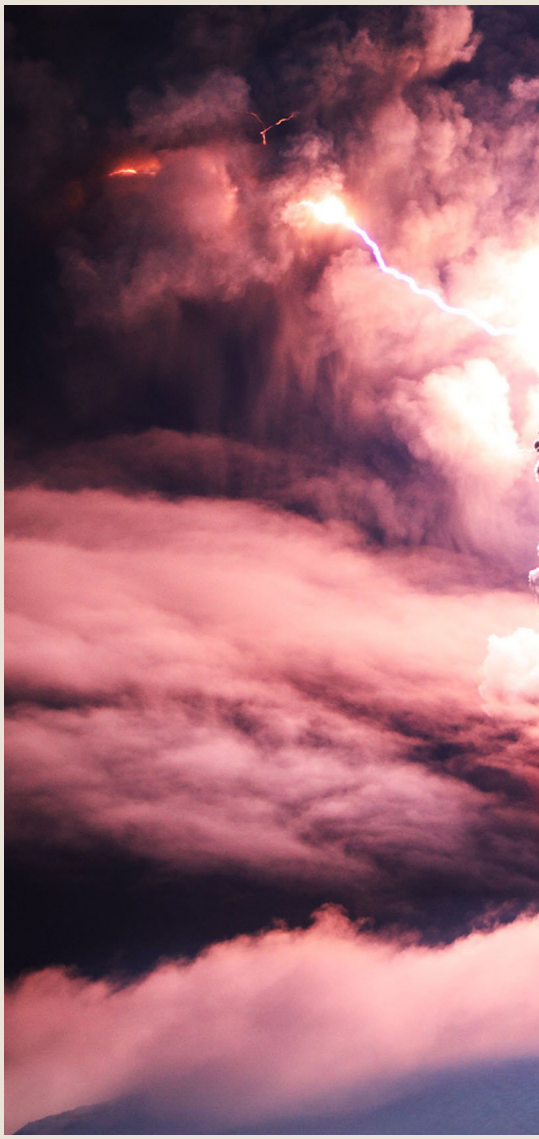
Hva er så de viktigste verdiene for vår samfunnssikkerhet i dag? En faktor som bidrar til at det har blitt vanskeligere å vurdere helhetlig sikkerhet, er at samfunnsverdiene våre er spredt på flere hender enn tidligere. De er hos offentlige sivile og militære myndigheter, men slettes ikke bare der. I stor grad ligger verdier i det private næringslivet, med norsk, men også med økende innslag av internasjonalt eierskap. I gamle dager var det enklere: De største og viktigste verdiene var våre forsvarshemmeligheter, og trusselen var stabil. I takt med samfunnsutviklingen blir verdiene våre flere og mer avhengig av hverandre. Utviklingen i det globale samfunnet har ført til at trusselbildet har blitt mindre oversiktlig og forutsigbart. Flere verdier og det uforutsigbare trusselbildet gjør oss sårbare.

BAS 7 konkluderte med at økt teknologisk avhengighet av elektronisk kommunikasjon gir økt sårbarhet for nasjonal krisehåndtering og ledelse. BAS 7 utførte også andre studier. Forsvarets forsyningsberedskap ble gått etter i sømmene, og det ble gjort utredninger om samarbeidet mellom politi og forsvar. Nasjonal beredskap for kjemiske, biologiske, radiologiske og nukleære (CBRN) hendelser ble vurdert, også opp mot det europeiske samfunnet og kommunikasjon til befolkningen i slike kriser. Beskyttelse mot høyenergetiske mikrobølger var også en del av BAS 7. Øvelser og øvelsesevaluering var også temaer i prosjektet, og dette arbeidet blir videre utdypet i det pågående BAS 8. Et eksempel på en konkret krisehåndteringsstudie som ble gjort i BAS 7, er askeskykrisen i 2010. ■

Fra 7. til 11. juni 2015 samarbeidet sivile og militære partnere i øvelse Oslofjord. Øvelsen skulle bidra til å styrke samfunnssikkerheten. Innsatsstyrke Polar Bear VI og politiet sikret sammen politihuset i Østfold.
Foto: Forsvaret

SUKSESSKRITERIER FOR GOD KRISEHÅNDTERING

- Erkjenne krisen
- Etablere kriseledelse
- Avklare roller og ansvar
- Involvere alle berørte parter (offentlige/private, sivile/militære)
- Involvere fagmiljøer
- Kontinuerlig oppdatering av situasjonsbildet
- Etablere samordningsfora (lokalt, regionalt, nasjonalt og internasjonalt)
- Etablere en koordinert kommunikasjonsstrategi
- Forberede og innføre tiltak, inkludert bistandsordninger



HÅNDTERING AV ASKESKYKRISEN

I april 2010 ble europeisk luftfart rammet av utbruddet fra vulkanen Eyjafjallajökull på Island. Det krevde krisehåndtering og sivilt-militært samarbeid som vi kan lære av.

Mangel på empirisk grunnlag fra reelle hendelser for relevante kriser i den øvre delen av krisespekteret er en utfordring. Innrettingen av nasjonal, regional og lokal krisehåndtering skal være så lik som mulig i fred, krise og væpnet konflikt jamfør likhetsprinsippet. I den grad det er erfaringer fra reelle hendelser vi kan dra nytte av, og som kan ha en potensiell overføringsverdi, må vi derfor gjøre det.

Askeskyens spredning førte til at hele luftrommet over Norge ble stengt torsdag 15. april 2010. Restriksjonene i luftfart og flyvirksomhet skapte utfordringer i helse-Norge, spesielt i Nord-Norge der vi i stor grad er avhengig av luftambulanser. Askeskykrisen utløste militær støtte til helseberedskapen i Nord-Norge. Videre var det nyttig lærdom å trekke fra håndteringen av denne krisen, fordi den krevde samarbeid og samvirke mellom en rekke myndigheter og andre aktører nasjonalt og internasjonalt.

Myndighetene tidlig ute

Norske myndigheter og berørte aktører håndterte generelt sett askeskykrisen på en god måte. Myndighetene var tidlig ute med å etablere en sentral kriseledelse og samordning på sentralt nasjonalt nivå ved Regjeringens kriseråd (RKR) med Samferdselsdepartementet som lederdepartement. Hele åtte departementer, Statsministerens kontor og seks andre etater deltok i RKR. Dette bidro til at de sentrale myndighetenes krisehåndtering framsto enhetlig, godt fundert og at informasjonen fra departementene ble godt koordinert.

Luftfartsaktørene kom stort sett godt ut av krisen. De lyktes med informasjon til og kommunikasjon med andre myndigheter, private aktører, media og publikum. Det største usikkerhetsmomentet var knyttet til målinger og prognoser for askespredning i luften og hvilke konsekvenser dette egentlig hadde for flyene. Myndighetene valgte først en føre-var-strategi med en meget restriktiv linje som innebar å stenge luftrommet. Dette ble senere omgjort til et tresoners regime. Helseberedskapen i Nord-Norge ble styrket både ved forsterkning fra helseforetak i Sør-Nor-

Utbruddet fra vulkanen Eyjafjallajökull på Island la en askesky over store deler av Europa i april 2010. *Foto: NTB Scanpix/wenn.com*

ge og bruk av militære ressurser. Det sivil-militære samarbeidet ble styrket og forbedret under askeskykrisen.

Nye initiativ etter krisen

I etterkant av askeskykrisen har vi observert ulike typer læring som har ført til nye initiativ. For eksempel er det etablert en egen etatsgruppe for vulkansk aske, alternative beredskapsruter for busser i Nord-Norge, forskning og utvikling av askesensorer på fly, ubemannede droner som kan måle askenivå, videreutvikling av video-basert akuttmedisinsk konferanse i helsesektoren og ulike internasjonale initiativ som skal forbedre kunnskapen om vulkanaske og dens effekt på flymotorer. Sosiale medier vokste fram som en viktig informasjonskanal for flyselskapene. Flere aktører, for eksempel Fylkesmannen i Finnmark, så nytteverdien av sosiale medier i sin kommunikasjon med befolkningen og innførte selv dette høsten 2012.

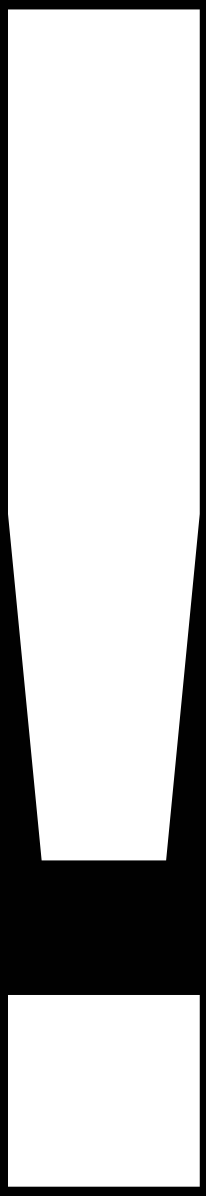
Hva var det ved myndighetenes håndtering av denne krisen som ga suksesskriterier for god krisehåndtering? Myndighetene erkjente krisen på et tidlig stadium og etablerte kriseledelse der de berørte parter, både offentlige og private, sivile og militære, ble involvert. Roller og ansvar ble avklart, og Samferdselsdepartementet ble etablert som lederdepartement. Myndighetene framsto oppdatert om situasjonsbildet. Fagmiljøene ble konsultert og involvert gjennom hele krisen. Myndighetene etablerte nødvendige samordningsfora lokalt, regionalt, nasjonalt og internasjonalt. Kommunikasjon med media og publikum framsto enhetlig og godt koordinert. Dette vitner om en klart etablert kommunikasjonsstrategi. Tiltak og bistand ble etablert for å håndtere flyforbudet. Dette var særlig viktig i våre nordligste fylker der avhengigheten av flytrafikk er stor.

DET SOM ENNÅ IKKE HAR SKJEDD

Teknologiutviklingen de siste tiårene har ført til drastiske endringer i samfunnet som påvirker trusler og sårbarheter. Dermed kan vi ikke anta at vår forståelse av samfunnssikkerhet basert på tidligere hendelser gir et godt nok grunnlag for å møte utfordringene vi får i framtiden. For å håndtere noe som tidligere ikke har skjedd, må vi være klar over hvordan systemer fungerer og hva som potensielt er sårbart. Vi må kunne identifisere og forstå områder som er i rask utvikling og kan føre til plutselige eller uventede utfordringer. Med økt forståelse for risiko, sårbarhet og trusler i et moderne samfunn i utvikling står vi bedre stilt til å møte framtidens utfordringer innen samfunnssikkerhet.

Ettersom utfordringene vi står overfor stadig blir mer sammensatte, er det nødvendig med samarbeid mellom flere aktører og sektorer for å finne løsninger. Det pågående prosjektet BAS 8 legger vekt på behovene og systemene for samarbeid mellom sivile og militære, så vel som tverrsektorielle øvelser. På disse områdene er det mye som gjenstår før vi har gode systemer på plass for en helhetlig samfunnssikkerhet tilpasset et moderne samfunn.

BAS 8 undersøker sivil-militær krisehåndtering og beredskap, og er basert på behovet for å forske videre på problemstillinger som ble tatt opp i BAS 7 i tillegg til noen



nye områder. Arbeidet med og FFIs bidrag til Forsvarssjefens fagmilitære råd (FMR 2015) har også medvirket til utformingen av BAS 8.

Samfunnsbehov i endring

Et mer dynamisk trusselbilde gjør det nødvendig å tenke nytt om samfunnssikkerhet. Trusler mot samfunnet er i utvikling, og truslene kan ramme samfunnet på andre måter enn tidligere. Stadig større avhengighet av teknologi gjør samfunnet, også Forsvarets virksomhet, utsatt for cybertrusler. Cybertrusler kan rettes mot en rekke systemer og tjenester som har stor betydning for alle, fra enkeltindivid til næringsvirksomheter og Forsvaret. Det er et interessant utviklingstrekk at militære og sivile infrastrukturer for informasjonsformidling i stor grad er i ferd med å smelte sammen, samtidig som disse infrastrukturene har blitt globale.

Ting skjer raskere og krever raskere respons. Denne utviklingen gir Norge nye utfordringer. De nye truslene vi vil kunne stå overfor vil i langt større grad enn tidligere være dynamiske og mangfoldige. De vil ofte kunne avsettes raskt med svært kort varslingstid, og de vil kunne være sammensatte kombinasjoner av vidt forskjellig virkemidler. Truslene vil også utvikles raskere, og det vil være langt vanskeligere enn tidligere å forstå truslenes opphav og innhold på forhånd. Det er ikke lenger gitt at en statlig aktør med fiendtlige hensikter vil erklære krig og bruke konvensjonelle metoder mot en uniformert motstander. Aktørene kan være alt fra individer til grupper og statlige aktø-

Offentlige instanser samarbeidet med Forsvaret for å øve på å behandle skadd personell under øvelse Oslofjord 2015.
Foto: Forsvaret

rer. Deres intensjoner, midler og mål kan variere. Særlig trusler i cyberdomenet vil være vanskelige å spore. Det blir dermed svært viktig at forvaltningen er i stand til å møte det som måtte komme på en effektiv måte, og det må være mulig å gjøre dette svært raskt. Det dreier seg i hovedsak om et økende behov for en styrket etterretningsbasert analytisk tilnærming med tilhørende organisering og kompetanse. Effektiv koordinering på tvers av dagens forvaltningsnivåer og myndighetsområder blir svært viktig.

BAS-forskningen vil bidra til å øke forståelsen for endrede rammeforutsetninger for samfunnssikkerheten og til å tenke framover i samarbeid med aktørene. Det åttende prosjektet i rekken ser på overordnede problemstillinger fra de tidligere BAS-prosjektene i lys av samfunnsutviklingen, i tillegg til at nye forskningsområder har kommet til. Prosjektet vil ved forskning på fire hovedområder komme med anbefalinger for hvordan samfunnet – både det sivile samfunn og forsvarssektoren – kan samarbeide om samfunnssikkerhet. Etter 22. juli 2011 ble det innført et nytt prinsipp for krisehåndtering: samvirkeprinsippet. Samvirke og samarbeid må til for å møte særlig sammensatte utfordringer som krever at flere departementer, underliggende etater og aktører griper inn samtidig. Det er flere utfordringer ved tverrsektorielt samarbeid og støtte mellom aktører som gjør det nødvendig med bedre forståelse og planlegging for at samvirke skal fungere i praksis. Dette vil forskningen i BAS utdype.

De fire hovedområdene vi forsker på i BAS 8, er sivil støtte til Forsvaret, kritisk infrastruktur og kritiske samfunnsverdier, krisehåndteringsøvelser og sivile beskyttelsestiltak. En effektiv og helhetlig beredskap og krisehåndtering innebærer gjensidig støtte og samarbeid mellom Forsvaret og det sivile samfunn i hele krisespekteret. Det krever en klar ansvarsfordeling, samvirke og kommunikasjon i ledelse av kriser og utnyttelse av samfunnets samlede ressurser. I BAS 7 avdekket vi flere områder innenfor logistikk og forsyningsberedskap som bør forbedres, og dette tar vi videre i BAS 8.

Rammeforutsetningene for totalforsvaret har endret seg betydelig etter den kalde krigen, og BAS 8 vil bidra til å gi et bedre kunnskapsgrunnlag om gjensidig sivilt-militært samarbeid innen totalforsvaret, med vekt på sivil støtte og logistikk til Forsvaret i sikkerhetspolitisk krise og væpnet konflikt. Videre skal BAS 8 utrede kritisk infrastruktur og kritiske samfunnsverdier for å få en helhetlig nasjonal forståelse av hvilke verdier som er kritiske og bør beskyttes på grunn av sin betydning for nasjonal sikkerhet. Komplekse samfunnsinfrastrukturer som kraftforsyning, telekommunikasjon, transport og informasjon/ledelse er hovedtemaer i denne forskningen. Tilnærming og metodikk er viktige redskaper når vi skal vurdere sårbarhet, risiko og beredskap for komplekse samfunnsinfrastrukturer. Slik metodikk vil vi videreutvikle. Et hovedspørsmål er hvorvidt en helhetlig framstilling av nasjonal risiko, trusler og sårbarhet er mulig. Dette vil vi forsøke å avklare. Et bedre kunnskapsgrunnlag kan gi bedre risikostyring, utforming og prioriteringer av helhetlige og balanserte beskyttelsestiltak.

BAS 8 tar også for seg en konkret studie av samfunnets behov for sivile beskyttelsestiltak på oppdrag fra DSBs sivilforsvarsavdeling. I studien vil vi blant annet bruke relevant informasjonsgrunnlag fra tidligere BAS-prosjekter. Funnene vil vi vurdere og oppdatere. Hovedspørsmålet er hvilke sivile beskyttelsestiltak et moderne samfunn trenger i lys av dagens trussel- og risikobilde. I studien skal vi i tillegg utrede tilfluktsrom og eksisterende befolkningsvarslingsregime. I BAS 1 ble det gjennomført en studie av tilfluktsrom og luftvarsling, og funnene fra denne studien er nå, etter nesten 20 år, klare for revisjon. Vi tar nå for oss mange av de samme problemstillingene, men med et bredere perspektiv som dekker hele krisespekteret og tar høyde for samfunnsendringer siden 90-tallet.

Vi må øve på å samarbeide

Øvelser er nøkkelen til at samvirke skal fungere. Et viktig grunnlag for en effektiv beredskap er tverssektorielle krisehåndteringsøvelser der aktørene øver på samhandling innen visse scenarioer. Prosjektet vil forske på øvelser og effekten av øvelser, og på metoder for planlegging, gjennomføring, evaluering og erfaringslæring av tverrsektorielle øvelser. En utfordring ved mange av øvelsene som blir gjennomført, er at oppfølging og læring er mangelfull. Hva er årsaken til at identifiserte læringspunkter fra øvelser ikke følges opp eller gir ønsket læring? Hva skal til for å lage effektive øvelser for samtrening av Forsvaret og sivil beredskap, som gir god mestringsfølelse og samvirkekultur?

Mange ulike deltakere er involvert i tverrsektorielle øvelser, for eksempel nødetatene, Sivilforsvaret og Forsvaret, i tillegg til direktorater og departementer. I denne forskningen vil vi konsultere organisatorer og øvelsesdeltakere om øvingsmål, gjennomføring, resultater og læring. Vi vil ta inn både nasjonale og internasjonale øvelser som grunnlag for studien. Studien vil legge særlig vekt på hvordan læring fra øvelser best kan tilbakeføres i form av forbedringer i organisasjoner og planverk. Prosjektet skal så gi råd og anbefalinger til Forsvaret og sivile myndigheter.

Gjennom BAS 8-prosjektet skal FFI videreutvikle et godt kunnskapsgrunnlag for å styrke det sivil-militære samarbeidet innen totalforsvaret i alvorlige kriser. Dette gjelder særlig sivil støtte til Forsvaret. I tillegg vil vi finne bedre metoder for å forstå risiko og sårbarhet, spesielt innen gjensidige avhengigheter i kritiske infrastrukturer og kritiske samfunnsverdier.

BAS 8 har videre som mål å bidra til å utnytte tverrsektorielle kriseøvelser bedre. Vår forskning vil kunne bidra til at de sivile myndighetene og Forsvaret lærer av erfaringer og forbedrer praksis etter øvelser. Forskningsaktivitetene i BAS vil kunne bidra til å bedre samfunnssikkerheten i Norge. ■

REFERANSER

Birkemo, G. A., Grunnan, T. & Nystuen, K. O. (2015). Kommunikasjon mellom totalforsvarsaktører i en kompleks sikkerhetspolitisk krise. *FFI-rapport 2015/00372* (Begrenset), Kjeller, Forsvarets forskningsinstitutt.

Forsvarets forskningsinstitutt (2014). *FFI-FAKTA: Krisehåndtering i et sårbart cybersamfunn.* Kjeller.

Forsvarssjefens fagmilitære råd (2015). *Et forsvar i endring.* Oslo, Forsvaret.

Fridheim, H. & Hagen, J. M. (2007). Beskyttelse av samfunnet 5 (BAS5): Sårbarhet i kritiske IKT-systemer – Sluttrapport, *FFI-rapport 2007/00874.* Kjeller, Forsvarets forskningsinstitutt.

Fridheim, H., Hagen, J. M. & Henriksen, S. (2001). En sårbar kraftforsyning. *FFI-rapport 2001/02381.* Kjeller, Forsvarets forskningsinstitutt.

Hagen, J. M. & Nystuen, K. O. (1999). Beskyttelse av samfunnet med vekt på offentlig telekommunikasjon. *FFI-rapport 99/00240.* Kjeller, Forsvarets forskningsinstitutt.

Hagen, J. M., Fridheim, H. & Grunnan, T. (2010). Sikkerheitspolitisk krise, nasjonal kriseleiing og sivilmilitært samarbeid. *FFI-rapport 2010/01009* (Begrenset). Kjeller, Forsvarets forskningsinstitutt.

Hagen, J. M., Knutsen, B. O., Bjørnenak, M. & Sandrup, T. (2011). Scenarioer for samfunnssikkerhet og nasjonal beredskap, *FFI-rapport 2011/00648* (Begrenset). Kjeller, Forsvarets forskningsinstitutt.

Hagen, J. M., Rodal, G. H., Hoff, E., Lia, B., Torp, J. E. & Gulichsen, S. (2003). Beskyttelse av samfunnet med fokus på transportsektoren. *FFI-rapport 2003/00929.* Kjeller, Forsvarets forskningsinstitutt.

Hæsken, O. M., Olsen, T. G. & Fridheim, H. (1997). Beskyttelse av samfunnet (BAS): sluttrapport. *FFI-rapport 97/01459.* Kjeller, Forsvarets forskningsinstitutt.

Innstilling til Stortinget 234 (2003-2004) til Stortingsproposisjon 42 (2003-2004). Oslo, Forsvarskomiteen.

Innstilling til Stortinget 49 (2004-2005) til Stortingsmelding 39 (2003-2004). Oslo, Forsvarskomiteen.

Justis- og beredskapsdepartementet & Forsvarsdepartementet (2015). *Støtte og samarbeid. En beskrivelse av totalforsvaret i dag.* Oslo.

Løkken, K. H., Grunnan, T. & Birkemo, G. A. (2015). Muligheter og begrensninger ved kommunikasjonssystemer for bruk i krisehåndtering. *FFI-rapport 2015/01453.* Kjeller, Forsvarets forskningsinstitutt.

Maal, M., Endregard, M. & Birkemo, G. A., (2012). Askeskyen fra vulkanutbruddet på Island i 2010 – norsk krisehåndtering og noen erfaringer. *FFI-rapport 2012/01319.* Kjeller, Forsvarets forskningsinstitutt.

Meyer, S. (2009). Typologi over uønskede hendelser. *FFI-rapport 2009/00447.* Kjeller, Forsvarets forskningsinstitutt.

NOU (2000:24). *Et sårbart samfunn. Utfordringer for sikkerhets- og beredskapsarbeidet i samfunnet.* Oslo, Justis- og politidepartementet.

NOU (2006:6). *Når sikkerheten er viktigst. Beskyttelse av landets kritiske infrastruktur og kritiske informasjonssystemer.* Oslo, Justis- og politidepartementet.

Stortingsmelding 24 (1992-93). *Det fremtidige sivile beredskap.* Oslo, Justis- og politidepartementet.

Stortingsmelding 29 (2011-2012). *Samfunnssikkerhet.* Oslo, Justis- og beredskapsdepartementet.

Stortingsmelding 37 (2004-2005). *Flodbølgekatastrofen i Sør-Asia og sentral krisehåndtering, Justis- og politidepartementet.* Oslo, Justis- og beredskapsdepartementet.

Stortingsmelding 47 (2000-2001). *Telesikkerhet og -beredskap i et telemarked med fri konkurranse.* Oslo, Samferdselsdepartementet.

Stortingsmelding 48 (1993-94). *Langtidsplan for det sivile beredskap 1995-98.* Oslo, Justis- og politidepartementet.

Stortingsproposisjon 48 (2007-2008). *Et forsvar til vern om Norges sikkerhet, interesser og verdier.* Oslo, Forsvarsdepartementet.

The President's Commission on Critical Infrastructure Protection (1997). *Critical Foundations: Protecting America's Infrastructures.* Washington DC.

Les mer på ffi.no/BAS

FFI Forsvarets forskningsinstitutt