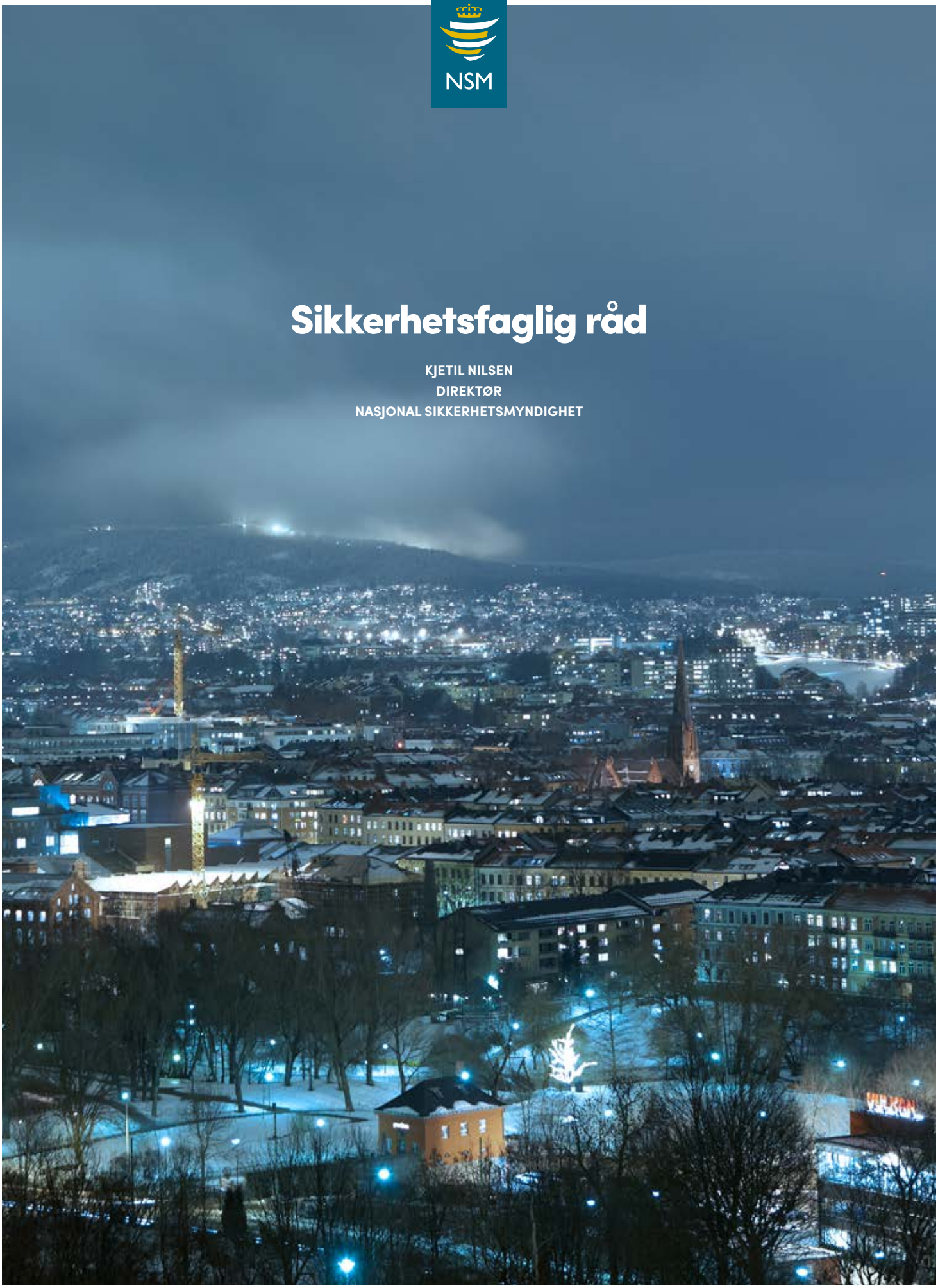
NSM

Sikkerhetsfaglig råd

KJETIL NILSEN
DIREKTØR
NASJONAL SIKKERHETSMYNDIGHET



Nasjonal sikkerhetsmyndighet (NSM) er Norges ekspertorgan for informasjons- og objektsikkerhet, og er det nasjonale fagmiljøet for IKT-sikkerhet.

Innhold

Forord

Norge er et trygt samfunn. Men samfunnet er ikke uten sårbarheter. Utviklingen i Norge og verden for øvrig skjer hurtig og er stadig mer uforutsigbar. Dette gjør at vi må ha sterkere fokus på de sikkerhetsmessige sårbarhetene i samfunnet vårt slik at vesentlige behov kan løses. Samtidig må vi erkjenne at all risiko ikke kan elimineres, og at samfunnet må leve med en viss restrisiko. I Sikkerhetsfaglig råd gir vi i Nasjonal sikkerhetsmyndighet (NSM) vårt syn på hvordan sårbarheter i det norske samfunnet kan utbedres og dermed hvordan sikkerhetsrisikoen kan reduseres til et akseptabelt nivå. Mange av forslagene vil kreve ytterligere utredninger, og vi imøteser oppdrag om dette.

Målsettingen med NSMs sikkerhetsarbeid er å sikre samfunnsverdier mot alvorlige, tilsiktede uønskede handlinger. Disse verdiene, enten det dreier seg om informasjon, infrastruktur eller menneskelig aktivitet, er i sin tur viktige for at de overordnede samfunnsmålene skal nås. Til disse målene hører blant annet nasjonens eksistens og vår demokratiske styreform, en sikker og effektiv forvaltning, befolkningens velferd, et konkurransedyktig næringsliv samt trygghet for den enkelte i hverdagen. Samtidig må sikkerhetsarbeidet sees i et perspektiv hvor befolkningens personvern ivaretas like godt og sidestilles med behovet for sikkerhet, slik at sikkerhetstiltakene ikke undergraver de samme verdiene som skal beskyttes. I følge Finansdepartementets perspektivmelding må vi ta høyde for hardere økonomiske prioriteringer i årene som kommer, blant annet som følge av en økende andel eldre og en gradvis utfasing av petroleumsvirksomheten. Samtidig vil trangere tider i næringslivet gjøre det vanskeligere for private virksomheter å prioritere utgiftsposter som ikke gir dokumenterbar økonomisk effekt. Vi må derfor ha derfor ha kostnadseffektivitet som en rettesnor for tiltak vi ønsker å gjennomføre.

To innsatsfaktorer står i en særstilling for å oppnå samfunnsmålene fremover: 1) Vår evne til å fatte riktige beslutninger og gjennomføre disse, og 2) kvaliteten på digitale løsninger. Å dyrke frem kunnskaps-

basen og hele tiden optimalisere bruken av IKT vil være strategisk avgjørende for Norge som samfunn i tiden som kommer. Dette krever ressurser og det krever omstilling på mange områder.

Ett område som krever ressurser og omstilling er sikkerhetsarbeidet i samfunnet. Vi må gjennom sikker kommunikasjon, sikker lagring av informasjon og sikker infrastruktur kunne være trygge på at vi oppnår samfunnsmålene på en mest mulig kosteffektiv måte. Dette er et behov som vi ikke er alene om i Norge, men som vi deler med resten av Europa. Sikkerhetsfaglig råd legger til grunn at det innenfor de sikkerhetsområder hvor NSM har ansvar fremdeles vil være behov for endringer, både i form av kraftfulle grep men også mindre justeringer av det bestående. Mindre justeringer vil på flere områder være tilstrekkelig fordi mye av det sikkerhetsarbeidet som i dag gjøres allerede er godt begrunnet i et fremtidsperspektiv, og derfor bør videreføres og styrkes. For å få til den nødvendige helhetlige omstilling i sikkerhetsarbeidet kreves imidlertid én kraftfull overordnet endring som de øvrige forslag vil være avhengig av. Endringen innebærer å gå fra å se på sikkerhet som organisatoriske og tekniske reaktive svar på frittstående behov som dukker opp, eller som påtvinges samfunnet utenfra, til å se på sikkerhet som en viktig forutsetning som det aktivt må tilrettelegges for i forkant på en helhetlig måte (security by design). Denne endringen i grunnleggende tenkning om sikkerhet må skje på alle nivåer.

Sikkerhetsarbeidet har i for stor grad fokusert på usammenhengende organisatoriske og tekniske løsninger, som er fragmenterte og suboptimale. Dette blir mer utfordrende desto mer nettverksorientert samfunnet blir. Sikkerhet som en grunnleggende forutsetning vil legge til rette for det motsatte, nemlig årvåkenhet, helhetsblikk, sammenheng, klarhet, gjenbruk og langsiktig besparelse.

Etterspørselen etter NSMs tjenester er økende. Vi åpnet høsten 2014 et kompetansesenter som tilbyr opplæring i samfunnssikkerhet. Allerede etter få måneder hadde etterspørselen overgått tilbudet. Deltakelsen på NSMs årlige sikkerhetskonferanse øker år for år. Etterspørselen etter råd og veiledning fra NSM er likeledes økende. Dette er bare noen få eksempler. Som følge av omstillingen nevnt ovenfor vil den øke ytterligere.

Hvordan mener NSM at den fortsatt økende etterspørselen etter direktoratets tjenester skal dekkes, i lys av at kompetansetilfanget på kort sikt er begrenset? Svaret må være at NSM kraftsamler rundt de kjerneoppgavene direktoratet er best i stand til å utføre, og at andre oppgaver fordeles på en hensiktsmessig måte mellom nasjonale etater og sektormyndigheter. Det må inngås langsiktig partnerskap med akademia med tanke på kunnskapsutvikling, og næringslivet må stimuleres til å levere sikkerhetstjenester og -produkter. Ikke minst må samfunnet ettespørre sikrere tjenester. Hensynet til å skape miljøer som evner å levere gode løsninger må veie tungt.

Tiltak for å redusere sårbarhet i samfunnet vil kreve ressurser. Vi i NSM er bedt om å utrede vår fremtidige innretning innenfor en flat budsjettbane. Gitt omstillingsbehovet og interneffektiviseringskravet må NSM uansett i noen grad refokusere sin virksomhet. Når dette har skjedd, vil vi ha en organisasjon som er noe bedre tilpasset de behov vi mener samfunnet og virksomhetene har. Likevel mener vi at det vil være samfunnsmessig riktig å bruke ytterligere ressurser på å redusere sårbarheter, i forkant, både gjennom NSM og andre aktører. Hvis disse tiltakene ikke gjennomføres, mener vi at restrisikoen vil være uakseptabel for samfunnet.

Kjetil Nilsen
Sjef Nasjonal sikkerhetsmyndighet

Sammendrag

Forsvarsministeren har gitt NSM i oppdrag å utarbeide et Sikkerhetsfaglig råd om trender, utviklingstrekk og foreslåtte sikkerhetstiltak innen NSMs fagområder frem mot 2020 og videre fremover. Sikkerhetsfaglig råd skal, på samme måte som fagmilitært råd, fungere som et grunnlag for langtidsplanen for forsvarssektoren. Rådet skal også være et underlag for stortingsmeldingen om samfunnssikkerhet fra Justis- og beredskapsdepartementet.

Bakgrunnen for oppdraget er de omfattende sikkerhetspolitiske endringene som har skjedd siden forrige langtidsplan for forsvarssektoren ble utarbeidet. Trusselaktørene benytter mer avanserte metoder enn tidligere, og risiko- og sårbarhetsbildet er blitt mer komplekst. Endringene i trusselbildet bidrar til en situasjon hvor vi må ta høyde for ingen eller kort varslingstid ved uønskede tilsiktede hendelser. Kortere varslingstid utfordrer samfunnets evne til å reagere med ønsket kraft og hurtighet når et angrep skjer. Det stiller større krav til forebygging, gjennom både redusering av sårbarheter og hendelseshåndtering.

Sikkerhetsfaglig råd er NSMs vurdering av hvordan Norge bør innrette arbeidet med forebyggende sikkerhet frem mot 2020. Vurderingen omfatter områdene IKT-sikkerhet, personellsikkerhet og fysisk sikkerhet. NSM foreslår i rådet til sammen 73 ulike tiltak for å styrke arbeidet i årene fremover. Tiltakene dreier seg både om tydeliggjøring av roller, regelverksendringer, iverksettelse av nye prosjekter, tekniske tiltak, kompetansetiltak, og nye strategier.

TYDELIGGJØRE ORGANISERING, LEDELSE OG KOORDINERING. Sikkerhet utøves i dag på flere nivåer i samfunnet. Vi foreslår å tydeliggjøre roller og utvikle rolleforståelsen. Dette er spesielt nødvendig innen IKT-sikkerhet. Blant tiltakene er en tydeliggjøring og styrking av Justis- og beredskapsdepartementets samordningsrolle og en styrket evne til koordinering og samvirke mellom aktørene i beredskaps- og krisesituasjoner.

STYRKE IKT-SIKKERHETEN. NSM foreslår en rekke tiltak for å styrke IKT-sikkerheten i Norge. Blant tiltakene er å implementere innholdet i EUs direktiv for nettverks- og informasjonssikkerhet, og etablere nasjonale minimumskrav og anbefalinger som vil legge til rette for samordning. For å styrke sikkerheten foreslår vi å forenkle og legge til rette for færrest mulig miljøer for utvikling av drift av IKT-systemer i det offentlige, og kraftsamle om én offentlig nasjonal leverandør av høygraderte IKT-løsninger[1]. Det bør utvikles felles sikre mobil- og IKT-løsninger for sensitiv og begrenset informasjon. Kryptering av informasjon bør være et nasjonalt satsningsområde. Tilsyn med IKT-sikkerheten i norske virksomheter bør økes, og tilsynskompetansen bør samordnes.

STYRKE EVNEN TIL HÅNDTERINGEN AV CYBERANGREP. Vi foreslår en betydelig styrking av samfunnets samlede evne til hendelseshåndtering av cyberangrep. NSMs kapasitet til å koordinere håndteringen av cyberangrep bør styrkes. Det bør etableres et nasjonalt cybersikkerhetssenter i ett felles bygg, som kan samle og skape synergieffekter mellom ulike sektormiljøer, myndigheter og eiere av sam-

funnskritisk IKT-infrastruktur. En slik samling skal ikke forrykke eksisterende ansvarsforhold. Nasjonal deteksjonsevne av cyberangrep bør styrkes og videreutvikles.

STYRKE PERSONELLSIKKERHETEN. NSM foreslår å profesjonalisere og effektivisere arbeidet med sikkerhetsklareringer. Vi støtter de foreslåtte endringer i sikkerhetsloven, som innebærer færre klareringsmyndigheter. Andre tiltak innen området er å automatisere innhenting fra kilderegistre, tiltak for å redusere risikoen for innsidere, og utarbeide og etablere en ny tverrsektoriell ordning for bakgrunnskontroll på områder utenfor sikkerhetsloven.

STYRKE ARBEIDET MED FYSISK SIKKERHET. Det er behov for å ha fortsatt oppmerksomhet på at skjermingsverdige objekter utpekes, klassifiseres og sikres på en tilstrekkelig måte. Arbeidet med råd og veiledning om fysisk sikkerhet bør styrkes. Blant tiltakene er å vurdere om det bør etableres et felles rådgivingssenter for å samle og dermed utnytte samfunnets ressurser på en best mulig måte.

SAMARBEID OG INFORMASJONSDELING MED NÆRINGSLIVET. NSM ønsker å legge til rette for at samfunnets samlede kompetanse om sikkerhet utnyttes best mulig, blant annet gjennom å styrke samarbeidet med næringslivet. NSM anbefaler en ordning for akkreditering av private selskaper for utøvelse av sikkerhetstjenester, og forenkling av arbeidet med leverandørklareringer. NSM anbefaler også et kompetanseprogram om sikkerhetsdesign for aktørene i byplanlegging og byggeprosjekter, for å øke kunnskapen om god sikkerhetsdesign i det offentlige rom.

STYRKE KOMPETANSEN OM SIKKERHET. Etter NSMs syn er det behov for en betydelig styrking av kompetansen, spesielt innen IKT-sikkerhet, i samfunnet. Vi foreslår blant annet en sterkere satsning på IKT-sikkerhet på universiteter og høgskoler, etablering av egne bachelor- og mastergrader i IKT-sikkerhet, en innføring i IKT-sikkerhet i lærerutdanningen, og å styrke og videreutvikle undervisningen ved NSMs kurssenter i forebyggende sikkerhet.

STYRKING AV NSM. Gjennom oppdraget med Sikkerhetsfaglig råd er NSM for egen del bedt om å utrede tiltak som kan iverksettes innenfor dagens økonomiske ramme, og tiltak som vil kreve en økning av tildelingene. Flere av tiltakene innen organisering og ledelse kan implementeres, og noen av tiltakene innen IKT-sikkerhet, personellsikkerhet, fysisk sikkerhet og kompetanse kan påbegynnes. NSMs vurdering er likevel at nødvendige kraftfulle grep for å styrke sikkerheten i årene fremover vil kreve en betydelig økning av tildelingene til NSM for i tilstrekkelig grad kunne følge opp fagområdene som er beskrevet i denne rapporten. ⊙

[1] Høygraderte IKT-løsninger er løsninger som brukes for sikkerhetsgradering KONFIDENSIELT og høyere.

Innledning

Forsvarsministeren ga i brev av 5. januar 2015 NSM i oppgave å utarbeide et Sikkerhetsfaglig råd (SFR). Forsvarssjefen er også gitt i oppdrag å fremme et fagmilitært råd (FMR). Disse rådene skal danne grunnlag for en ny langtidsplan for forsvarssektoren for perioden 2017-2020, som skal utarbeides av Forsvarsdepartementet (FD) og som vil komme som en proposisjon til Stortinget våren 2016. SFR skal også inngå i grunnlaget for en melding til Stortinget om samfunnssikkerhet som skal fremmes av Justis- og beredskapsdepartementet (JD).

TOLKNINGEN AV MANDATET. Av mandatet fremgår at SFR skal utarbeides innen rammen av NSMs ansvarsområde. De oppgaver som tilligger Sjef NSM i instruks gitt i desember 2014 danner utgangspunktet for hva som inngår i direktoratets ansvarsområde og er tema for dette rådet. Instruks for Sjef NSM er vedlagt dette dokumentet (Vedlegg A). Rådet skal omfatte helheten i det forebyggende sikkerhetsarbeidet, herunder tiltak for tilstrekkelig beredskap på sikkerhetsområdet. Rådet omfatter ikke bare tiltak som bør iverksettes av NSM, men også tiltak som bør iverksettes av departementer, andre etater og virksomhetene selv.

Rådet skal i henhold til mandatet være et faglig innspill til arbeidet med ny langtidsplan for forsvarssektoren og melding om samfunnssikkerhet. Vi har valgt ikke å la disse to formål være strukturdannende i rapporten, men har gjennomgående søkt å tydeliggjøre hvilke tiltak som retter seg særskilt mot henholdsvis militær og sivil side der dette har vært naturlig. Der det ikke er presisert, gjelder beskrivelser og tiltak i rapporten alle sektorer i samfunnet.

Rådet skal videre omfatte en vurdering av trender innenfor områdene personell-, informasjons- og objektsikkerhet, og hvordan disse påvirker forsvarssektoren og sivil sektor. Innenfor informasjonssikkerhetsområdet er dessuten NSM spesielt bedt om å ha et særlig fokus på IKT-sikkerhet. Så vel informasjonssikkerhet som objektsikkerhet handler om å sørge for god IKT-sikkerhet, personellsikkerhet og fysisk sikkerhet. For å tydeliggjøre dette, har vi i vårt råd valgt å holde oss til følgende tre fagområder: IKT-sikkerhet, fysisk sikkerhet og personellsikkerhet. Det understrekes at begrepene IKT-sikkerhet og fysisk sikkerhet omfatter administrative tiltak i tillegg til rent tekniske tiltak. For en nærmere presentasjon av begrepshierarkiet vises til kapitlet «Informasjonssikkerhet, personellsikkerhet og objektsikkerhet» senere i denne innledningen.

Rådet skal i henhold til mandatet beskrive tverrsektorielle og internasjonale avhengigheter og fremme relevante forslag til tiltak. Disse aspekter er beskrevet i dokumentet der det er naturlig.

En rekke tiltak som beskrives i rådet vil ha relevans for lovarbeidet som nylig er igangsatt (Sikkerhetsutvalget). Disse er samlet i eget vedlegg til dette dokumentet (Vedlegg B).

Kostnadseffektiv organisering presiseres som et ufravikelig krav for alle deler av forsvarssektorens virksomhet, og at dette er en forutsetning som skal legges til grunn for videreutviklingen av NSM som etat. Sikkerhetsfaglig råd er utformet slik at dette kravet oppfylles.

I Sikkerhetsfaglig råd er NSM bedt om å utrede videre utvikling av NSMs drift gitt at dagens budsjettramme på kapittel 1723, post 01 holdes på 2015-nivå, alternativt en økning av rammen med 0,5% prosent. Dette vil utgjøre en økning på drøyt 1 million kroner, eller cirka ett årsverk. En økning av budsjettrammen på 0,5 prosent anses ikke som vesentlig, og utredes ikke nærmere.

Vi foreslår en rekke begrunnede tiltak som vil forbedre sikkerhetstilstanden, men som vil medføre tilførsel av ressurser til NSM i perioden 2017-2020. Kostnadsberegningen av disse tiltakene vedlegges ikke denne rapporten.

SENTRALE BEGREPER. En rekke begreper benyttes gjennomgående i dette dokumentet som grunnlag for beskrivelser og drøftinger. Disse forklares kort i det følgende.

SIKKERHET. Sikkerhet i sin alminnelighet defineres som tilstand av fravær av uønskede hendelser, frykt eller fare. Begrepet brukes i tillegg om tiltakene som benyttes for å oppnå denne tilstanden, og begrepet «sikring» ses også benyttet for dette. Innen sikkerhet skilles det mellom hva man ønsker

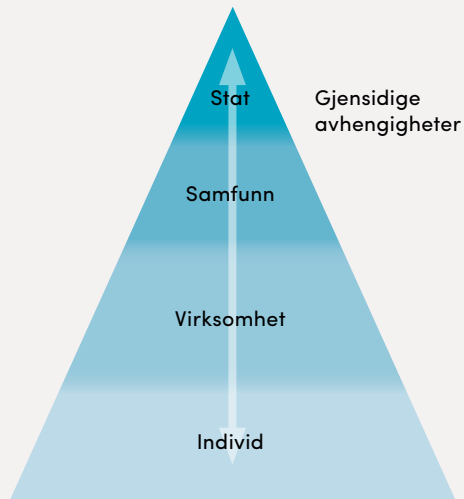
å beskytte seg mot; tilsiktede uønskede handlinger og tilfeldige hendelser. Enkelte typer tiltak kan være de samme uavhengig av om du beskytter mot tilsiktede uønskede handlinger eller tilfeldige hendelser. For eksempel vil redundante IKT-systemer redusere konsekvensen av både sabotasje og brann. Sikkerhetsarbeidet innenfor NSMs ansvarsområde er begrunnet i behovet for å motstå tilsiktede uønskede handlinger. Arbeidet vil likevel i praksis også få betydning for det å forebygge og motvirke mer tilfeldige hendelser som kan medføre de samme skader.

FOREBYGGE OG HÅNDTERE. Kjernen i sikkerhetsarbeid er å forebygge at uønskede hendelser inntreffer. All erfaring tilsier likevel at man ikke kan satse på at det er tilstrekkelig, særlig ikke når hensikten er å motvirke handlinger som det kan stå ressurssterke aktører bak. Sikkerhetsarbeidet må derfor også bestå av evne til å håndtere uønskede hendelser om de skulle oppstå, begrense skadefølgen og om mulig gjenopprette sikker tilstand.

GRUNNSIKRING OG BEREDSKAP. Med grunnsikring menes sikkerhetstiltak som er iverksatt i en normalsituasjon. Beredskap er forberedelsen av de påbygningstiltak som på kort varsel iverksettes for å øke sikringstiltakene utover grunnsikringen, for eksempel styrket adgangskontroll i en situasjon med økt trussel. En annen form for beredskap er forberedelser til å håndtere en akuttsituasjon, krise eller en katastrofe, samt hvordan virksomheten raskt kan komme tilbake til normal produksjon igjen om skaden allerede har skjedd.

STATSSIKKERHET, SAMFUNNSSIKKERHET OG ANDRE SIKKERHETSHENSYN. Arbeidet med sikkerhet omfatter hele spekteret fra enkeltpersoners datamaskiner, offentlige registre, digitale styringssystemer (SCADA-systemer) i kritiske samfunnsfunksjoner og til politiets og Forsvarets kommando- og kontrollsystemer. Vi kan dele dette rent konseptuelt i fire nivåer; statssikkerhet, samfunnssikkerhet, virksomhetssikkerhet og individets sikkerhet, se figur 1. Disse fire nivåene kan også benyttes for å beskrive i hvilken grad myndighetene vil engasjere seg i sikkerhetsarbeidet i samfunnet.

FIGUR 1 NIVÅER AV SIKKERHET



Statssikkerhetsarbeidet vil si å ivareta statens eksistens, suverenitet, suverene rettigheter og integritet. Det er dette formålet sikkerhetsloven understøtter gjennom at den regulerer beskyttelse av verdier av betydning for rikets sikkerhet og selvstendighet og andre vitale nasjonale sikkerhetsinteresser. Sikkerhetsloven har et sterkt sektorovergripende perspektiv og har et særlig nedslag i forsvarssektoren, utenrikstjenesten, etterretnings- og sikkerhetstjenestene, sentralforvaltningen, sentrale deler av kritisk infrastruktur, sivile deler av totalforsvaret samt leverandører av varer og tjenester til disse.

Samfunnssikkerhet handler om å ivareta befolkningens liv, helse og trygghet, og å sikre sentrale samfunnsfunksjoner og viktig infrastruktur, og andre samfunnsmessige interesser mot skade. Dette er også et viktig område for statlig regulering av sikkerhet, men er kjennetegnet av mer sektorvise løsninger. Innenfor enkelte områder som for eksempel personvern har man tverrsektorielle regler.

Den enkelte virksomhet, privat eller offentlig,

har også et behov for på selvstendig grunnlag å sikre sin drift og sine interesser mot svindel og skadeverk. Det samme har enkeltindividet. Sikkerhet på disse nivåene fremkommer ofte som et resultat av forsikringsordninger som fremtvinger sikkerhetsløsninger for å oppnå premiereduksjoner.

For at modellen i figur 1 skal bli anvendbar i forståelsen av vårt digitale samfunn må den tilføres et tilleggsmoment – gjensidig avhengighet. Sikkerheten i en enkeltvirksomhet kan påvirke sikkerheten i lagene over og under, ofte uten at det er tydelig for virksomheten selv. Dette ved at sårbarheter i enkeltvirksomheter utnyttes til å angripe over internett eller kompromittere informasjonen til både samarbeidspartnere, kunder og brukere. Både Forsvaret og forvaltningen generelt bruker i dag stadig mer produkter og tjenester fra private leverandører. Private virksomheter vil gjennom slike oppdrag direkte involveres i statssikkerheten og samfunnssikkerheten. Videre vil individets handlinger og atferd gjennom at vi alle kommuniserer over internett kunne påvirke både egen og samfunnets sikkerhet. Manglende sikkerhet på individnivå kan dessuten ramme virksomheten individet arbeider i.

RISIKO, RISIKOSTYRING OG RISIKOAKSEPT. Risiko defineres som forholdet mellom faktorene verdier, trusler og sårbarheter. Dette forholdet er ofte omtalt som risikotrekanten.

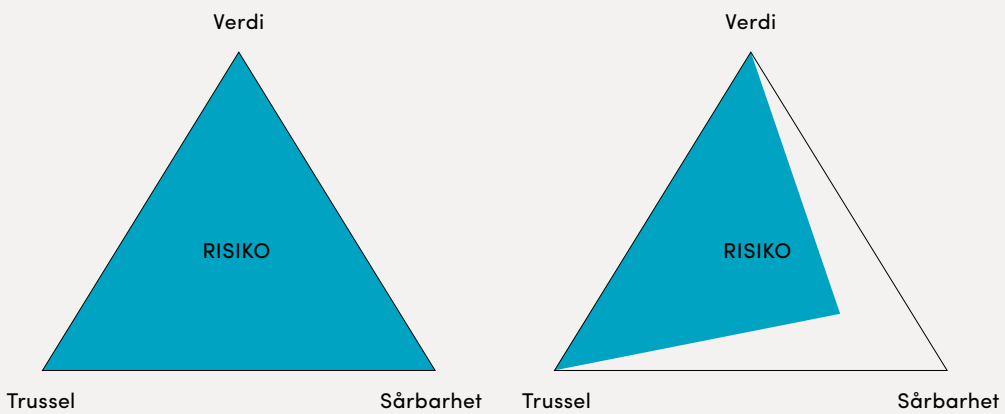
Et kjennetegn med tilsiktede uønskede hendelser er at vi ikke kan si når, hvor og med hvilke metoder en trusselaktør vil slå til. Trusselbildet ligger av den grunn utenfor det de fleste har mulighet til å gjøre noe med. Derfor må fokuset i sikkerhetsarbeidet rettes mot det vi kan gjøre noe med. Det vil si å identifisere verdiene og interessene som kan være mål for trusselaktørene, og redusere sårbarhetene som kan utnyttes.

Særlig viktig er det å etablere en oversikt over de verdier som finnes. En slik kartlegging kalles gjerne en verdivurdering. Den vil gi en oversikt og en rangering av de verdiene og interessene som er så viktige at de må beskyttes.

I risikostyringsarbeidet er det også vesentlig å kartlegge sårbarhetene, da det er disse vi først og fremst kan gjøre noe med gjennom sårbarhetsreduserende tiltak.

Erfaringer fra de siste årene, i forbindelse med kriser og hendelser i både det fysiske og det digitale rom, er at man i mange tilfeller ikke kan forvente

FIGUR 2 RISIKOTREKANTEN – AREALET I TREKANTEN ER ET UTTRYKK FOR RISIKO. FOR Å VURDERE RISIKO MÅ DET GJENNOMFØRES VERDIVURDERING, TRUSSELVURDERING OG SÅRBARHETSVURDERING.



at det vil være en varslingstid som gir mulighet til å iverksette ytterligere tiltak. Derfor må det prioriteres å ha en god grunnsikring og evne til å håndtere hendelser. God risikostyring er et viktig virkemiddel.

INFORMASJONSSIKKERHET, PERSONELLSIKKERHET OG OBJEKTSIKKERHET[2]. Informasjonssikkerhet dreier seg om å sørge for at informasjon og underliggende infrastruktur er tilstrekkelig sikret gjennom god IKT-sikkerhet, personellsikkerhet og fysisk sikkerhet. Informasjonssikkerhet som begrep favner dermed videre enn IKT-sikkerhet. Fysisk sikkerhet omfatter tiltak for å beskytte mot fysiske anslag mot informasjon eller objekter. IKT-sikkerhet og fysisk sikkerhet omfatter teknologiske og administrative sikringstiltak. Viktige prinsipper når det gjelder informasjonssikkerhet er:

- Konfidensialitet; at kun de som skal ha tilgang til informasjon får tilgang.
- Integritet; at informasjonen ikke blir endret i forhold til hva den skal være
- Tilgjengelighet; at informasjonen er tilgjengelig når det er behov for det

Objektsikkerhet dreier seg om å sørge for at objekter er tilstrekkelig sikret gjennom god fysisk sikkerhet, IKT-sikkerhet og personellsikkerhet.

Personellsikkerhet dreier seg om å sikre at personell og ansatte har en atferd som gjør at informasjon eller objekter ikke blir kompromittert; kort sagt at de ansatte er til å stole på.

SPESIELT OM IKT-SIKKERHET. Når det gjelder begreper som digitale angrep, er både betegnelser som IT-sikkerhet, datasikkerhet, digital sikkerhet og cybersikkerhet i bruk. Ulike betegnelser brukes i forskjellige bransjer og profesjoner. Begrepene er, med nyanseforskjeller, å betrakte som synonymer. I denne rapporten bruker vi IKT-sikkerhet spesifikt om informasjonsteknologiske og administrative sikringstiltak. Når det gjelder begreper som digitale angrep, cyberangrep, IKT-angrep, IT-angrep, informasjonsoperasjoner med videre, vil vi her bruke dataangrep og cyberangrep (som synonymer). Unntaket er der vi har rene henvisninger til andre kilder (som for eksempel rapporter fra Etterretningstjenesten eller andre). Ulike fagretninger legger ulike betydninger i betegnelsen dataangrep og cyberangrep. Når det gjelder betegnelser som digitale trusler, cybertrusler, IKT-trusler, IT-trusler, informasjonstrusler med videre vil vi her bruke cybertrusler. Vedrørende fremtidig omforent begrepsbruk vises til forslag i Del III om å erstatte IKT-sikkerhet som term med cybersikkerhet. Dette er på grunn av den stadig økende bruken av begrepet cybersikkerhet både internasjonalt og nasjonalt, og for å sikre at vi i Norge har en terminologi som vil være sammenlignbar også i internasjonale sammenhenger. ⊙

[2] Vedrørende anvendelsen av begrepene i denne rapporten vises til omtale i tolkningen av mandatet foran.

Del I

Situasjonsbilde

1. Overordnede trender

Trendene beskrevet under er basert på observerte endringer i samfunnet som NSM vurderer vil vedvare, og som samfunnet må ta høyde for når det innretter seg for å møte fremtidige sikkerhetsutfordringer.

SIKKERHETSPOLITISKE OG SAMFUNNSMESSIGE ENDRINGER.
Den sikkerhetspolitiske situasjonen har den siste tiden utviklet seg på en måte som stiller nye krav til sikkerhet i samfunnet. «Ekspertgruppen for forsvaret av Norge» (heretter benevnt Ekspertgruppen) beskriver blant annet et Russland med en mindre forsonende tone overfor NATO enn tidligere, i kombinasjon med en endret fremferd utenfor egne grenser.

Ekspertgruppen peker videre på at internasjonale konflikter de siste årene har vist seg å omfatte et bredere spenn av virkemidler enn hva vi er dimensjonert for å håndtere. Trusselaktørene benytter mer avanserte metoder enn tidligere. Risiko- og sårbarhetsbildet er blitt mer komplekst. Den økte terrortrusselen bidrar til en situasjon hvor vi må ta høyde for kort varslingstid ved slike tilsiktede uønskede hendelser. Kortere varslingstid utfordrer samfunnets evne til å reagere med ønsket kraft og hurtighet når et angrep skjer. Det tvinger frem en mer bevisst holdning til hvor stor risiko samfunnet er villig til å akseptere, for å kunne prioritere sine ressurser hensiktsmessig. Terrorhendelsen 22. juli 2011 viste oss hvor raskt en hendelse kan inntreffe.

De tverrsektorielle avhengighetene øker, blant annet som følge av digitaliseringen av samfunnet. Datanettverk binder de fleste sektorene sammen. Dette innebærer økte muligheter og behov for samvirke i både offentlig og privat sektor. Forsvaret er i økende grad avhengig av sivile leverandører. Sikkerhetsmessige hensyn må ivaretas når Forsvaret bruker disse.

Vi blir også mer internasjonale. Flere med utenlandsk bakgrunn kommer til Norge for å arbeide. Samtidig reiser nordmenn mer enn før, og har interesser i utlandet. Lojalitets- og tilknytningsforholdene hos ansatte blir mer komplekse. Det stiller nye krav i arbeidet med sikkerhetsklareringer, for å sikre at de som blir klarert er til å stole på. Internasjonaliseringen fører også til at konflikter i andre deler av verden kan få store konsekvenser nasjonalt, for eksempel gjennom radikalisering og fremmedkrigere, og økt terrortrussel.

TEKNOLOGISK UTVIKLING. Norge er i henhold til The Networked Readiness Index 2015[3] et av verdens mest digitaliserte land (nr 5 av 143). Antall tjenester som tilbys og antallet enheter som kobles til internett, mangedobles flere ganger hvert år. Vi må forvente at samfunnets evne til utnytte internett vil være en viktig del av den fremtidige verdiskapingen. Eksempler på dette er stordata (lagring og analyse av store mengder informasjon), skytjenester (lagring av data på servere i serverparker) og «Internet of Things» (nettverk med fysiske objekter knyttet sammen over internett). Robustheten og kapasiteten i telenettene øker, blant annet på grunn av det voksende behovet for strømmetjenester til private konsumenter, gjennom tjenester som Netflix eller YouTube.

Vi må anta at internett i løpet av de neste 10 årene vil bære stort sett all datakommunikasjon som understøtter kritisk infrastruktur. Også Forsvaret får økt avhengighet av internett som bærer av informasjon og infrastruktur. Datakraft og lagringsplass i fremtiden vil være en vare som tilbys til meget lav pris på virtuelle plattformer på tvers av landegrenser. Datamengder vil øke dramatisk, ikke bare på grunn av at man samler inn mer data, men også fordi stordata-teknologi i seg selv mangedobler og dupliserer data i stort monn.

Parallelt med samfunnets økte avhengighet av internett ser vi hvordan omfanget og kompleksiteten påvirker mulighetene for dataangrep.

Når stadig flere IKT-systemer kobles til hverandre og til internett, øker antall ledd og dermed sannsynligheten for et svakt ledd. I tillegg øker skadepotensialet dersom en sårbarhet blir utnyttet. Store konstruksjoner av flere ulike nett kan være vanskelige å ha full oversikt over, og er dermed vanskelige å sikre.

Spesielt er det utfordrende å sikre digitale styringssystemer (SCADA-systemer) som gjør det mu-

[3] http://www3.weforum.org/docs/WEF_Global_IT_Report_2015.pdf

lig å fjernstyre industriprosesser og andre viktige funksjoner. Når slike systemer direkte eller indirekte kobles til internett, gir det trusselaktører nye veier inn.

ØKONOMISK UTVIKLING. Ressurstilfanget til statlige organer som skal ivareta samfunnets sikkerhet vil bli påvirket av statens samlede betalingsevne. I følge Finansdepartementets perspektivmelding må vi ta høyde for hardere økonomiske prioriteringer i årene som kommer, blant annet som følge av en økende andel eldre og en gradvis utfasing av petroleumsvirksomheten.

Samtidig vil trangere tider i næringslivet gjøre det vanskeligere for private virksomheter å prioritere utgiftsposter som ikke gir dokumenterbar økonomisk effekt. Tiltak for å bedre sikkerheten må være kostnadseffektive.

2. Risikobildet

I dette kapitlet beskrives det aktuelle risikobildet innen IKT-sikkerhet, personellsikkerhet og fysisk sikkerhet. Under hvert delkapittel presenteres det som kan være angrepsmål for trusselen, relevante trusselaktører, aktørenes metoder, sårbarheter som kan utnyttes og mulige konsekvenser om risikoen utløses.

IKT-RISIKO. Med IKT-risiko menes faren for at tilsiktede hendelser skal kunne oppstå i, rette seg mot, eller benytte seg av IKT-systemer for å oppnå en for oss uønsket målsetting.

ANGREPSMÅL. Datanettverksoperasjoner er avdekket mot norsk forsvars-, sikkerhets- og beredskapssektor, politiske prosesser, norsk kritisk infrastruktur og enkeltvirksomheter eksempelvis innen petroleum, kraft, romfart, shipping og tele.

Alvorlige trusler retter seg mot flere sentrale samfunnsområder. Dette gjelder statssikkerhetsområdet representert ved departementene, utenrikstjenesten, Forsvaret, EOS-tjenestene og politiet. Det gjelder også samfunnssikkerhetsområdet representert ved viktige infrastruktur- og produksjonsområder som telekommunikasjon, kraftforsyning og petroleum. Trusler retter seg også mot nyhetsmedier og interesseorganisasjoner, næringslivet i sin alminnelighet og enkeltpersoner.

Målsettingen kan være å skaffe seg informasjon som stats- og forretningshemmeligheter, informasjon om forskningsresultater og teknologiske nyvinninger, og informasjon om strategier og planer. Det kan også være å skade en motpart ved å påvirke, redusere eller ødelegge funksjonalitet i produksjonssystemer, eller for eksempel stjele privat informasjon fra enkeltpersoner.

I 2014 varslet og håndterte NSM totalt 88 alvorlige dataangrep, mot 51 i 2013. Flesteparten av angrepene hadde som formål å stjele informasjon fra datasystemene til store eller viktige norske virksomheter. 4 prosent av norske virksomheter, og 5 prosent av de store, sier de har opplevd datainnbrudd. Realiteten er over 50 prosent, viser Mørketallsundersøkelsen 2014[4].

TRUSSELAKTØRER. Nettverksoperasjoner blir stadig mer målrettede og teknisk avanserte. Det er statlige aktører som står bak den mest alvorlige trusselen. Russland og Kina er iht. Etterretningstjenesten de mest aktive aktørene bak nettverksbaserte etterretningsoperasjoner rettet mot Norge.[5]

Listen over aktører som kan tenkes å ha målsettinger som nevnt ovenfor er lang og spenner fra overbeviste aktivister og terrorister til organiserte kriminelle, konkurrenter og stater.

Aktivister går under navnet «hacktivister» når de overfører sine kampanjer til internett. Deres aktivitet er oftest av forstyrrende karakter. De er mest interessert i kortsiktig synlighet og anerkjennelse. Tjenestenektangrep (DDoS) mot politiske motstandere, endring av nettsider og lekkasjer av sensitiv informasjon er eksempler på angrepstyper. En særskilt kategori ekstreme aktivister er terrorister. Disse må antas å ha høyere villighet til å begå alvorlig skadeverk og ødeleggelse, men til nå har de vist liten evne eller vilje til å utføre egentlige terrorhandlinger på internett. Terrorister bruker imidlertid nettet til propaganda og planleggingsformål, herunder å innhente informasjon om mulige terrormål.

Organiserte kriminelle står ofte bak kriminalitet som kredittkortsvindel. Salg av stjålet informasjon

[4] Mørketallsundersøkelsen 2014 – Informasjonssikkerhet, personvern og datakriminalitet, http://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/M%C3%B8rketallsunders%C3%B8kelsen/M%C3%B8rketall_2014.pdf

[5] Etterretningstjenestens rapport «FOKUS 2015»: https://forsvaret.no/ForsvaretDocuments/FOKUS2015-endelig.pdf

og hackerverktøy er også viktig i det kriminelle markedet. De siste 12 måneder har NSM sett at fokus har vært på banktrojanere og skadelig programvare som brukes i utpressingsforsøk (såkalt løsepengevirus) og til ID-tyveri.

Aktører innenfor internasjonal industri og næringsliv, med dedikerte offensive ressurser, bruker avanserte teknikker for å skaffe seg fordeler i forbindelse med anbud og forhandlinger om store statlige kontrakter.

Stater anvender sine respektive etterretnings- og sikkerhetstjenester for å ramme andre land med cybertrusler, og tjenestene kan ha lang tradisjon for å utføre spionasje og andre typer av skjulte operasjoner for påvirkning og sabotasje. Aktiviteten vil være knyttet til landenes interesser, både sikkerhetsmessige, økonomiske og andre interesser. I flere land understøtter slike tjenester landenes industri og næringsliv. Statlige aktører har særlig sterk evne til å utføre aktivitet med høy grad av kompleksitet og med et langsiktig perspektiv. Deres aktivitet er meget vanskelig å beskytte seg mot, og effektive mottiltak vil kreve en koordinert nasjonal innsats. Statlige aktører er en gruppe med særlig sterk evne til å utføre trusselaktivitet på internett. I sin årlige trusselvurdering for 2015 trekker Politiets sikkerhetstjeneste (PST) frem Russland og Kina som aktører med stor kapasitet.

TRUSSELMETODER. Innhenting av informasjon (spionasje) skjer i dag i stor grad ved hjelp av nettverksoperasjoner. De mest kraftfulle vedvarende trusler vi ser på nettet (Advanced Persistent Threats – APT) dreier seg hovedsakelig om spionasje. Det antas at betydelige mengder informasjon stjeles på denne måten. Flere omfattende spionasjeoperasjoner er blitt kjent gjennom åpne kilder. I april skrev tyske medier at datasystemene i Bundestag i Tyskland var blitt hacket, og data fra 20 000 kontoer stjålet.

Det registreres løpende et stort antall hendelser som er rent skadeverk. Dette omfatter tjenestenektangrep (DDoS) og endring av websider. De fleste av disse har liten varig effekt, men kan være virkningsfulle inn i en sikkerhetspolitisk eller innenrikspolitisk krevende situasjon. Eksempler på dette har vært i forbindelse med krisene i Georgia og Ukraina.

Hendelser av sabotasjekarakter forekommer også, men her er grensen mellom dette og plagsomt skadeverk flytende. Estland opplevde i 2007 alvorlige dataangrep som førte til store problemer. En av konsekvensene var at nettbanktjenester var utilgjengelige i flere dager. I 2013 rammet et cyberangrep både tv-stasjoner og banker i Sør-Korea. I juni 2015 måtte det polske flyselskapet LOT innstille ti og utsette 12 flyvninger som følge av dataangrep. I april 2015 opplevde det franske TV-selskapet TV5 Monde et større cyberangrep, hvor hackere tok 11 tv-kanaler av lufta, samtidig som de forandret selskapets nettsider og sosiale medier. Hackerne hevdet i dette tilfellet at de var tilknyttet IS.

Den mest ødeleggende nettverksoperasjonen kjent hittil er Stuxnet, sannsynligvis rettet mot digitale styringssystemer (SCADA-systemer) anvendt i iransk kjernekraftindustri. Operasjonen skal også ha blitt forsøkt mot det nordkoreanske atomvåpenprogrammet, men uten å lykkes. Den illustrerer potensialet i de metoder som i dag ligger i verktøykassen til andre staters tjenester. Det må antas at statlige aktører er tilbakeholdne med å eksponere sine mest avanserte kapasiteter på området.

SÅRBARHETER. Sårbarhetene som gjør oss utsatt for angrep er enten menneskelige, organisatoriske eller tekniske.

Blant de menneskelige sårbarheter er vår evne til å la oss lure. Denne sårbarheten utnyttes aktivt gjennom sosial manipulasjon. På denne måten lures ansatte til å gi fra seg passord, beskrive vedlikeholds- og sikkerhetsrutiner eller benytte minnepinner som er infisert. Erfaringsmessig er det alltid noen som lar seg lure av slike angrep. En annen menneskelig sårbarhet er lav motivasjon for å følge sikkerhetsbestemmelser, eksempelvis fordi dette vil gå ut over effektiviteten. Manglende kunnskap og evner er også en betydelig menneskelig svakhet.

Organisatoriske sårbarheter dreier seg blant annet om manglende lederforankring og styring av arbeidet med sikkerhet. Mangel på tydelig ansvarsdeling og bevisstgjøring er ytterligere kompliserende for sikkerhetsarbeidet. Generelt er det betydelige sårbarheter knyttet til at IKT driftsmiljøer kan være små, og kan ha mangler i forhold til ressurser og kompetanse. Det varierer stort fra virksomhet til virksomhet hvor stor fokus det er på sikkerhet i IKT-systemer.

På den tekniske siden finnes også en rekke sår-

barheter. Ikke oppdaterte dataprogrammer er som regel inngangen som brukes til å bryte seg inn i datasystemene til en virksomhet. Sikkerheten ved bruk av komponenter i IKT-systemer er sterkt varierende. IKT-produkter kan inneholde implementasjons- og designfeil. De kan konfigureres, installeres og brukes på måter som utgjør en sikkerhetsrisiko. Mulige sårbarheter kan finnes i maskinvare, operativsystem og applikasjoner. Vi ser også at manglende logging av trafikk kan innebære en betydelig sårbarhet, samt manglende tiltak for å oppdage irregulær bruk og aktivitet.

Svak informasjonssikkerhet er i følge Enisa Threat Landscape 2014 den viktigste årsaken til datainnbrudd. Det gjelder blant annet svake passord, sårbare nettverk og applikasjoner, virus, feil brukerautentisering, innsidetrussel og databasefeil. I følge samme rapport blir dataangrepene også stadig mer avanserte og målrettede. Trusselaktørene utnytter sikkerhetssvakheter effektivt når de blir kjent. Flere av funnene i rapporten samsvarer godt med NSMs egne funn. NSM erfarer at trusselaktørene gjør gode vurderinger av hva som er informasjon av høy verdi. Trusselaktørene arbeider stadig mer målrettet, og stadig mer profesjonelt.

Den norske delen av internett er preget av få store, og et stort antall mindre infrastruktureiere. Infrastrukturen er kompleks og den endrer seg hurtig. De enkelte virksomheter har begrenset evne til å vurdere risiko utover den risikoen virksomheten selv direkte står over for, for eksempel risiko knyttet til funksjonen virksomheten har i et større samfunnsperspektiv. Virksomhetene selv, og myndighetene, har begrenset kapasitet til å oppdage ondsinnede handlinger, og det er for stor forsinkelse fra man eventuelt oppdager hendelser til effektiv skadereduserende respons blir gjennomført.

KONSEKVENSER. Konsekvensen av vellykkede dataangrep kan være store. En rapport fra 2014, skrevet av Center for Strategic and International Studies (CSIS) i samarbeid med sikkerhetsselskapet McAfee, har estimert kostnaden av datakriminalitet for en rekke land. Den globale økonomien taper mer enn 400 milliarder dollar årlig på grunn av datakriminalitet[6]. De norske tapene er anslått til 0,64 % av BNP, det vil si 19 milliarder kroner for den norske økonomien[7]. Det er grunn til å ta forbehold om tapenes størrelse, men de antas å være betydelige.

NSM har sett flere eksempler på vellykkede datainnbrudd der angriperne har fått tilgang til virksomhetskritisk informasjon, og at forretningshemmeligheter, kursdrivende eller annen sensitiv informasjon har kommet på avveier. Skadevirkningene kan variere fra sak til sak, men de alvorligste konsekvensene skjer i et langsiktig perspektiv hvor virksomhetene etter tap av immaterielle verdier mister sin konkurranseevne og eksistensgrunnlag.

For offentlige virksomheter kan skadevirkningene være tap av tillit til det offentliges digitale løsninger på en slik måte at det påvirker samfunnets evne til å ta ut ytterligere gevinster ved modernisering og digitalisering.

Konsekvensene av vellykkede datainnbrudd kan også medføre tap av personopplysninger og annen sensitiv informasjon. Risikoen for mulig tap av virksomhetens omdømme er også tilstede. Nedetid på nettsider eller IKT-tjenester er også en alvorlig konsekvens for mange virksomheter, slik for eksempel flere norske banker opplevde i 2014. Nedetid i kritiske samfunnsfunksjoner som f.eks. helsevesen, energi- og vannforsyning kan ha alvorlige konsekvenser og medføre fare for innbyggernes liv og helse.

Tap av sikkerhetsgradert eller annen taushetsbelagt informasjon av operativ karakter tilhørende f.eks. politiet og Forsvaret kan både direkte og indirekte medføre tap av menneskeliv. Konsekvensen ved økt digital spionasje av militær karakter må også sees i et langsiktig perspektiv. Skadevirkningene blir ikke nødvendigvis synlige før en militær konflikt igangsettes.

DEN PERSONELLSIKKERHETSMESSIGE RISIKO.

Med personellsikkerhetsmessig risiko menes faren for at tilsiktede uønskede handlinger skal kunne utføres som følge av plassering eller utnyttelse av personell med adgang til en virksomhet, systemer, informasjon eller prosesser. Et annet navn på personellsikkerhetsmessige risiko er innsiderisiko.

ANGREPSMÅL. Innsidere vil kunne ha et bredt spekter av angrepsmål, gjennom mulighetene til å komme i særlig posisjon til å påvirke beslutninger, innhente sensitiv informasjon, gi feilaktig informasjon eller forårsake skade og ødeleggelse

[6] Net Losses: Estimating the Global Cost of Cybercrime. Economic impact of cybercrime II. Juni 2014

[7] NSR - Mørketallsundersøkelsen 2014

som kan tjene den opprinnelige oppdragsgivers målsettinger.

TRUSSELAKTØREN. Aktører som står bak forsøk på å utnytte mulighetene for innsidere kan være mange, herunder andre staters etterretnings- og sikkerhetstjenester, organiserte kriminelle miljøer mv. Innsidetrusselen er høyst reell, også i Norge. Utenlandsk etterretning har forsøkt å rekruttere PST-ansatte, og flere personer har forsøkt å få seg jobb i den norske sikkerhetstjenesten, skriver PST i sin trusselvurdering for 2015.

TRUSSELMETODE. Innsidere kan deles inn i tre kategorier:

- Infiltratøren, som i utgangspunktet arbeider for en trusselaktør og som blir forsøkt innplassert i et ansettelses- eller tilknytningsforhold for å utøve eller bistå i utøvelsen av tilsiktede uønskede hendelser
- Den vervede, som i utgangspunktet står i et ansettelses- eller tilknytningsforhold, men som av forskjellige grunner frivillig eller etter manipulering, påvirkning eller press lar seg overtale til å utøve eller bistå i utøvelsen av tilsiktede uønskede hendelser, eller som av egen fri vilje endrer lojalitet og utøver eller bistår i utøvelsen av slike hendelser
- Den utnyttede, som har manglende kunnskap, manglende sikkerhetsbevissthet eller generelt manglende dømmekraft, og som av den grunn indirekte bidrar til at en trusselaktør kan utøve tilsiktede uønskede hendelser

SÅRBARHETER. Sårbarheter i forhold til infiltratører kan være at virksomheter i liten grad kontrollerer identiteten til den de ansetter eller benytter seg av. Svak kvalitet på arbeidet med å etablere sikker identitet kan representere en vesentlig nasjonal sårbarhet.

Eksempler på personlige sårbarheter i forhold til verving kan være misnøye med arbeidsforhold, økonomiske eller personlige problemer. I de fleste innsidesakene i USA som er blitt kjent og har latt seg undersøke har det vært tegn på unormal aktivitet fra vedkommendes side i forkant[8]. Misnøye knyttet til arbeidsforholdet viser seg å være en sterk driver for egenmotiverte innsidere.

Sårbarheter i forhold til det å la seg utnytte kan være at man i virksomhetene fokuserer på formelle beslutninger, og i mindre grad følger opp den enkeltes sikkerhetsmessige skikkethet gjennom daglig sikkerhetsmessig ledelse.

KONSEKVENSER. Innsidere kan gjennom sin posisjon i det stille undergrave eksternt rettede sikkerhetstiltak og kan dermed forårsake store skader som for eksempel økonomiske tap, tap av renomme, skadeverk, samt tap av kritisk og gradert informasjon. Særlig store konsekvenser vil kunne oppstå om man lykkes med å innplassere infiltratører eller verve personell som alt er på plass i virksomheten.

RISIKO FOR FYSISKE ANSLAG.

Med risiko for fysiske anslag menes faren for at en trusselaktør vil kunne bryte fysiske barrieretiltak eller manipulere tilknyttede administrative rutiner, eksempelvis adgangskontroll, for å kunne gjennomføre tilsiktede uønskede hendelser.

ANGREPSMÅL. For å beskytte samfunnsviktige interesser mot sabotasje, spionasje og terrorhandlinger må en rekke områder, bygninger, anlegg, transportmidler eller annet materiell beskyttes med robusthetsskapende barrieretiltak som kan motstå fysiske anslag. Det gjelder også informasjonsinfrastruktur. Etteretningstjenesten fremholder i sin vurdering Fokus 2015 at en tendens for terrorangrep mot mål i Europa er at det rettes mot symboltunge mål. Dette representerer en utfordring da slike mål ikke nødvendigvis kan sikres med forebyggende fysiske tiltak.

Terrorhendelsen i Oslo og 22. juli 2011 og senere tids hendelser i Paris, København og Brussel viser at risikoen for fysiske anslag er reell. Forsvaret har i lengre tid hatt en forhøyet beredskap i Norge, og sommeren 2014 ble politiet midlertidig bevæpnet som en konsekvens av vurderingen om økt trussel.

TRUSSELAKTØRER. Aktørene som truer norsk sikkerhet kan spenne fra statsstøttede spesialister innen spionasje og sabotasje med mye trening og gode verktøy, til terrorgrupper med betydelige ressurser og noe kamperfaring, og enkeltpersoner med begrenset kapasitet. Etteretningstjenesten og PST trekker i sine vurderinger særlig frem islamistiske terrorgrupperinger som en trussel mot norske inter-

[8] Informasjon fra US Personnel and Security Research Centre (PERSEREC)

esser. I tillegg vises det til at fremmede stater samler informasjon om norske interesser, som senere kan brukes i sabotasjeøyemed i krisesituasjoner.

TRUSSELMETODER. Fysiske anslag kan ta en rekke ulike former. Typiske angrepsmetoder har vist seg å være bruk av eksplosiver, våpen, inntrengning med kjøretøy og gisseltaking for å tvinge seg adgang. Angrep kan også skje med kjemiske, biologiske eller radiologiske midler. Selv bare å fremsette trusler om slike angrep kan føre til betydelige forstyrrelser og kostnader i et samfunn.

En kombinasjon av cyberangrep, fysisk inntrengning og bruk av innsidere kan være formålstjenlig for en trusselaktør. Slike kombinerte operasjoner er spesielt relevant i mellomstatlige konflikter. For enkelte aktører vil det være mest hensiktsmessig å bruke enklere virkemidler for å kommunisere sine budskap. Etteretningstjenesten fremholder i sin vurdering Fokus 2015 at angrep mot mål i Europa har blitt mindre komplekse, og at tendensen er bruk av enkle våpentyper som håndvåpen og kniv.

Fysiske terroranslag utført av enkeltpersoner eller små grupper kan skje med minimale forberedelser og er vanskelig å få forvarsel om. Generelle beredskapsplanverk vil ha liten eller ingen effekt i tilfeller uten forvarsel. En god grunnsikring kan imidlertid vanskeliggjøre gjennomføringen og begrense skadene av enkelte angrep.

SÅRBARHET. Vårt åpne samfunn inneholder sårbarheter mot fysiske anslag. Eksempelvis vil hensynet til fri ferdsel og effektivitet i den daglige virksomheten kunne gi trusselaktører muligheter til å kunne utøve tilsiktede uønskede handlinger. Diskusjonen om sikringen av regjeringskvartalet før og etter 2011 og i fremtiden viser dilemmaene her.

Erfaring fra NSMs tilsyn, råd og veiledning viser at praksis for fysiske sikringstiltak er fragmentert og lite koordinert. Dette medfører at kostnadskrevende og potensielt ineffektive tiltak kan bli implementert.

Et eksempel på sårbarheter innen fysisk sikkerhet er den enkle adgangen til Jernbaneverkets relestasjon som Aftenposten avdekket ved flere besøk høsten 2014. På en svært enkel måte viste det seg mulig å få adgang til rommet hvor relestasjonen som styrer togtrafikken er. Et målrettet angrep ville lammet togtrafikken i Oslo i lang tid. Sårbarheten er senere utbedret.

Om ikke fysiske sikringstiltak er hensyntatt under konstruksjon, så er disse tiltakene ofte krevende å realisere og kostbare hvis de monteres/etableres i etterkant av byggingen. Disse tiltakene kan bli nedprioritert av den grunn.

KONSEKVENSER. Terror og sabotasje kan få alvorlige konsekvenser for samfunnet om det rammer kritisk infrastruktur, samfunnskritiske funksjoner eller rikets sikkerhet. I tillegg kommer muligheten for tap av liv, spesielt ved terrorhandlinger.

3. Sikkerhetsarbeidet i samfunnet

Den enkelte virksomhet har primæransvaret for egen sikkerhet mot tilsiktede uønskede handlinger. Det overordnede ansvaret for sikkerhet i en sektor påhviler det enkelte fagdepartement, som gjerne støttes i dette arbeidet av fagorganer innenfor sektoren. På nasjonalt plan er det overordnede ansvar fordelt mellom Forsvarsdepartementet innen militær sektor og Justis- og beredskapsdepartementet (JD) som samordner de sivile sektorene. NSM er etablert til støtte for FD og JD, og forestår en rekke utøvende oppgaver rettet mot etater og virksomheter i samtlige samfunnssektorer.

Sikkerhetsarbeidet mot tilsiktede uønskede handlinger vil være styrt av de fire hovedprinsippene om ansvar, nærhet, likhet og samvirke. I tillegg kommer eventuell lovregulering virksomheten er underlagt. Sikkerhetsarbeidet som utøves for å ivareta viktige samfunnsmessige interesser har lang tradisjon for å være detaljregulert i lover, forskrifter og instrukser. På statssikkerhetsområdet er reguleringen av sikkerhetsarbeidet gjennomgående sektorovergripende, mens den på samfunnssikkerhetsområdet i større grad er sektorspesifikk.

Sentralt i sikkerhetsarbeidet står sikkerhetsloven. Denne loven ble iverksatt i 2001 som en tverrsektoriell lov om sikkerhet mot spionasje, sabotasje og terrorhandlinger. Loven samlet, moderniserte og kodifiserte en rekke eldre bestemmelser som var spredt i forskrifter, instrukser og direktiver, men som samlet sett representerte en helhetlig beskyt-

telse av informasjon som kunne skade rikets sikkerhet mv. om den kom til uvedkommendes kunnskap (skjermingsverdig informasjon), uansett i hvilken form denne informasjonen forelå. I tillegg ga man i loven nye overordnede tverrsektorielle bestemmelser for beskyttelse av materiell, infrastruktur og annen eiendom som kunne skade rikets sikkerhet mv. dersom den ble ødelagt eller kom ut av rettmessig kontroll (skjermingsverdige objekter).

Frem til 2003 var det Forsvarets overkommando/Sikkerhetsstaben (FO/S) som fulgte opp det tverrsektorielle sikkerhetsarbeidet i samfunnet på vegne av FD. Dette året ble oppgaven overtatt av det nyopprettede direktoratet Nasjonal sikkerhetsmyndighet, administrativt underlagt Forsvarsdepartementet. Direktoratet ble gitt en faglig rapporterings- og ansvarslinje til Justis og beredskapsdepartementet for oppgaveløsningen rettet mot de sivile sektorer. Dette tydeliggjorde Justis og beredskapsdepartementets samordningsansvar for sikkerhetsarbeidet i de sivile sektorer.

Siden 2003 har det tverrsektorielle sikkerhetsarbeidet i samfunnet vært i stadig utvikling. I det følgende pekes det på enkelte vesentlige utviklingstrekk i de senere år.

OBJEKTSIKKERHET. Et relativt nytt område for sektorovergripende tiltak innenfor forebyggende sikkerhet er objektsikkerhet. På dette området er sektormyndighetene og sektorregelverket trukket inn på en helt annen måte enn på informasjonssikkerhetsområdet. NSMs rolle er overordnet, men forutsetter nær dialog og samhandling med sektorene. I tillegg forutsettes koordinering mellom NSM, Forsvaret og politiet i forbindelse med planlegging av sikringsstyrker til beskyttelse av objekter.

HÅNDTERING AV CYBERANGREP. I 1999 etablerte EOS-tjenestene Varslingssystem for digital infrastruktur (VDI). Hensikten var å gi myndighetene tidlig varsel om koordinerte og alvorlige dataangrep. VDI ble i 2003 lagt til NSM. I 2006 ble VDI utvidet til også å omfatte en nasjonal responsfunksjon ved slike angrep, NorCERT (Norwegian Computer Emergency Response Team). NSM NorCERT er nasjonalt IKT-responsmiljø og skal koordinere håndteringen av alvorlige IKT-hendelser mot samfunnskritisk infrastruktur og informasjon. NorCERT-funksjonen ble etablert som en integrert del av Nasjonal sikkerhetsmyndighet fra 1. januar 2006 og er en oppfølging av St.meld. nr. 39 (2003-2004). I St. meld. nr. 22 (2007-2008) er det uttalt at «NorCERT er Norges nasjonale senter for å håndtere alvorlige dataangrep mot samfunnskritisk infrastruktur og informasjon.» Det legges i meldingen til grunn at «enheten legger til rette for effektiv håndtering av alvorlige IKT-sikkerhetsangrep mot viktig infrastruktur og informasjon i Norge.» Et helt sentralt element i utøvelsen av NorCERT-funksjonen er innhenting og videreformidling av informasjon om sårbarheter, potensielle risikoer, angrepsmetoder og ondsinnet kode. Dette oppnås dels gjennom innhenting av informasjon fra VDI-systemet, og dels gjennom informasjonsdelingen som skjer som en del av nasjonalt og internasjonalt samarbeid. NSM NorCERT samarbeider tett med Etterretningstjenesten og Politiets sikkerhetstjeneste, blant annet gjennom cyberkoordineringsgruppen (CKG). Samarbeidet ledes av NSM, og er regulert i egne retningslinjer. Formålet med gruppen er at EOS-tjenestene mest mulig effektivt skal kunne forebygge og håndtere alvorlige cyberangrep , samt gi overordnede beslutningstakere og utsatte virksomheter et best mulig virkemiddel for å iverksette tiltak. NSM støtter i tillegg politiet ved cyberkriminalitet som ikke omfattes av PSTs ansvar. Blant andre særlige nære samarbeidspartnere for NSM i rollen som nasjonal håndteringsinstans er Nasjonal kommunikasjonsmyndighet (Nkom). Nkom har et oppfølgingsansvar for ekom-infrastrukturen, herunder internett i Norge.

Nasjonal strategi for informasjonssikkerhet har utkommet i tre versjoner siden 2003. Den siste versjonen kom i 2012. Strategien gir føringer for videreutvikling av det samlede informasjonssikkerhetsarbeidet i samfunnet. Et viktig grep i strategien er målsettingen om at de enkelte fagdepartementer skal etablere sektorvise responsmiljøer i egen sektor. Sektormiljøer er til nå etablert i Forsvaret (ved Cyberforsvaret/Avdeling for beskyttelse av kritisk infrastruktur - BKI), helsesektoren (HelseCSIRT), finanssektoren (FinansCERT), kraftsektoren (KraftCERT), og universitets- og høyskolesektoren (UNINETT CERT).

ROLLER OG ANSVAR. Et viktig grep i 2013 var at samordningsansvaret for IKT-sikkerhet på sivil side ble overført fra det daværende Fornyings-, administrasjons- og kirkedepartementet, nå Kom-

munal- og moderniseringsdepartementet, til Justis- og beredskapsdepartementet. På den måten ble alt samordningsansvar innen samfunnssikkerhet på sivil side samlet i Justis og beredskapsdepartementet. Tilsvarende ansvar på militær side tilligger Forsvarsdepartementet. Ansvaret for koordinering av regjeringens helhetlige IKT-politikk, samt særskilt ansvar for å arbeide for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen, ble imidlertid beholdt i Fornyings-, administrasjons og kirkedepartementet, nå Kommunal- og moderniseringsdepartementet. Sentralt utviklingsmiljø for Kommunal- og moderniseringsdepartementet er Direktoratet for forvaltning og IKT (Difi) og sentralt driftsmiljø for departementsfellesskapet er Departementenes sikkerhets- og servicesenter (DSS).

Ved inngangen til inneværende langtidsperiode ble NSMs rolle som ekspertorgan for informasjons- og objektsikkerhet, samt det sentrale fagmiljøet for IKT-sikkerhet, stadfestet av Regjeringen. I desember 2014 ble det for første gang gitt en samlet instruks for Sjef NSMs ansvar og oppgaver, hvor også denne rollen ble bekreftet. Instruksen ble gitt av Forsvarsdepartementet i samråd med Justis og beredskapsdepartementet.[9]

NASJONALE BEREDSKAPSSYSTEMER. Våren 2015 er det gjort enkelte endringer i Nasjonalt beredskapssystem (NBS). NBS består av Sivilt beredskapssystem (SBS) og Beredskapssystem for forsvarssektoren (BFF). SBS og BFF er vedtatt med hjemmel i beredskapsloven § 18 og Kongens instruksjonsmyndighet. Endringene er av betydning for hvordan IKT-sikkerhetsarbeidet og NSMs oppgaver skal utføres. En viktig endring er at Sjef NSM, med utgangspunkt i ansvaret for VDI og den nasjonale responsfunksjonen NSM NorCERT, har fått i oppdrag å iverksette eller gi nasjonale anbefalinger om å iverksette tiltak og koordinere håndteringen.

Det nasjonale arbeidet med forebyggende sikkerhet har grenseflater opp mot det alminnelige samfunnssikkerhetsarbeidet, hvor Direktoratet for samfunnssikkerhet og beredskap (DSB) er sentral. Forholdet mellom NSM og DSB har vært vurdert og klargjort. De to direktoratene samarbeider om viktige sider ved oppgaveløsningen, herunder tilsyn.

FELLES EUROPEISKE STANDARDER. Internasjonal utvikling påvirker også hvordan vi besvarer behovene nasjonalt. IKT-sikkerhet er høyt på agendaen internasjonalt, herunder i NATO og EU. Utviklingen og implementeringen av EUs program Digital Agenda for Europa vil ha stor betydning også for Norge gjennom vår EØS-tilknytning. IKT-sikkerhet er viet en egen pilar i Digital Agenda, pilar III «Trust & Security». Som en del av oppfølgingen av pilar III er det utarbeidet et forslag til direktiv for forsterket nettverks- og informasjonssikkerhet (NIS-direktivet)[10]. Direktivet vil omfatte offentlig forvaltning, tilbydere av informasjonstjenester for samfunnet, samt eiere og driftere av samfunnskritisk IKT-infrastruktur. Hensikten er å etablere felleseuropeiske sektorovergripende minimumsstandarder for IKT-sikkerhet.

4. NSMs støtte til Forsvarets operative evne

En betydelig del av NSMs ressurser er innrettet mot å støtte og øke Forsvarets operative evne. NSMs nåværende støtte til Forsvaret er mangefasettert, og favner et bredt spekter av ulike fag- og leveranseområder. Under belyses sentrale områder innen den nåværende støtten NSM bidrar med.

NSM bidrar til Forsvarets operative evne primært gjennom:

- Deteksjon og håndtering av hendelser av betydning for operative og strategiske systemer i Forsvaret
- Sikkerhetsgodkjenning av operative systemer
- Rådgivning mot, og deltagelse i Forsvarets prosjekter som skal understøtte operative leveranser
- Sikkerhetsklarering av personell som skal benyttes i operativ tjeneste
- Tekniske sikkerhetsundersøkelser av Forsvarets lokasjoner
- Emisjonssikring av Forsvarets tekniske utstyr som inngår i operative leveranser
- Tilsyn som bidrar til å avdekke og lukke avvik som kan påvirke operative leveranser

[9] Se Vedlegg A

[10] COM(2013)48 final, datert 7.2 2013

- Inntrengingstesting som bidrar til mer robuste tekniske løsninger for operativ bruk
- Virksomhetskontroll som bidrar til å sikre leverandørkjedene for Forsvarets tekniske materiell for understøttelse av operasjoner
- Veiledninger og krav for sikker bruk og implementering av operativt nødvendig teknologi
- Forskning og utvikling innen felter som bidrar til økt informasjonssikkerhet i operative systemer
- Sikker kommunikasjon i og utenfor operasjoner gjennom distribusjon og produksjon av kryptografiske nøkler. NSM ivaretar i Norge rollen som NDA (National Distribution Authority)

Flertallet av disse leveransene er avgjørende for Forsvarets operative evne i både fred, krise og krig. Bortfall av leveranser fra NSM som deteksjon og håndtering av hendelser av betydning for operative og strategiske systemer i Forsvaret, distribusjon og produksjon av kryptografiske nøkler, sikkerhetsklarering av personell, og tekniske sikkerhetsundersøkelser vil i alvorlig grad ramme Forsvarets operative evne.

5. NSMs evner og kapasiteter

Sjef NSM er gitt ansvar og oppgaver i sin instruks[11]. Innen rammen av denne instruksen er NSM gitt en rekke oppgaver gjennom øvrig regelverk og oppdrag. For at NSM skal kunne løse sitt samfunnsoppdrag som beskrevet i instruksen og i henhold til de krav som stilles gjennom de årlige iverksettingsbrev må direktoratet besitte en rekke evner og kapasiteter.

I SFR har NSM benyttet betegnelsen evne, mens man i forsvarssektoren forøvrig benytter begrepet kapabilitet. Disse er å betrakte som synonymer i dette dokumentet. Med evne i denne sammenhengen, mener vi en overordnet evne til å utføre eller å ivareta noe. I tillegg til å ha en evne er det nødvendig å vite hvilken kapasitet man besitter (mengden av en evne).

Evner må vedlikeholdes og utvikles i samsvar med, og helst i forkant av samfunnsutviklingen. En strukturert prosess for utvikling av evner og mengden av disse evnene er nødvendig for at NSM kan løse sitt samfunnsoppdrag.

NSMs arbeid går langs tre primære akser. Forebyggende arbeid som søker å unngå at sikkerhetstruende hendelser inntreffer, håndtering som ivaretar situasjoner der slike hendelser likevel inntreffer, og kontroll som følger opp at krav til sikkerhet ivaretas innen de to øvrige akser i henhold til regelverket og på en god måte. NSM har i det følgende utarbeidet en foreløpig og ikke uttømmende oversikt over organisasjonens evner gruppert innen disse tre aksene.

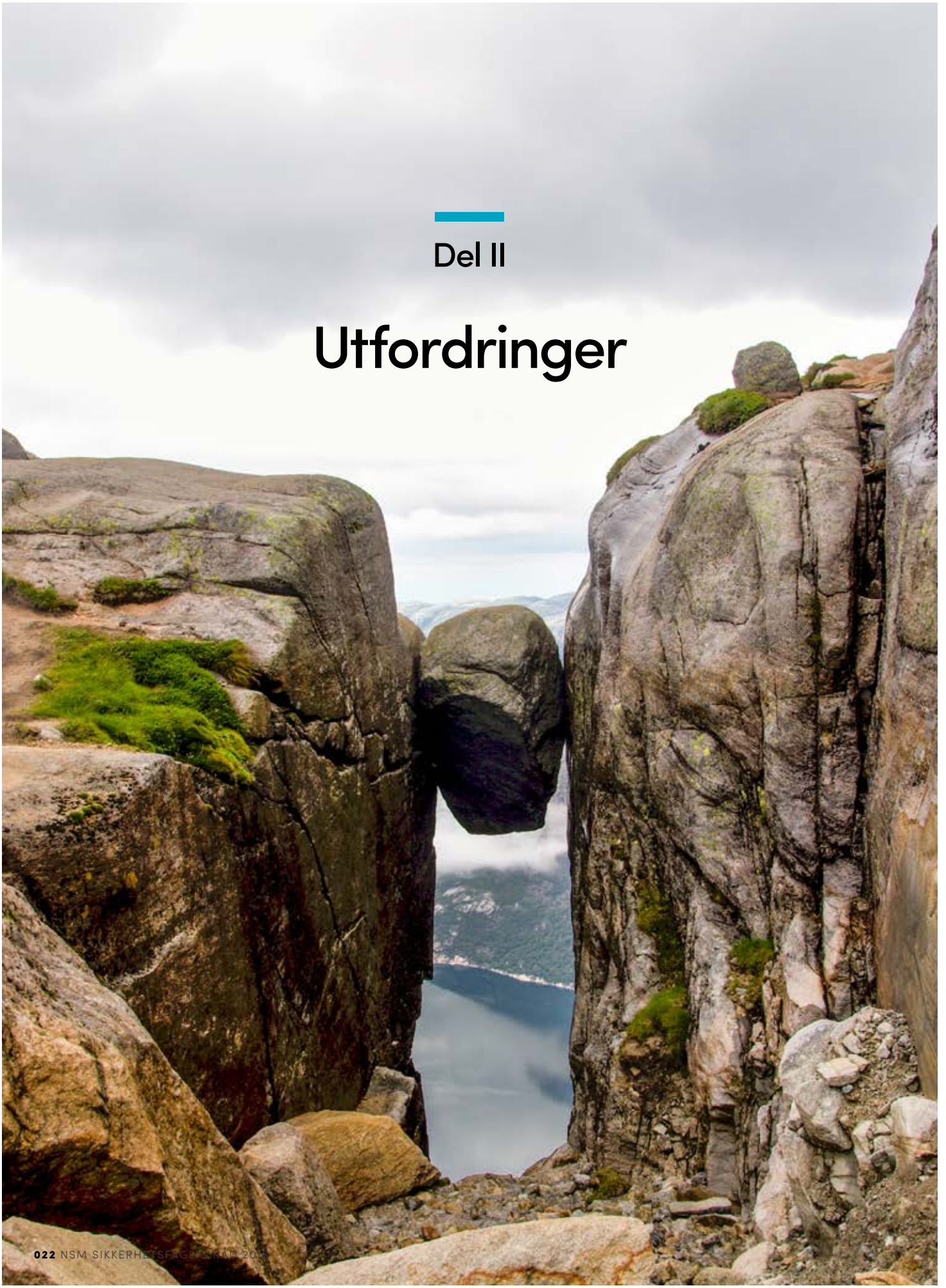
[11] Vedlegg A – Instruks for sjef NSM

FIGUR 3 OVERSIKT OVER NSMS EVNER

FOREBYGGE	HÅNDTERE	KONTROLLERE
Evne til å styrke sikkerheten gjennom å redusere sårbarhet	**Evne til å redusere konsekvensene av en hendelse**	**Evne til å kontrollere at sikkerheten ivaretas**
Evne til:	Evne til:	Evne til:
E-f1 Råd, veiledning om forebyggende sikkerhet	**E-h1** Opprettholdelse av sensornettverk	**E-k1** Tilsyn
E-f2 Person og virksomhetsklarering	**E-h2** Hendelseshåndtering og varsling	**E-k2** Godkjenning av sikkerhetsgraderte informasjonssystemer
E-f3 Kontroll med luftbårne sensorer	**E-h3** Støtte ved hendelsesrespons	**E-k3** Forskning og utvikling (FoU) - kontrollere
E-f4 Sertifisere informasjonssystemer	**E-h4** Teknisk analyse av skadevare	
E-f5 Kryptosikkerhet	**E-h6** Bidra med ressurser til tverrsektorielt nasjonalt samarbeid og nasjonal krisehåndtering	
E-f6 IKT-sikkerhet	**E-h7** Opprettholde og vedlikeholde handlefrihet og situasjonsforståelse i det digitale rom	
E-f7 Analyse, risikovurdering og tiltaksutvikling	**E-h8** Forskning og utvikling(FoU) - håndtere	
E-f8 Kompetansebygging		
E-f9 Tekniske undersøkelser		
E-f10 Forskning og utvikling (FOU) - forebygge		

Del II

Utfordringer



Nedenfor presenteres de viktigste utfordringene sett fra NSMs perspektiv med utgangspunkt i det situasjonsbildet som er beskrevet tidligere.

6. Organisering, ledelse og koordinering

JUSTIS- OG BEREDSKAPSDEPARTEMENTETS KOORDINERINGSROLLE. Mange ulike aktører, både departementer og etater, har koordinerende ansvar for et fagfelt. Dette kan være utfordrende innenfor rammene av konstitusjonelle ansvarsforhold, der den enkelte statsråd er ansvarlig innenfor sitt fagfelt. Justis- og beredskapsdepartementets koordinerende rolle innenfor forebyggende sikkerhet i sivil sektor er ikke i tilstrekkelig grad operasjonalisert slik at departementet kan ta sin rolle med den kraft som er nødvendig. En slik operasjonalisering er en forutsetning for dette. Rollen må anerkjennes av aktørene som skal bidra i koordineringen. I tillegg ser vi at det mangler, eller er for dårlig utviklede, samvirkemekanismer på plass mellom aktørene. Dette gir en utilstrekkelig koordinering på området. Opplevde uklarheter på høyere nivå vil forplante seg nedover.

MANGLENDE STYRING OG KONTROLL MED FOREBYGGENDE SIKKERHET. Tilsyn i regi av NSM har gjennomgående avdekket avvik og sårbarheter som virksomhetene selv burde ha oppdaget og korrigert gjennom interne sikkerhetsrevisjoner og evalueringer. Sårbarhetene i norske virksomheter er store, og forebyggende tiltak er ikke i nødvendig grad på plass i virksomhetene. Arbeidet med forebyggende sikkerhet mangler lederfokus. Dette gjelder for statlig virksomhet på ulike nivåer, og i private og offentlige virksomheter. Konsekvensen er at risikostyringen er utilstrekkelig.

EVNE TIL SAMVIRKE I BEREDSKAPS- OG KRISESITUASJONER. Ukraina-krisen viste at samvirkemekanismene i hele beredskapskjeden hadde mangler. Det handlet om alt fra hvordan varslinger ble gitt, til hvem som faktisk kunne motta informasjon. For NSMs del var dette særlig tydelig innenfor IKT-sikkerhet, herunder forberedende oppgaver i tilknytning til hendelseshåndtering. NSM erfarte at det var flere vi ikke kunne dele informasjon med, og det ble nødvendig å finne alternative måter å gjøre dette på. Utfordringene var på flere plan: Beredskapsplanverk var ikke oppdatert og tydeliggjort når det gjaldt tiltak innenfor IKT-sikkerhet, herunder hendelseshåndtering. De nasjonale planverk er imidlertid blitt revidert i ettertid, der NSMs roller er tydelig fastsatt. Det gjenstår å operasjonalisere disse. Det var og er ikke en enhetlig og sikker kommunikasjonsinfrastruktur som understøtter behovet for rask og effektiv informasjonsdeling og koordinerte beslutningsprosesser. Videre er det mange private aktører som har en rolle i beredskapskjeden. I en beredskaps- eller krisesituasjon, vil myndighetene ha behov for å dele sikkerhetsgradert informasjon med disse. Fordi mange av de private aktørene ikke er underlagt sikkerhetsloven, lar det seg ikke gjøre å dele den informasjonen som er nødvendig for krisehåndteringen. NSM har oversendt et forslag til Forsvarsdepartementet om en rekke private virksomheter som bør underlegges sikkerhetsloven i kraft av sin rolle i krise- og beredskapskjeden for å kunne få tilgang til nødvendig gradert informasjon. Forslaget er fremdeles til behandling.

Når det gjelder IKT-sikkerhet er det i for liten grad tverrsektorielle øvelser på jevnlig basis. I tillegg er det flere aktører som gjennomfører øvelser hvor IKT-sikkerhet er relevant. Det er behov for å systematisere øvelsesplanleggingen og tydeliggjøre hvem som har hovedansvaret innen dette feltet.

SAMLOKALISERING AV NSM. Styrkingen av NSM i 2013 og 2014 har gjort det nødvendig å etablere NSM på flere lokasjoner. For NSM som et relativt lite direktorat, er det krevende å være lokalisert på flere steder. Det er kostbart og lite effektivt. I tillegg er det krevende for egne ansatte og samarbeidspartnere, og svekker grunnlaget for å skape en felles

kultur. Det har i tidligere dialog med Forsvarsdepartementet, som en del av Perspektivplan EBA, vært diskutert ulike alternativer for en fremtidig samlokalisering av NSM. Et slikt prosjektforslag er foreløpig ikke prioritert inn i perspektivplanen, men det er avgjørende for NSM at prosessen starter opp igjen.

NSM NorCERT er det nasjonale koordineringspunktet for støtte til håndtering av IKT-sikkerhetshendelser. I sitt samvirke med ulike aktører, er det et tydelig uttrykt behov hos alle at det er nødvendig å legge fysisk til rette for samhandling og liaisonering både i det daglige og i forbindelse med hendelser.

7. Rammer og bestemmelser

FRAGMENTERTE REGELVERK. Virksomheter, både statlige og private, må ofte forholde seg til mange regelverk om informasjonssikkerhet. Regelverkene er fragmenterte, regulerer forskjellige områder og har forskjellig detaljeringsnivå. Terminologi og språkbruk mellom regelverkene avviker også. Regelverkene bygger på til dels forskjellige tradisjoner. Personopplysningsloven med forskrift bygger på ISO-standarder[12], sikkerhetsloven bygger på NATOs regelverk for gradert informasjon, mens IKT-forskriften som benyttes i finanssektoren har tatt utgangspunkt i internasjonale rammeverk[13]. Forskjellig tilnærming reduserer samhandling og øker kostnader.

Forskjellige tilnærminger til informasjonssikkerhet, krav på forskjellige nivåer, basert på forskjellige metoder og med forskjellige formål, skaper samhandlingsutfordringer.

Forskjellig tilnærming er kostnadsdrivende for den enkelte virksomhet som omfattes av flere regelverk. Virksomheten må bruke ressurser på å sette seg inn i og forstå de ulike regelverkene, og vurdere i hvilken grad deres ordninger og systemer tilfredsstiller alle regelverkene.

[12] ISO/IEC 17799, senere ISO/IEC 27001

[13] CobiT

8. IKT-sikkerhet

MANGLENDE TYDELIGGJØRING AV DEN NASJONALE MYNDIGHETEN FOR IKT-SIKKERHET. Innenfor sikkerhetslovens område er NSM den nasjonale myndigheten for IKT-sikkerhet. Roller og myndighet er her avklart.

Utenfor sikkerhetslovens område er det ikke like avklart. NSM er tillagt oppgaver og ansvar som nasjonalt fagmiljø for IKT-sikkerhet av JD som følge av departementets ansvar for IKT-sikkerhet etter Kgl. res. av 22. mars 2013. I sin instruks er Sjef NSM gitt omfattende oppgaver og ansvar innen IKT-sikkerhet, herunder å koordinere håndteringen av alvorlige IKT-angrep. I henhold til samme instruks er Sjef NSM gitt oppgaven med å være forsvarsministerens og justis- og beredskapsministerens nærmeste rådgiver i spørsmål om forebyggende tiltak mot sikkerhetstruende virksomhet som kan ramme nasjonale og samfunnsmessige verdier. Instruksen er gitt av Forsvarsdepartementet i kraft av instruksjonsmyndighet og i samråd med Justis- og beredskapsdepartementet. Den er derfor ikke formelt bindende for etater utenfor forsvarssektoren. Dette er en svakhet da gjennomføringen av instruksen fordrer utstrakt samhandling med sivile sektorer, og mellom sivil og militær sektor. Det er behov for tydeliggjøring av en nasjonal myndighet for IKT-sikkerhet utenfor sikkerhetslovens område.

IKKE OPPDATERT NASJONAL STRATEGI FOR INFORMASJONSSIKKERHET. Nasjonal strategi for informasjonssikkerhet ble vedtatt i 2012. Dette var det tredje strategidokumentet i rekken siden det første utkom i 2003. Etter 2012 har det skjedd endringer som tilsier at strategien og tilhørende handlingsplan må gjennomgås og revideres. I 2013 ble eksempelvis ansvaret for forebyggende IKT-sikkerhet overført fra nåværende Kommunal- og moderniseringsdepartementet til Justis- og beredskapsdepartementet. Nåværende strategi tydeliggjør i for liten grad roller og ansvar. Dette har svekket evnen til effektiv implementering og oppfølging av strategien. Som følge av endringer i

risikobildet vil det være naturlig å vurdere tiltakene i strategien på nytt.

MANGE BETEGNELSER OM IKT-SIKKERHET. Mange betegnelser er i bruk om IKT-sikkerhet. Både IT-sikkerhet, datasikkerhet, digital sikkerhet og cybersikkerhet blir brukt, til dels som synonymer, men med mindre nyanseforskjeller. Informasjonssikkerhet, som i utgangspunktet favner bredere enn IKT-sikkerhet (i og med at begrepet også omfatter områder som ikke er digitale, som papir, dokumenter og tale), blir av flere brukt om den digitale delen av sikkerhetsarbeidet. Regjeringens strategi for informasjonssikkerhet blir eksempelvis kalt «Cyber Security Strategy for Norway» i engelsk oversettelse. Betegnelser vil være i endring over tid, og vil også av natur være til dels ulike avhengig av utdannelse, bakgrunn, bransje og sektor. Mange av begrepene som er i bruk fungerer som synonymer, men kan likevel ha ulike nyanser som kan utfordre samhandling og koordinering dersom man ikke er bevisst på forskjellene. Samme diskusjoner går også internasjonalt.

MANGLENDE OVERSIKT OVER ALVORLIGE IKT-HENDELSER. I dag foreligger rapporteringsplikt til NSM om alvorlige IKT-hendelser kun innenfor sikkerhetslovens område. Det finnes rapporteringsordninger som går til andre myndighetsorganer, eksempelvis Finanstilsynet og Nkom. Disse rapporteres ikke nødvendigvis til NSM. Dette svekker NSMs evne til å kunne utarbeide og forvalte et best mulig IKT-risikobilde på nasjonalt nivå, og ha nasjonal evne til tverrsektoriell respons.

UTVIKLINGSBEHOV I DEN NASJONALE CERT-FUNKSJONEN (NSM NORCERT). Man må anta at i løpet av de neste ti årene vil stort sett all datakommunikasjon som understøtter kritisk infrastruktur i Norge bruke internett som bærer av datatrafikk. Denne utviklingen gjør det viktigere enn noen gang at norske myndigheter har en nasjonal kapasitet som evner å detektere angrep i norsk infrastruktur, varsle, koordinere og håndtere hendelsen raskt slik at skadeomfanget reduseres, og bidra til at normalsituasjon raskt kommer på plass igjen. Med den økte avhengigheten Forsvaret og annen kritisk IKT-infrastruktur får til internett som bærer av informasjon, vil NSM NorCERT ha behov for en betydelig kapasitetsøkning for å kunne bistå eiere av kritisk IKT-infrastruktur i årene fremover.

NSM har i løpet av 2015 gjennomført en større strategiprosess, som har resultert i økt fokus på sektorvise responsmiljøer og skaleringspotensiale. Den nye ordningen vil til en viss grad imøtekomme økningen i antall cyberangrep, men er på langt nær robust nok. Full effekt av ordningen forutsetter også at det legges til rette fysisk for at sektorvise responsmiljøer, eiere av kritisk IKT-infrastruktur, EOS-tjenestene og andre viktige aktører vil kunne være til stede i samme lokale for å sikre en effektiv hendelseshåndtering. Dette er ikke mulig innenfor dagens løsning.

I forbindelse med hendelseshåndtering er det i dag ingen felles plattform eller distribuert kommunikasjonstjeneste som gjør at kritisk informasjon kan deles i forkant av eller under en cyberhendelse. I dag håndteres dette primært gjennom e-post, en løsning som er svært lite tilpasset formålet. Det kan i verste fall medføre at kritisk informasjon ikke når frem til de rette aktørene under en hendelse.

Det er også behov for å styrke evnen til koordinering og samvirke, og øke felles kunnskap om strategiske utfordringer og sårbarheter. Det mangler nasjonale møtearenaer eller nettverk med deltakelse fra de sentrale myndighetene, næringslivet og eiere av kritisk IKT-infrastruktur.

SVAKHETER VED NASJONAL DETEKSJONSEVNE. Nasjonal sikkerhetsmyndighet drifter Varslingssystem for digital infrastruktur (VDI). Systemet består av sensorer som varsler om cyberangrep mot kritisk infrastruktur og viktige virksomheter i Norge. Sensorene gir et bilde av hvilke angrep som rammer samfunnsviktige norske virksomheter, og er således et sentralt element i den samlede nasjonale deteksjonsevne. Den nasjonale deteksjonsevnen er for svak som følge av for få VDI-sensorer og manglende dekningsomfang. Systemet er i dag basert på frivillig deltakelse, og finansiering av private aktører. Situasjonsbildet knyttet til sårbarheter i viktig norsk IKT-infrastruktur er avhengig av om aktuelle selskaper ønsker å være med i samarbei-

det eller ikke. Andre myndigheters deteksjonsevner omtales ikke.

FRAGMENTERTE IKT-LØSNINGER I DET OFFENTLIGE. Utvikling, forvaltning og drift av IKT-løsninger for det offentlige er i dag spredt på en rekke forskjellige aktører. Løsningene er bygd opp på ulike måter, og har ulik grad av sikkerhet. En rapport for forsvarssektoren, utarbeidet av konsulentselskapet McKinsey, beskriver at forsvarssektoren ikke er et unntak.

Når det gjelder løsninger for ugradert informasjon, er det i dag mange driftsorganisasjoner og betydelig fragmentering i staten. Ulike leverandører av ulike løsninger utfordrer effektivitet, samhandling og kommunikasjon på tvers av graderingsnivåer og sektorer. Misnøye med tidligere leveranser kan ha bidratt til at aktører har utviklet egne løsninger.

Når det gjelder løsninger for sikkerhetsgradert (høy og lavgradert) informasjon, leverer både Forsvaret, FD, DSS og NSM slike løsninger.

MANGLENDE FELLESLØSNINGER FOR HØYGRADERTE[14] IKT LØSNINGER. Flere aktører i Norge har behov for høygraderte IKT-løsninger. De ulike aktørene har også behov for at disse høygraderte løsningene tilbyr elektronisk samhandling med andre systemer. Utvikling av sikre høygraderte informasjonssystemer er ressurskrevende og krever spesiell kompetanse. Manglende felles utvikling kan utfordre samhandling mellom de ulike aktørene, så vel som å være kostnadsdrivende. Når det gjelder løsninger for høygradert informasjon, leverer både Forsvaret, FD, PST og NSM slike løsninger. Enkelte etater har også egne løsninger.

MANGLENDE FELLESLØSNINGER FOR UGRADERT SENSITIVT OG LAVGRADERT[15] NIVÅ. Det er et betydelig antall aktører i Norge som har behov for ugraderte og lavgraderte IKT-systemer. Erfaringer fra øvelser og konkrete hendelser viser at det mangler gjennomgående fellesløsninger på et lavgradert nivå. I dag er det ulike løsninger som anvendes for ulike sensitivitetsnivåer. Dette skaper utfordringer i det daglige i forbindelse med utveksling av informasjon og ved håndtering av hendelser. Flere løsninger må anvendes samtidig for å kunne formidle og motta informasjon, noe som kan forsinke og komplisere nødvendig samhandling. Når det gjelder løsninger for lavgradert informasjon, leverer både Forsvaret, FD, Departementenes sikkerhets og serviceorganisasjon (DSS) og NSM slike løsninger. Enkelte etater har også egne løsninger.

SÅRBARHET MOT IKT-ANGREP[16]. Det er mange måter å angripe IKT-systemer på. Vi skiller i denne sammenheng mellom sårbarheter som er menneskelige, organisatoriske eller tekniske.

Menneskelige sårbarheter er ofte en sentral faktor innen IKT-angrep. Særlig er individers mottagelighet for manipulasjon og villedning viktige faktorer i dette bildet. IKT-angrep skjer i stor grad ved å bruke virksomhetenes brukere og ansatte som mellomledd. Brukerne villedes ofte gjennom falske eposter med lenker eller vedlegg, eller infiserte nettsider. Dette kan åpne en eller flere veier inn i systemet. Angrepene er ofte vanskelige å oppdage. Videre kan brukere manipuleres til å gi fra seg sentral informasjon relatert til sikkerhetstiltak, rutiner og lokasjoner. Individer kan også manipuleres eller tilbys goder for å endre sin lojalitet, og dermed bevisst bidra til å åpne for IKT-angrep. En annen menneskelig driver for sårbarhet er manglende vilje til å følge, samt kunnskap om og ferdigheter til å følge, sikkerhetsrutiner. Mangelen på generell IKT-kompetanse kan også øke sårbarheten for IKT-angrep.

Organisatoriske sårbarheter gjør seg gjeldende gjennom uklar ansvarsdeling eller manglende eierskap til sikkerhetsarbeidet i en organisasjon. Manglende fokus og ressurser innen sikker drift av IKT-systemer kan også øke risiko for IKT-angrep betydelig. Videre vil manglende fokus i organisasjonen på sikkerhetskultur og opplæring medføre økt sårbarhet mot IKT-angrep.

En betydelig del av sårbarhetene i forbindelse med IKT-angrep er av teknisk art. Utdatert programvare og programvare med svake sikkerhetsmekanismer er typiske angrepsvektorer. Selv om et produkt i seg selv kan anvendes på en sikker måte, er det stor variasjon i implementeringen av de enkelte komponenter i IKT-systemer. Videre er manglende

[14] Høygraderte IKT-løsninger er løsninger for informasjon sikkerhetsgradert som KONFIDENSIELT eller høyere.

[15] Med lavgradert nivå menes informasjon sikkerhetsgradert som BEGRENSET.

[16] Det vises også til omtale av sårbarheter under redegjørelsen for IKT-risikobildet tidligere i dette dokumentet.

fokus på feil, svakheter og konstruksjonsavvik i maskinvare en kilde til en rekke ulike sårbarheter. Mangler IKT-systemet evne til å klassifisere og agere på unormal trafikk, er det også betydelig risiko for at data kan tappes eller ødelegges uten at dette registreres og stanses.

Det er i dag utstrakt sammenkobling av IKT-systemer, som medfører nye sikkerhetsutfordringer. Sårbarhet i ett system kan øke sårbarheten i et annet. Dette gjelder spesielt digitale styringssystemer (SCADA-systemer) og annen viktig infrastruktur, som kobles til internett for å kunne fjernstyres, som igjen gjør dem svært sårbare for cyberangrep over internett.

Mobilitet og trådløshet er i sterk utvikling, og det ventes at utviklingen vil fortsette. Mobile enheter er ofte koblet til flere typer nettverk. Nettverkene varierer i sikkerhet og robusthet, som gir mulighet for overvåking og avlytting av brukeren. Overvåking og avlytting kan gjøres med enkelt utstyr og krever kun helt grunnleggende IT-kompetanse. På arbeidsplassen kan én kompromittert enhet gi tilgang til både åpen og kryptert informasjon og være opphav til et fjernstyrt avlyttingsnettverk med mikrofon og kamera i kontorer over hele virksomheten.

UTILSTREKKELIG SIKKERHET MOT AVLYTTING AV ELEKTRONISK INFORMASJON. Kommunikasjon (tale og data) og lagring (data) lar seg avlytte med relativt enkle midler dersom det ikke tas skritt for å beskytte denne. Kryptering bidrar til å sikre data mot avlytting, men det er varierende bruk av kryptering på data som er sensitive men ikke underlagt sikkerhetsloven. Eksempler på sensitiv ugradert informasjon kan være helseopplysninger, privat epost, bedriftshemmeligheter med mer. Til tross for at det eksisterer kommersielt tilgjengelige løsninger for å kryptere tale og data, er det mange aktører som ikke benytter seg av dette. Manglende bruk av kryptering medfører at ugradert men sensitiv informasjon ofte er utsatt for avlytting.

BEHOV FOR TILLIT TIL DIGITALE SERTIFIKATER. Det er i dag flere ulike aktører som tilbyr digitale sertifikattjenester. Et digitalt sertifikat kan sammenlignes med et elektronisk pass eller identitetskort som kan brukes som digital legitimasjon. I senere tid har man hatt tilfeller der utsteder av sertifikater har hatt svakheter i sin sikkerhet. Det kan videre være problematisk å kjøpe sertifikattjenester fra aktører som er underlagt kontroll av andre lands myndigheter. Det er derfor sentralt å ha tillit til aktører som skal utstede dette, og deres løsninger.

NSM utsteder i dag digitale sertifikater til bruk i forsvarssektoren. Det er imidlertid ikke en enhetlig tilnærming til dette i offentlig forvaltning i Norge i dag.

UTILSTREKKELIG BRUK AV INNTRENGNINGSTESTING. Mange norske virksomheter har store digitale sårbarheter. I tillegg ser NSM at det også ofte er dårlig fysisk sikkerhet i virksomhetene. Dette medfører at det i mange tilfeller er enkelt å gjøre digitale innbrudd i datasystemer, fysisk stjele informasjon eller ødelegge systemer. NSM har gjennom inntrengingstesting avdekket en rekke alvorlige sårbarheter innen en lang rekke samfunnssektorer.

NSM ser at inntrengingstesting bidrar til ytterligere sikkerhet i samfunnet. Til tross for dette fremstår det for NSM som at bruken av slik testing er lite utbredt i de fleste sektorer.

I dag har NSM mandat til etter forutgående samtykke fra virksomheten å gjennomføre inntrengningstesting i graderte systemer og i ugraderte systemer i virksomheter som er omfattet av sikkerhetsloven. Utover dette har ikke NSM hjemmelsgrunnlag for å drive slik testing. I dialog med virksomheter som ikke er underlagt sikkerhetsloven har NSM en utfordring med å anbefale konkrete kommersielle leverandører. Dette som følge av at det ikke eksisterer en nasjonal standard eller akkrediteringsordning.

MANGLENDE TILSYNSKOMPETANSE PÅ IKT. Tilsynsmeldingen (St.meld. nr. 17 (2002-2003)) peker på behov for klare og tydelige formål for tilsynene. Dette innebærer at motstridende formål skal unngås i samme tilsyn. Men samtidig bør man unngå at de samme formål ivaretas av forskjellige tilsyn. Der flere organer fører tilsyn med IKT-sikkerhet i de samme systemene, kan dette fremstå som fragmentert og ukoordinert fra myndighetenes side

og oppleves unødvendig ressurskrevende for tilsynsobjektene.

NSM har i dag høy kompetanse på IKT-sikkerhetsområdet, men begrenset kapasitet til å gjennomføre tekniske IKT-sikkerhetstilsyn.

Det finnes i dag over 40 statlige tilsyn. De fleste av disse kontrollerer innenfor sine respektive regelverk at virksomhetene har et styringssystem eller internkontrollsystem på plass. Kompetansen til å gjennomføre tekniske IKT-sikkerhetstilsyn er svak hos mange tilsynsmyndigheter. NSM anser at det ikke er tilstrekkelig IKT-sikkerhetskompetanse nasjonalt til at alle tilsynsmyndigheter kan bygge opp egne IKT-sikkerhetsmiljøer.

NSMS TILSYNSROLLE. NSM er pålagt å ta brukerbetaling for enkelte tjenester. I tillegg utøver NSM godkjenningsmyndighet, og gir råd og veiledning. NSM har videre ansvar for NorCERT-funksjonen og koordinerer håndteringen av IKT-sikkerhetshendelser nasjonalt. NSM opplever at disse rollene problematiseres av enkelte i forbindelse med at NSM også har tilsynsmyndighet.

I henhold til tilsynsmeldingen er tilsyn definert til å omfatte alle virkemidler myndigheten har for å sikre etterlevelse av regelverket, herunder forhåndsgodkjenninger samt råd og veiledning. Så fremt virksomheten står fritt til å etterspørre disse tjenestene, vil det i utgangspunktet ikke oppstå en rollekonflikt om disse er brukerfinansierte.

Det er derfor NSMs vurdering at det heller ikke er en utfordring at samme direktorat både er tilsynsmyndighet og bistår virksomhetene med håndtering av IKT-hendelser. Dette understøttes av at NSMs tilsynsrolle er begrenset til sikkerhetsloven, og at bistand til håndtering av IKT-sikkerhetshendelser i hovedsak gjelder ugraderte systemer som vi ikke fører tilsyn med.

[17] http://www.dhra.mil/perserec/currentinitiatives.html#ADS

9. Personellsikkerhet

KOMPLISERT OG TIDKREVENDE PROSESS FOR SIKKERHETSKLARERINGER. Alle som skal ha tilgang til sikkerhetsgradert informasjon må autoriseres, og ved tilgang til høyere graderingsnivå enn BEGRENSET også sikkerhetsklareres. Hensikten er å redusere risikoen for innsidere. Regelverket for personellsikkerhet er detaljert og omfattende. Rettssikkerhet og personvern må ivaretas samtidig som samfunnets behov for sikkerhet imøtekommes. Klareringsprosessen er i mange saker tidkrevende. Det fører til samfunnsøkonomiske tap ved at personell ikke kan benyttes rettidig av arbeids- eller oppdragsgivere. Det er til personlig belastning for personellet det gjelder. Lang saksbehandlingstid påvirker også statens konkurranseevne, da man mister mange godt kvalifiserte kandidater til andre stillinger som følge av en lang klareringsprosess.

Norske rutiner for klareringsprosessen er preget av manuell saksbehandling. NSM er kjent med at enkelte andre land har saksbehandlingsverktøy som i stor grad prosesserer slike saker automatisk, supplert med manuelle stikkprøver. For eksempel har USA et system for Automated Decision Support (ADS) som de antar behandler cirka 30 prosent av klareringssakene for militær sektor[17].

I 2006 ble det i større grad enn tidligere åpnet for å gi utenlandske statsborgere sikkerhetsklarering. Som en følge av lovendringen, har antallet anmodninger om klarering av personer med tilknytning til andre land økt kraftig. Det samme gjelder også norske statsborgere med utenlandsk tilknytning. Antallet forventes å stige. NSM ser også en økning av klareringssaker der privatøkonomi, psykisk helse og tilknytning til organiserte kriminelle miljøer er sentrale vurderingstemaer.

De kompliserte vurderingene kombinert med et krevende regelverk stiller krav til stor bredde i kompetanse som må være tilgjengelig for klareringsmyndighetene. Relevante fagfelt er blant annet psykologi, statsvitenskap, sosiologi, rettsvitenskap, religionsvitenskap og etterforskning. Som fagmyndighet har NSM ikke vært i stand til

å utvikle kompetanse og veilede på dette området i tilstrekkelig grad.

LITE EFFEKTIVE PROSESSER VED INNHENTING OG BEARBEIDING AV INFORMASJON. Innhenting av informasjon om personell som skal sikkerhetsklareres skjer fra mange ulike registre. Prosessen er til dels manuell og tidkrevende. Enkelte operasjoner kunne med fordel vært automatisert eller effektivisert gjennom elektronisk datautveksling direkte mellom aktørene[18]. Gjeldende regelverk gir ikke NSM hjemmel til å kreve automatisert elektronisk utlevering fra de ulike registrene.

Informasjonsteknologien har betydning for kildeomfanget for klareringsmyndighetene. Mye relevant kildemateriale er lett tilgjengelig på internett, uten at det i dag foretas systematisk innhenting av informasjon i forbindelse med klareringsprosesser. I tråd med at teknologien utvikles, endres kilderegistrene hurtigere og nye registre etableres.

Klareringsmyndighetene har i dag ingen direkte oppslagsmulighet i kilderegistrene. Når de skal innhente tilleggsopplysninger, vil innhentingen derfor skje manuelt. Det bidrar til at saksbehandlingstiden blir lengre.

I flere innsidesaker har det i forkant vært tegn på at vedkommende har vært eller var i ferd med å bli en utro tjener. Nye sårbarheter oppdages ofte i forbindelse med kildekontroll ved reklarering etter fem år. NSM er kjent med at andre land reduserer denne risikoen gjennom regelmessige automatiske registerkontroller av personell som har en gyldig klarering. Slike regelmessige kontroller gir også mulighet til å bedre kunne håndtere sårbarheter som oppstår. For eksempel utvikler USA et slikt system, betegnet Automated Continuous Evaluation System (ACES)[19]. Slike systemer vil også bidra til en mindre ressurskrevende reklareringsprosess da oppståtte sårbarheter har blitt håndtert fortløpende.

HJEMMELSGRUNNLAGET VANSKELIGGJØR UTLEVERING AV INFORMASJON. Risikoen for innsidere er blitt mer kompleks. Personell som sikkerhetsklareres er mer eksponert for trusselaktører, som viser stor evne og vilje til å utnytte sårbarheter. Bevisst eller ubevisst tas det i dag også en større risiko enn tidligere, ved at det klareres og autoriseres flere personer som kan ha andre lojaliteter eller sårbarheter som i gitte situasjoner kan utnyttes. For å møte denne utviklingen er det behov for å kunne utveksle informasjon med PST og eventuelt andre om enkeltsaker i langt større grad enn i dag.

Det er i dag begrensninger i regelverket for personellsikkerhet som vanskeliggjør slik utveksling. Opplysninger som er gitt klareringsmyndigheten i forbindelse med personkontroll, skal ikke benyttes til andre formål enn vurdering av sikkerhetsklarering. Eksempelvis vil PST da ikke ha tilstrekkelig evne til å gjøre målrettet oppfølging av den økte restrisikoen. Situasjonen gjør at det må tas stilling til hvor mye usikkerhet samfunnet aksepterer, herunder om det bør innføres nye risikoreduserende tiltak som kan synes inngripende i personvernet.

MANGE BLIR UNØDIG SIKKERHETSKLARERT. Det er i dag ulike ordninger for bakgrunnskontroll i Norge. Ordningene varierer både med hensyn til informasjonsgrunnlag for vurderinger som blir gjort, og rettsikkerhet og personvern til den som kontrolleres. Eksempler på slike ordninger er vandelskontroll etter politiregisterloven, kredittkontroll, egne sektorvise kontrollordninger etter særlovgivning, og sikkerhetsklarering etter sikkerhetsloven. Sikkerhetsklarering er den klart mest inngripende kontrollen. Samtidig er sikkerhetsklarering den ordningen som best ivaretar den enkeltes rettssikkerhet. I enkelte av kontrollordningene mangler for eksempel skriftlig begrunnelse for ufordelaktig avgjørelse og klageordning (to-instansbehandling) for den som kontrolleres.

Noen virksomheter benytter sikkerhetsklareringer til å få undersøkt personell som verken skal ha, eller vil kunne få, tilgang til skjermingsverdig informasjon eller objekter. Sikkerhetsklarering benyttes da som en slags bakgrunnskontroll i mangel på andre hjemler for slik kontroll.

MANGLENDE SIKKER IDENTIFIKASJON I PERSONKONTROLLEN. En bakgrunnskontroll har kun verdi dersom det er riktig person som kontrolleres. Dette betyr at sikker identifisering av personellet er viktig. På samme måte er det også viktig å være trygg

[18] Noe av informasjonen i klareringssaker innhentes i dag ved at kilden tar ut informasjonen fra sitt digitale system og sender denne med posten, hvorpå klareringsmyndigheten deretter digitaliserer denne igjen for å legge den inn i eget system.

[19] http://www.dhra.mil/perserec/currentinitiatives.html#ACES

på at det personellet som til slutt gis tilgang faktisk er det samme personellet som er kontrollert. NSM er kjent med saker fra det private næringsliv der det er andre personer enn de som egentlig er ansatt som utfører arbeidet, gjerne om natten.

MANGLENDE KOMPETANSE I DEN ENKELTE VIRKSOMHET TIL Å MOTVIRKE INNSIDETRUSSELEN. Det kreves målrettet innsats i den enkelte virksomhet for å motvirke innsidetrusselen. I dag er det få virksomheter som arbeider systematisk for å motvirke innsidetrusselen. Dette skyldes primært mangel på kompetanse og gode systemer som kan implementeres. Tilstrekkelig prioritering av arbeidet er også viktig. NSM har i dag ikke kapasitet til å understøtte alle virksomheter som ber om bistand innen fagfeltet.

10. Fysisk sikkerhet

KONKURRERENDE GRUNNLAG FOR PRIORITERING AV SIKRINGSSTYRKER. I tillegg til objekteiers egne grunnsikrings- og påbygningstiltak, kan både politiet og Forsvaret sikre objekter med sikringsstyrker ved forhøyet trussel. For enkelte objekter er det forhåndsplanlagt med slike sikringsstyrker. Flere ulike ordninger for klassifisering av objekter og infrastruktur vanskeliggjør imidlertid en god prioritering av sikringsstyrkene. Utfordringen blir særlig tydelig i vektingen av behovet for sikringsstyrker på tvers av ulike sektorer. Uten en helhetlig nasjonal oversikt etter like kriterier er det meget vanskelig å prioritere sikringsstyrker slik at det reflekterer nasjonale sårbarheter.

RÅDGIVING FRA SMÅ OG SPREDTE FAGMILJØER. De statlige fagmiljøene innen fysisk sikkerhet er relativt små og spredt i ulike etater med ulikt hjemmelsgrunnlag. I tillegg har små fagmiljøer begrenset evne til å holde seg oppdatert på utvikling og produkter innenfor et så vidt fagområde.

NSM er fagmyndighet for kravene etter sikkerhetsloven, og har veiledningsplikt iht. sikkerhetsloven § 9 og forvaltningsloven § 11. PST har etablert en viss kapasitet innen rådgivning i fysisk sikkerhet, med utgangspunkt i PSTs instruks § 6. PSTs rådgivningsfunksjon gjelder også overfor norske næringslivsinteresser. Det er imidlertid en glidende overgang, da næringsaktører og offentlige etater med betydning for nasjonal sikkerhet også kan omfattes av NSMs ansvarsområde. PST og NSM gir råd innen fysisk sikkerhet til mange av de samme virksomhetene. NSM og PST har samarbeidet innen råd og veiledning vedrørende informasjons- og objektsikkerhet i en årrekke, men uten en formalisert avtale. Forsvarsbygg har et nasjonalt kompetansesenter for sikring av bygg som tar oppdrag spesielt i Forsvaret, men også til annen offentlig virksomhet og privat sektor på kommersiell basis. Forsvarsbygg har også et eget forskningsmiljø som kommer kompetansesenteret til gode. NSM og Forsvarsbygg har et samarbeid med en formell avtale som grunnlag. Det er flere statlige sektortilsyn som følger opp bestemmelser i sektorregelverk når det gjelder sikring av infrastruktur mot ulike former for anslag. Det er uheldig dersom det oppstår situasjoner hvor ulike statlige instanser for rådgivning innen fysisk sikkerhet ikke er samstemte. Prosjektering av fysiske sikkerhetstiltak kan være tids- og kostnadskrevende for virksomhetene. NSMs erfaring er at mange har lav kompetanse på anskaffelse av fysiske sikringstiltak. Valg av feil løsninger kan være dyre og vanskelig å rette opp. Mange virksomheter vil være avhengig av profesjonelle og uavhengige råd for å treffe riktige beslutninger. Det er derfor en utfordring at rådgivningsmiljøene er små og fragmenterte.

UENIGHET OM BEHOV FOR SIKRING. Sikkerhetslovens objektsikkerhetsregime er avhengige av at alle sektormyndigheter samarbeider. Sett i lys av erfaringene fra utvelgelsesprosessen, vil det fortsatt kunne oppstå situasjoner der det er nødvendig å avdømme uenighet om et objekts skjermingsverdighet. NSM forutsetter at problemstillingen behandles av Sikkerhetsutvalget, og utdyper derfor ikke dette nærmere.

SIKKERHETSDESIGN. Det er krevende og kostbart å installere fysiske sikkerhetstiltak i ettertid. NSM

har i samarbeid med PST tatt initiativ til å lansere begrepet sikkerhetsdesign blant norske arkitekter og byplanleggere. Målet er å bidra til bevisstgjøring om sikkerhet i en plan- og byggeprosess, men også øke kreativiteten for effektive løsninger. Dette vil i sin tur bidra til en bedre samfunnsøkonomisk anvendelse av tilgjengelige sikringsressurser. Det er noe diskusjon blant byggherrer, objekteiere, arkitekter og samfunnsvitere om hva begrepet sikkerhetsdesign egentlig inneholder. Det er varierende kunnskap hos relevante aktører, hvilket gjør at den offentlige debatten tidvis sporer av til løsrevede problemstillinger. At fleksible konsepter for sikkerhetsdesign fortsatt er lite kjent av aktørene gjør det utfordrende å gjennomføre byggeprosesser med god sikkerhetsdesign og gode løsninger.

11. Samarbeid med næringslivet

SPREDTE TILTAK. Dagens tiltak for myndighetenes samarbeid med næringslivet innen sikkerhet er spredte, uten en helhetlig tilnærming for samarbeid på de ulike områdene. Det er ulike problemstillinger dette dreier seg om, alt fra kunnskap om anskaffelsesplaner i tilknytning til fremtidige behov og bestillerkompetanse på den ene siden, til informasjon om trussel- og risikobildet og krav til sikring på den andre siden.

FLERE ANSKAFFELSER KAN SIKRES BEDRE. Ordningen med sikkerhetsgraderte anskaffelser er lite benyttet i sivile sektorer. Det er antakelig langt flere anskaffelser som burde sikres ved hjelp av ordningen. NSM har ikke i tilstrekkelig grad kunnet gi målrettet rådgiving mot sivile sektorer. Ressursene har gått med til enkeltsaksbehandling av leverandørklareringer.

Næringslivet trenger informasjon om hvilke anskaffelsesplaner det offentlige har som kunde for å kunne redusere kommersiell risiko og innrette sin virksomhet mot de fremtidige behovene planene representerer. På den annen side må også det offentlige utvikle bedre bestillerkompetanse, slik at det er de rette produktene og løsningene som anskaffes.

BEHOV FOR PRIVAT RÅDGIVNING. Det er vanskelig for potensielle kunder å få oversikt over aktørene og kvaliteten på tjenestene innen IKT-sikkerhetsrådgivning. Det eksisterer ikke i dag en akkrediteringsordning som omfatter aktører som tilbyr rådgivning og andre tjenester innenfor IKT-sikkerhetsområdet.

12. Kompetanse

MANGEL PÅ KOMPETANSE OM IKT-SIKKERHET. Mangelen på kompetanse om IKT-sikkerhet er en stor utfordring for sikkerhetsarbeidet i samfunnet. På kort sikt er mangelen på IKT-sikkerhetskompetanse kritisk. Mangel på kompetanse påvirker evnen til både å løse nasjonale sikkerhetsoppgaver, og sikre norske virksomheter.

Opplæringen innen informasjonssikkerhet i Norge er i dag individuell og tilfeldig[20]. Mangel på sikkerhetsopplæring i utdanningsprogrammer for IKT også internasjonalt bidrar i betydelig grad til digitale sårbarheter[21].

Det utdannes for få med den kompetansen NSM og resten av samfunnet i økende grad etterspør. Årlig tas rundt 1500 studenter opp i ulike IKT-utdanninger på universiteter og høgskoler i Norge. På flere universiteter er ikke IKT-sikkerhet et obligatorisk fag som ledd i IKT-utdannelsen. Det betyr at studenter som skal bygge vår fremtidige infrastruktur og applikasjoner ikke har den grunnleggende kompetansen for sikring av IKT-systemer. Konkurransen om de nyutdannede er hard, da det er få kvalifiserte kandidater med både sikkerhetsfaglig og høyere teknisk utdanning tilgjengelig.

BEHOV FOR MER FORSKNINGSBASERT KUNNSKAP. Forskning og utvikling er spredt på mange små fagmiljøer. Det skjer ingen samlet satsning innen feltene, til tross for et stort behov i samfunnet som

[20] «Opplæring i informasjonssikkerhet», Nina Hoddø Bakås, Universitetet i Oslo, 2015

[21] «Cybersecurity through Secure Software Development», artikkel av Audun Jøsang, Marte Ødegaard og Erlend Oftedal 2015

vil øke kraftig i årene fremover. Sikkerhet mot tilsiktede uønskede handlinger (security) er lite utviklet som akademisk fagfelt i Norge, i motsetning til sikkerhet mot tilfeldige hendelser (safety). Feltet har lite publisering å vise til, og taper ofte kampen om ressursene og oppmerksomheten internt på utdanningsinstitusjonene. Det er behov for mer forskningsbasert kunnskap.

OPPLÆRING I SIKKERHET. NSMs erfaringer viser er at det er stort behov for opplæring av kortere varighet for personell med sentrale eller spesialiserte sikkerhetsoppgaver i både offentlig og privat sektor.

13. NSMs understøttelse av Forsvarets operative evne

Som nevnt i del I, er en betydelig del av NSMs ressurser innrettet mot å støtte og øke Forsvarets operative evne. NSMs nåværende støtte favner et bredt spekter av ulike fag- og leveranseområder. Generelt ser NSM at Forsvarets behov for støtte er større en NSMs kapasitet og ressurstildeling tillater.

NSM understøtter i dag et betydelig antall av Forsvarets materiellprosjekter. Disse prosjektene skal realisere operativ effekt gjennom nye kapasiteter, materiell og kompetanse. Støtten omfatter råd- og veiledning, sikkerhetsgodkjenning samt produksjon i arbeids- og styringsgrupper. Nåværende ressurstildeling svarer ikke til behovet sett opp mot antall aktiviteter og kompleksiteten i disse.

Antall cyberhendelser er økende i forhold til kapasiteten til å håndtere dem. Effektiv håndtering av cyberhendelser har også betydning for Forsvarets operative evne og evne til sikker drift av Forsvarets strategiske og taktiske systemer.

Det er i dag betydelige utfordringer med å få til rettidig sikkerhetsklarering av personell. Dette har stor betydning for Forsvarets operative evne og mulighet for omstilling og effektivisering.

14. Evner og kapasitet i Nasjonal sikkerhetsmyndighet

I del I ble NSMs foreløpige oversikt over organisasjonens evner presentert. NSM har så langt ikke adoptert fullt ut den metodiske tilnærming til Forsvaret og FD når det gjelder utvikling av evner. Mangel på dette gjør det utfordrende å ha en strukturert tilnærming til evner og evneutvikling, og ha en realistisk dialog med styrende departement og andre aktører om utvikling av organisasjonen.

Selv om det ikke foreligger en fullverdig modell, er det likevel mulig å sammenfatte enkelte utfordringer knyttet til NSMs evner og kapasiteter. Dette følger under.

SMÅ OG SÅRBARE FAGMILJØER. Små og sårbare fagmiljøer er en kritisk utfordring for NSM. Vi erfarer at det blir stadig mer krevende å levere når etterspørselen etter tjenester fra NSM øker til et nivå som ikke står i forhold til ressursene. NSM er nå kommet til et punkt der effektivisering og mindre justeringer ikke lenger er tilstrekkelig for å tilfredsstille leveransebehovet i samfunnet. Gapet mellom samfunnets behov og NSMs leveranseevne øker. Innen personellsikkerhet er det utfordringer relatert til kapasitet i gjennomføring av rettidig sikkerhetsklarering og utvikling av fagområdet, som nevnt under utfordringer innen personellsikkerhet.

BEHOV FOR RÅDGIVNING. Både virksomheter som har vært utsatt for hendelser, og virksomheter der NSM har vært på tilsyn, har et stort behov for oppfølgende rådgivning og kompetansebygging. Dette behovet er NSM per i dag ikke i stand til å møte. Særlig ser vi at den økende mengden med IKT-sikkerhetshendelser gjør at det er svært krevende å kunne gi god nok støtte til de virksomheter som rammes. Til tross for at vi er i ferd med å etablere en mer skalerbar modell for å støtte og samhandle med ulike aktører, erfarer NSM at det er et gap mel-

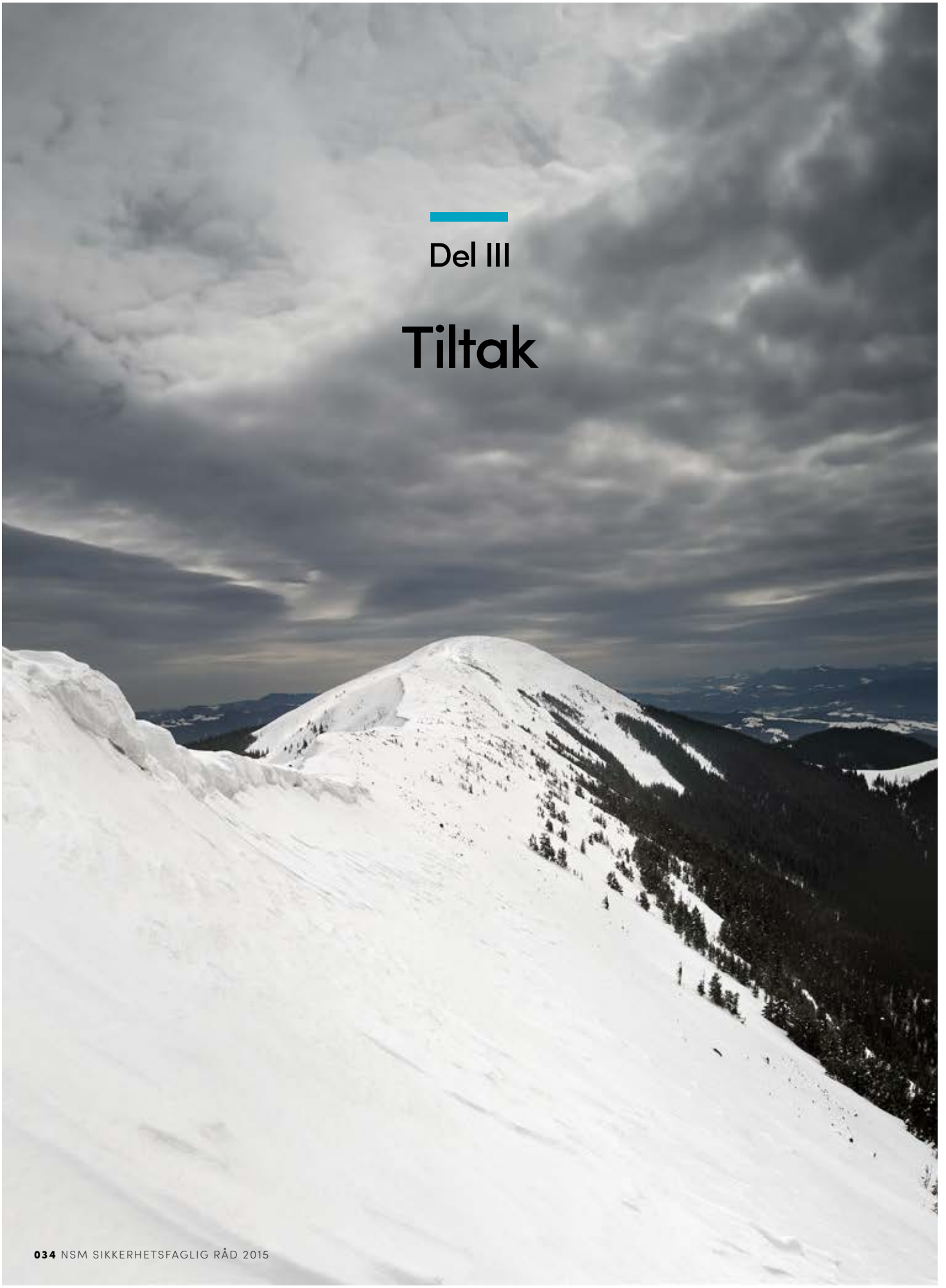
lom behovet for støtte og det vi er i stand til å yte. NSM erfarer videre at både FD og JD har behov for substansielle bidrag til støtte for sin politikkutforming innenfor samfunnssikkerhet og beredskap. Behovet er større enn det NSM er i stand til å etterkomme på en forsvarlig måte.

NSM støtter til enhver tid en betydelig andel av Forsvarets prosjekter med rådgiving innen ulike områder, sikkerhetsgodkjenning, så vel som deltagelse i arbeidsgrupper og utredninger. Støtten til prosjektene er således ikke avgrenset til selve godkjenningsprosessen. NSM har ikke ressurser til å støtte Forvarets prosjekter i en tilfredsstillende grad, gitt antall aktiviteter og spennet av de ulike aktivitetsområdene.

FORSKNING OG UTVIKLING. NSM har i løpet av de siste to årene bygget opp en portefølje for forskning og utvikling. Det er i dag flere nødvendige aktiviteter som det ikke finnes økonomisk handlingsrom for å håndtere. Det betyr at relevante og kritiske prosjekter for samfunnet ikke kan starte opp som ønsket.

INVESTERINGER OG FORUTSIGBARHET. En annen utfordring er NSMs tilgang på materiellinvesteringsmidler gjennom forsvarssektorens investeringsportefølje. Som deltaker i forsvarssektorens investeringsportefølje, er NSM kun en av mange aktører som til enhver tid fremmer behov. Investeringsbehov innenfor NSMs virkeområde kan være tidskritiske å gjennomføre. Særlig i perioder med store investeringer i Forsvaret, kan det være utfordrende å sikre at nye prosjekter opprettes og gjennomføres i tide. Til tross for positiv utvikling i senere tid, ønsker NSM større forutsigbarhet i forhold til behov for investeringer.

KUNNSKAP OM TEKNOLOGISK UTVIKLING. Den teknologiske utviklingen går raskt, og utfordrer både strategisk og teknisk nivå. Mesteparten av utviklingen av IKT-produkter og -tjenester foregår internasjonalt. Andre, større land enn Norge utvikler fortløpende strategier og handlingsplaner for å møte utviklingen sikkerhetsmessig. I fremtiden vil flere sikkerhetsløsninger, selv for høygraderte systemer, basere seg på kommersielle produkter som utvikles i enda større hastighet enn tradisjonelle offentlige prosjekter/produkter. Hastigheten på utviklingen, og muligheten til å ligge i forkant for å utvikle sikkerhetsmessige løsninger på ny teknologi både teknisk og strategisk, er en utfordring.



Del III

Tiltak

Nedenfor presenteres NSMs anbefalte tiltak for å styrke sikkerheten frem mot 2020 og fremover.

15. Tiltak innen organisering, ledelse og koordinering

STYRKE JUSTIS- OG BEREDSKAPSDEPARTEMENTETS KOORDINERINGSANSVAR OG -ROLLE. NSM anbefaler ikke at det gjøres vesentlige endringer i den organisatoriske strukturen som er lagt for å styre og koordinere arbeidet med samfunnssikkerhet og beredskap etter 22. juli 2011. NSM mener likevel det er behov for å tydeliggjøre og styrke rollen til noen av aktørene, og sette dem ytterligere i stand til å ta den rollen de er tildelt. Vi opplever forholdet mellom Forsvarsdepartementet og Justis- og beredskapsdepartementet i det vesentligste som avklart. Det er imidlertidig sentralt at departementene har en løpende og tett dialog om oppgaveløsing og samhandling mellom sektorene. Det er i kapittelet om utfordringer nevnt utfordringene omkring koordinering og samordningsansvaret innen samfunnssikkerhet og beredskap. Det er en forutsetning for NSMs rolle som sektorovergripende myndighetsorgan at rollen Justis- og beredskapsdepartementet er tildelt som samordningsansvarlig innenfor samfunnssikkerhet og beredskap er klar og tydelig for alle aktører. I dette henseende er det viktig at de andre departementene og sektormyndighetene aksepterer og respekterer denne rollen og lar seg samordne på de områder der dette er særlig viktig.

For å klargjøre den strategiske rollen til Justis- og beredskapsdepartementet innenfor forebyggende IKT-sikkerhet i sivil sektor, anbefaler NSM at ansvarsfordelingen mellom Justis- og beredskapsdepartementet og Kommunal- og moderniseringsdepartementet tydeliggjøres ytterligere med utgangspunkt i Kgl.res. 22. mars 2013. Det betyr at Justis- og beredskapsdepartementet gis et tydeligere ansvar for IKT-sikkerhet, og at Kommunal- og moderniseringsdepartementet gis et tydeligere ansvar for leveranser av IKT-tjenester. Dette vil kunne gi et godt grunnlag for en videre operasjonalisering mellom NSM og DIFI.

Det er besluttet å opprette et eget sekretariat for Regjeringens sikkerhetsutvalg (RSU). Sekretariatet vil få en viktig støttefunksjon for arbeidet i RSU og skal ledes av en egen fagdirektør ansatt på Statsministerens kontor. En slik løsning endrer ikke de konstitusjonelle ansvarsforholdene for Justis- og beredskapsdepartementet og Forsvarsdepartementet. Ansvarsforholdene mellom Justis- og beredskapsdepartementet, Forsvarsdepartementet og Statsministerens kontor, bør tydeliggjøres og kommuniseres på en måte som hindrer eventuell opplevelse av uklarhet i ansvarsdelingen. Dette vil sikre trygghet for de involverte, og økt kunnskap og forståelse i samfunnet.

På bakgrunn av dette anbefaler NSM følgende tiltak:

1. Kgl.res. 22. mars 2013 bør operasjonaliseres for å tydeliggjøre og gi et konkret innhold til samordnings- og koordineringsrollen Justis- og beredskapsdepartementet har. Dersom resolusjonen ikke gir muligheter til hensiktsmessig operasjonalisering, anbefales det at resolusjonen endres.
2. Ansvar og oppgaver mellom NSM og DIFI bør tydeliggjøres på grunnlag av klargjøringen mellom Justis- og beredskapsdepartementet og Kommunal- og moderniseringsdepartementet.
3. Justis- og beredskapsdepartementet bør tilføres ytterligere ressurser og kompetanse for å styrke rollen som ansvarlig for forebyggende sikkerhet i sivile sektorer, herunder IKT-sikkerhet.
4. Dersom ansvarsforholdene mellom sentrale departementer og Statsministerens kontor oppleves som utydelige, bør de tydeliggjøres og kommuniseres på en måte som gir bred forståelse i samfunnet.

STYRKET STYRING OG KONTROLL MED FOREBYGGENDE SIKKERHET. Styring og kontroll med det forebyggende sikkerhetsarbeidet har mangler i mange virksomheter i Norge. Det gjør blant annet Justis- og beredskapsdepartementets arbeid med å ha oversikt over situasjonen mer utfordrende.

På bakgrunn av dette anbefaler NSM følgende tiltak:

5. Justis- og beredskapsdepartementet bør ytterligere styrke arbeidet med styring og kontroll av det forebyggende sikkerhetsarbeidet i offentlig forvaltning. Styrkingen skjer ved at Justis- og beredskapsdepartementet i kraft av sin koordinerings- og samordningsrolle beslutter at forebyggende sikkerhet skal inngå som en del av den formelle styringen i hver sektor.
6. Justis- og beredskapsdepartementet bør gi oppdrag til alle departementene om årlig å evaluere og rapportere sikkerhetstilstanden i eget departement og i sine sektorer til Justis- og beredskapsdepartementet. Rapporteringen bør inkludere private virksomheter som har samfunnsviktige funksjoner. Oppdraget bør synliggjøres i lederkontrakter, i tildelingsbrev og i etatsstyringsmøter. Dialog om virksomhetenes sikkerhetstilstand anbefales i tillegg å være tema i minst ett av etatsstyringsmøtene gjennom året.
7. Kommunal- og moderniseringsdepartementet bør ta inn krav til IKT-sikkerhetskompetanse i sin felles lederplattform i staten for å utvikle offentlige medarbeidere og ledere.
8. NSM går i dialog med Næringslivets sikkerhetsråd (NSR) med sikte på å etablere en frivillig ordning i næringslivet for årlig rapportering til NSR om sikkerhetstilstanden i virksomhetene, som kan oppsummeres og stilles til rådighet for NSM og andre, for å ivareta offentlige og private interesser.

SAMLOKALISERING AV NSM FOR Å STYRKE SIKKERHETSARBEIDET I SAMFUNNET. Styrkingen av NSM i 2013 og 2014 har gjort det nødvendig å etablere NSM på flere lokasjoner. For NSM som et relativt lite direktorat, er det krevende å være lokalisert på flere steder. Det er kostbart og lite effektivt. I tillegg er det krevende for egne ansatte og samarbeidspartnere, og svekker grunnlaget for å skape en felles kultur både internt og med samarbeidspartnere. Hensikten med en samlokalisering er å legge til rette for å styrke evnen til samarbeid mellom NSM og sentrale samarbeidspartnere i Forsvaret og sivile sektorer.

Det har i tidligere dialog med Forsvarsdepartementet, som en del av Perspektivplan EBA, vært diskutert ulike alternativer for en fremtidig samlokalisering av NSM. Et slikt prosjektforslag er foreløpig ikke prioritert inn i Perspektivplanen, men det er avgjørende for NSM at prosessen starter opp igjen.

På bakgrunn av dette anbefaler NSM følgende tiltak:

9. Forsvarsdepartementet bør ta initiativet til at NSM samlokaliseres så raskt som mulig. Prosessen med å vurdere løsninger for samlokalisering av NSM bør starte snarest. Det vises til tiltak 43 nedenfor om samlokalisering med ulike samarbeidspartnere i et nasjonalt cybersikkerhetssenter i NSMs lokaler.

STYRKE EVNEN TIL KOORDINERING OG SAMVIRKE I BEREDSKAPS- OG KRISESITUASJONER. I kapittelet om utfordringer, pekes det på flere områder som trenger klargjøring for å styrke den samlede evnen til samvirke i beredskaps- og krisesituasjoner, slik det forutsettes i nasjonalt beredskapssystem. Evnen til koordinering og samvirke er ennå ikke god nok. Det gjelder spesielt kompetanse og informasjonsflyt. De samme utfordringene er også erfart i flere øvelser, blant annet i en NATO-øvelse våren 2015 (CMX).

På bakgrunn av dette anbefaler NSM følgende tiltak:

10. Justis- og beredskapsdepartementet og Forsvarsdepartementet bør klargjøre hvilke private aktører som har en rolle i krise- og beredskapssituasjoner. Aktørene må bli satt i stand til, og ha nødvendig kompetanse til, å motta nødvendig sikkerhetsgradert informasjon. En nødvendig forutsetning for dette er at aktørene blir omfattet av sikkerhetsloven.
11. Det må etableres en enhetlig og sikker kommunikasjonsinfrastruktur som understøtter effektiv og rask informasjonsdeling og koordinerte beslutningsprosesser. Det vises også til tiltak under kapitlet om IKT-sikkerhet.
12. Forsvarsdepartementet og Justis- og bered-

[17] The Network and Information Security Directive

skapsdepartementet bør gi NSM i oppdrag å gjennomføre årlige nasjonale øvelser i IKT-sikkerhet og hendelseshåndtering, på samme måte som NATOs øvelse CMX gjennomføres innen NATO-strukturen.

16. Tiltak for å styrke IKT-sikkerhet

ORGANISERING, LEDELSE OG KOORDINERING

IMPLEMENTERING AV EUS DIREKTIV FOR NETTVERKS- OG INFORMASJONSSIKKERHET[22]. Kapitlene situasjon og utfordringer har vist at det er nødvendig å styrke IKT-sikkerheten i Norge for å motvirke tilsiktede uønskede handlinger, og redusere konsekvensen av disse gjennom god forebygging og evne til håndtering.

EU har under behandling et direktiv for forsterket nettverks- og informasjonssikkerhet (NIS-direktivet). Det antas at direktivet kan være EØS-relevant, når det eventuelt blir vedtatt. Direktivet inneholder en rekke tiltak for å styrke sikkerheten. NIS-direktivet er en forutsetning for innføringen av et digitalt indre marked i EU, som skal fjerne digitale hindringer og skape vekst og arbeidsplasser i Europa. En del av tiltakene er allerede implementert i Norge. Noen av disse bør videreutvikles og styrkes.

I tiltakene som NSM anbefaler i dette kapittelet vil det vises til NIS-direktivet der det er naturlig og hensiktsmessig for at sammenhengen skal komme tydelig frem. NSM understreker at Norge, uavhengig av EUs behandling av direktivet, har en egeninteresse av å gjennomføre de foreslåtte tiltakene på grunn av det betydelige omstillings- og samhandlingsbehovet samfunnet har innenfor forebyggende sikkerhet og beredskap.

På bakgrunn av dette anbefaler NSM følgende tiltak:

13. Innholdet i NIS-direktivet bør implementeres.

TYDELIGGJØRE DEN NASJONALE MYNDIGHETEN FOR IKT-SIKKERHET[23]. Innenfor sikkerhetslovens område er NSM den nasjonale myndigheten for IKT-sikkerhet. Roller og myndighet er her avklart.

Utenfor sikkerhetslovens område er det ikke like avklart. NSM er tillagt oppgaver og ansvar som nasjonalt fagmiljø for IKT-sikkerhet av Justis- og beredskapsdepartementet som følge av departementets ansvar for IKT-sikkerhet etter Kgl. res. av 22. mars 2013. I sin instruks er Sjef NSM gitt omfattende oppgaver og ansvar innen blant annet IKT-sikkerhet, herunder å koordinere håndteringen av alvorlige IKT-angrep. Instruksen er ikke formelt gjeldende utenfor forsvarssektoren eller gjort kjent.

På bakgrunn av dette anbefaler NSM følgende tiltak:

14. Med utgangspunkt i Instruks for Sjef NSM gitt av Forsvarsdepartementet i samråd med Justis- og beredskapsdepartementet, og NSMs rolle i det nye nasjonale beredskapssystemet, bør det fastsettes en Kgl.res. for å gi NSM et tydelig tverrsektorielt mandat og styrke rollen som den nasjonale myndigheten for IKT-sikkerhet også utover sikkerhetsloven, og være strategisk IKT-sikkerhetsrådgiver i hele krisespennet. En Kgl.res. vil også tydeliggjøre og gjøre offentlig kjent Sjef NSM sin rolle som nasjonal og tverrsektoriell koordinator for håndtering av IKT-sikkerhetshendelser.

ETABLERING AV ATTACHÉORDNING FOR SIKKERHETSTEKNOLOGI. Den teknologiske utviklingen går raskt, og utfordrer både strategisk og teknisk nivå. Mesteparten av utviklingen av IKT-produkter og -tjenester foregår internasjonalt. Andre, vesentlig større land enn Norge, utvikler fortløpende strategier, handlingsplaner og konkrete tiltak for å møte utviklingen sikkerhetsmessig. Både politiet og Forsvaret har attachéordninger for kunnskapsinnhenting og nettverksbygging internasjonalt. NSM har på samme måte behov for en styrket evne til kunnskapsinnhenting fra andre land, både om den teknologiske utviklingen, og hvordan denne blir møtt sikkerhetsmessig. Det er sentralt å være oppdatert på utviklingen av sikkerhetstiltak internasjonalt.

[22] The Network and Information Security Directive

[23] Iht. NIS-direktivet artikkel 15

På bakgrunn av dette foreslår NSM følgende tiltak:

15. Forsvarsdepartementet bør styrke NSM for å kunne etablere en ordning med attachéer i ett eller flere land for å styrke evnen til kunnskapsinnhenting internasjonalt om IKT-sikkerhet generelt, og konkrete handlingsplaner og tiltak spesielt.

STYRKE NASJONALT SAMARBEID OG INFORMASJONSDELING VEDRØRENDE IKT-SIKKERHET. Den økende kompleksiteten i samfunnet med sterke tverrsektorielle avhengigheter nødvendiggjør økt samarbeid og informasjonsdeling mellom aktører på ulike nivåer og ulike sektorer, både private og offentlige.

Det er etablert ulike arenaer og nettverk på operativt nivå. Det er imidlertid ikke etablert tilsvarende på strategisk nivå nasjonalt. På strategisk nivå bør det etableres et råd som kan gi Forsvarsdepartementet og Justis og beredskapsdepartementet anbefalinger om IKT-sikkerhet. Rådet ledes av NSM som det nasjonale fagmiljøet for IKT-sikkerhet. I tillegg må arenaer og nettverk på operativt nivå styrkes og videreutvikles.

NSM anbefaler derfor at det etableres en formalisert struktur som knytter sammen ulike samarbeidsarenaer fra strategisk til operativt nivå. Hensikten er å utvikle kompetanse, skape felles forståelse og dele informasjon om utfordringer og løsninger innenfor IKT-sikkerhet. Foruten ulike myndighetsaktører, bør eiere av kritisk infrastruktur og andre sentrale næringslivsorganisasjoner og aktører delta. Tilsvarende strukturer er etablert i andre land, som følges opp av NSMs søsterorganisasjoner.

For å støtte denne strukturen ivaretar NSM funksjonen som permanent sekretariat. Det er mange aktører, og koordinerings- og sekretariatsrollen er ressurskrevende. NSM må styrkes for å kunne ivareta denne rollen.

På bakgrunn av dette anbefaler NSM følgende tiltak:

16. Forsvarsdepartementet bør styrke NSM for å videreutvikle eksisterende og etablere nye samarbeidsarenaer i en formalisert og helhetlig struktur på strategisk og operativt nivå.
17. Forsvarsdepartementet bør styrke NSM, og gi NSM i oppdrag å lede et tverrsektorielt råd på strategisk nivå som gir anbefalinger til Justis- og beredskapsdepartementet, Forsvarsdepartementet og andre sentrale departementer og virksomheter om IKT-sikkerhet.

REVIDERE DEN NASJONALE STRATEGIEN FOR INFORMASJONSSIKKERHET[24].

Nasjonal strategi for informasjonssikkerhet ble vedtatt i 2012. I 2013 ble ansvaret for forebyggende IKT-sikkerhet overført fra nåværende Kommunal- og moderniseringsdepartementet til Justis- og beredskapsdepartementet. Nåværende strategi tydeliggjør i for liten grad roller og ansvar. Dette svekker evnen til effektiv implementering og oppfølging av strategien. Som følge av endringer i risikobildet vil det være naturlig å vurdere tiltakene i strategien på nytt. Det bør vurderes om denne strategien bør forankres i en overordnet nasjonal sikkerhetsstrategi, hvor informasjonssikkerhet inngår som en delstrategi.

På bakgrunn av dette anbefaler NSM følgende tiltak:

18. Justis- og beredskapsdepartementet og Forsvarsdepartementet bør utarbeide en ny nasjonal strategi for informasjonssikkerhet. Strategien må være basert på et oppdatert IKT-risikobilde. Mål og prioriteringer må tydeliggjøres i større grad enn i dag. Det er viktig at roller og ansvar beskrives tydelig, og at tiltakene dekker både forebygging, evne til hendelseshåndtering og koordinering.
19. Justis- og beredskapsdepartementet og Forsvarsdepartementet bør utarbeide en ny overordnet handlingsplan tilknyttet strategien. Denne bør følges opp og revideres jevnlig. I handlingsplanen bør ansvars- og samarbeidsforhold og prosesser knyttet til dette konkretiseres ytterligere. En nasjonal øvingsplan for IKT-sikkerhet og samhandling mellom aktørene bør inngå.
20. Justis- og beredskapsdepartementet og Forsvarsdepartementet bør vurdere å ta initiativ til at det utvikles en nasjonal sikkerhetsstrategi.

[24] Iht. NIS-direktivet artikkel 4 og 5

ETABLERING AV NASJONALE MINIMUMSKRAV OG ANBEFALINGER[25]. Mange og fragmenterte regelverk innenfor IKT-sikkerhetsområdet er en utfordring. NSM foreslår å samle nasjonale krav og anbefalinger inn under ett felles, nasjonalt rammeverk for sikring av samfunnsviktige IKT-løsninger. Det bør legges opp til at bruk av nasjonale anbefalinger er hovedregelen, og at det kun stilles krav der det er nødvendig. Rammeverket bør beskrive minimumsbehov for sikkerhet gjennom å definere sikringsnivåer. Sikringsnivåene bør fastsettes ut fra en risikovurdering. Rammeverket skal gjøre det enklere for sektorer og virksomheter å oppfylle krav i ulike regelverk, og på den måten legge til rette for felles tekniske løsninger.

Det nasjonale rammeverket bør dekke de viktigste sikringsbehovene og anbefalte tiltak knyttet til disse, og bør innbefatte relevante anbefalinger innen personellsikkerhet og fysisk sikkerhet.

Parallelt med utviklingen av et slikt nasjonalt rammeverk bør det vurderes å utvikle en lovgivning med tverrsektorielle krav til sikring av sensitiv informasjon. En slik lovgivning bør utformes slik at den imøtekommer relevante internasjonale krav, herunder de krav som det antas at EU vil stille til forsterket nettverkssikkerhet (utkast til NIS-direktiv). NSM har fremmet en skisse til slik lovgivning overfor Justis og beredskapsdepartementet.

På bakgrunn av dette anbefaler NSM følgende tiltak:

21. Justis- og beredskapsdepartementet bør gi NSM i oppdrag å utvikle et nasjonalt rammeverk innenfor IKT-sikkerhet.
22. Sikkerhetsutvalget bør følge opp og konkretisere skisse til lovforslag om sikring av sensitiv informasjon og informasjonsinfrastruktur, som er til behandling i Justis- og beredskapsdepartementet.

KRAV TIL RAPPORTERING AV ALVORLIGE IKT-HENDELSER[26]. Mange IKT-hendelser er usynlige, og nasjonalt eksisterer det ikke en god nok oversikt over alvorlige IKT-hendelser på tvers av sektorer. Utenfor sikkerhetslovens virkeområde er det ingen krav om rapportering til NSM. For å kunne utarbeide og forvalte et best mulig IKT-risikobilde på nasjonalt nivå, og ha nasjonal evne til tverrsektoriell respons, er det sentralt at alvorlige IKT-sikkerhetshendelser raskt rapporteres til NSM. Slik vil NSM få mulighet til å se hendelser i sammenheng og koordinere hendelseshåndteringen kosteffektivt.

På bakgrunn av dette anbefaler NSM følgende tiltak:

23. Justis- og beredskapsdepartementet bør vurdere å stille krav til rapportering av alvorlige IKT-hendelser til NSM, for å sikre god nasjonal oversikt.

KRAFTSAMLING OM ÉN OFFENTLIG NASJONAL LEVERANDØR AV HØYGRADERTE IKT-LØSNINGER. Flere aktører i Norge har behov for høygraderte IKT-løsninger. De ulike aktørene har også behov for sikre løsninger for å samhandle. Utvikling av høygraderte informasjonssystemer er ressurskrevende og krever spesiell kompetanse. Kraftsamling rundt én offentlig leverandør vil bidra til å sikre tilstrekkelig volum og nødvendig kompetansenivå, og bidra til effektiv ressursutnyttelse. En leverandør med helhetlig ansvar for høygraderte nettverk vil også forenkle standardisering og derigjennom forenkle tverrsektoriell samhandling.

NSM anbefaler at forsvarssektoren, som har lengst og bredest erfaring i utvikling og drift av høygraderte IKT-systemer, blir gitt i oppdrag å utvikle og forvalte slike løsninger, herunder mobile løsninger i det offentlige. NSMs rolle i dette vil være å gi råd og stille krav, samt bidra til sikkerhetsgodkjenning. Innretningen bør utredes nærmere. Forslaget er ikke til hinder for at en eller flere næringsaktører kan være underleverandører til den offentlige leverandøren.

På bakgrunn av dette anbefaler NSM følgende tiltak:

24. Forsvarsdepartementet og Justis- og beredskapsdepartementet bør ta et initiativ til at forsvarssektoren gis i oppdrag å være den nasjonale leverandøren for å utvikle og forvalte løsninger for høygraderte IKT-behov i det offentlige, inkludert mobile løsninger. Hvordan dette innrettes bør utredes nærmere.

[25] Iht. NIS-direktivet artikkel 14 og 15

[26] Iht. NIS-direktivet artikkel 14

FÆRRE OG STØRRE IKT-MILJØER I OFFENTLIG SEKTOR. Utvikling, forvaltning, drift og anskaffelse av IKT-løsninger for det offentlige utføres i dag av en rekke ulike IKT-miljøer av ulik størrelse og med varierende sikkerhetskompetanse. Misnøye med tidligere leveranser har medført at aktører har valgt egne løsninger for å dekke sine egne behov innen utvikling og forvaltning.

NSM anbefaler at IKT-tjenester samles i færre og større IKT-miljøer i offentlig sektor, gjerne på tvers av etablerte grenser, sektorer, etater og virksomheter. Dette vil gi stordriftsfordeler med mer robuste kompetansemiljøer og kostnadseffektive sikkerhetsløsninger. Et av områdene som bør profesjonaliseres er IKT-anskaffelser og spesielt sikkerhetskrav ved IKT-anskaffelser.

I sentralforvaltningen/departementsfellesskapet bør det kun være ett IKT-miljø som har ansvaret for IKT-løsningene. NSM vurderer at det er flere aktører som kan ivareta en slik rolle for statlig sentralforvaltning. Én innretning vil være å plassere dette hos en av aktørene som gjør dette i statsforvaltningen i dag. En annen mulighet er å restrukturere og etablere et nytt IKT-miljø i en egen etat. En tredje mulighet er å vurdere om forsvarssektorens nye sivile materielletat kan inneha en slik rolle. En fjerde mulighet er at private selskaper kan fylle en slik rolle, gjennom avtaler.

På bakgrunn av dette anbefaler NSM følgende tiltak:

25. Justis- og beredskapsdepartementet og Forsvarsdepartementet bør ta initiativ til å utrede løsninger for færre IKT-miljøer (utviklings- og forvaltningsorganisasjoner) i offentlig sektor.
26. Justis- og beredskapsdepartementet og Forsvarsdepartementet bør ta initiativ til å utrede en løsning hvor ett enkelt IKT-miljø (utviklings- og forvaltningsorganisasjon) gis ansvaret for IKT-løsninger i sentralforvaltningen/departementsfellesskapet.

TILPASNING AV BEGREPER. Mange begreper er i bruk om IKT-sikkerhet. Både IT-sikkerhet, digital sikkerhet, cybersikkerhet og datasikkerhet er i bruk. Mange av begrepene som er i bruk fungerer som synonymer, men kan likevel ha ulike nyanser som kan utfordre samhandling og koordinering dersom man ikke er bevisst på forskjellene. NSM har de siste årene gjennomgående brukt IKT-sikkerhet om informasjonsteknologiske og administrative sikringstiltak. Nasjonalt og internasjonalt ser vi at cybersikkerhet i stadig større grad blir tatt i bruk.

På bakgrunn av dette anbefaler NSM følgende tiltak:

27. IKT-sikkerhet bør erstattes av cybersikkerhet som begrep i politiske og strategiske dokumenter. Dette kan implementeres gjennom revisjon av nasjonal strategi for informasjonssikkerhet.

FOREBYGGING

ETABLERING OG VIDEREUTVIKLING AV ET SIKRET OFFENTLIG NETT (SON). Sikret offentlig nett (SON) er nå under utvikling i et samarbeid mellom JD, FD, politiet og NSM. Nettet gir mulighet for et sikrere «nett i nettet», med tilgang til en redundant høyhastighets internettforbindelse gjennom NSM. Ansvaret for løsningen er imidlertid ikke avklart og det er heller ikke tatt stilling til hvilke aktører SON skal tilbys.

SON vil bidra til å sikre kritisk infrastruktur og gjøre det mulig å beskytte seg bedre mot blant annet tjenestenektangrep fra internett. SON gir mulighet til å koble nettet fra internett og fremdeles kommunisere mellom aktørene. SON kan også benyttes for å stoppe trafikk mot internettadresser som er skadelige eller leverer virus. NSM kan tilby deltagerne i nettet sikkerhetsgraderte sensorer, noe som i betydelig grad styrker den nasjonale deteksjonsevnen. SON vil også bidra til besparelser ved at eksisterende fiberkabler utnyttes bedre og fører til lavere internettkostnader.

På bakgrunn av dette anbefaler NSM følgende tiltak:

28. Justis- og beredskapsdepartementet bør lede utviklingen og etableringen av SON.
29. SON bør utvides til å omfatte flere offentlige aktører og til også å omfatte offentlig forvaltning utenfor Oslo. Dette bør utredes.

[23] Rapport fra Arbeidsgruppe kryptosystemer i Forsvaret. 2013

[24] http: hyper text transfer protocol (en protokoll som muliggjør å overføre og vise nettsider). https er en sikrere og kryptert utgave av http.

[25] PKI: Public key infrastructure (rammeverk for digitale sertifikater som brukes til identifikasjon, signering, og konfidensialitet)

FELLES SIKRE MOBIL- OG IKT-LØSNINGER FOR SENSITIV OG BEGRENSET INFORMASJON. Ulike og fragmenterte IKT-løsninger utfordrer effektivitet og samhandling. NSM ser at felles IKT-løsninger for behandling av informasjon er kritisk for sikker samhandling både innen sektorer, og mellom sektorer. Felles IKT-løsninger vil bidra til å ivareta nødvendig sikkerhet for behandling av både høygradert og lavgradert informasjon, herunder sensitiv informasjon som ikke omfattes av sikkerhetsloven. For å sikre utveksling av informasjon bør det etableres løsninger som kan benyttes på tvers av sektorer. I senere tid har grensene mellom tradisjonelle IKT-plattformer og mobile løsninger i økende grad blitt visket ut. Det er betydelige krav fra brukere om å kunne anvende mobile løsninger som en forlengelse av virksomhetens informasjonssystemer. Felles kravstilling, utvikling og forvaltning vil gi betydelige sikkerhetsmessige og samhandlingsmessige gevinster.

Det er i tillegg viktig å sikre et tydelig ansvar for de ulike løsningene.

På bakgrunn av dette anbefaler NSM følgende tiltak:

30. Forsvarsdepartementet og Justis- og beredskapsdepartementet bør ta initiativ til at det etableres felles IKT-systemer som håndterer sensitiv og BEGRENSET informasjon i ett.
31. Forsvarsdepartementet og Justis- og beredskapsdepartementet bør ta initiativ til at det etableres nye mobile løsninger for sensitiv og BEGRENSET informasjon.
32. Forsvarsdepartementet og Justis- og beredskapsdepartementet bør gi NSM i oppdrag å utrede sikkerhetsbehov og sikkerhetsmessige løsninger for nasjonale skytjenester for sensitiv og sikkerhetsgradert informasjon.

ETABLERING AV KRAV OM BRUK AV KRYPTO. Det er i dag varierende bevissthet om behovet for kryptering av informasjon. Kryptografiske mekanismer har meget stor betydning for IKT-sikkerhet. Kryptoløsninger er antakelig det mest effektive sikkerhetstiltaket for å ivareta konfidensialitet. Løsningene for høye graderingsnivåer er svært effektive. Bruk av slike reduserer vesentlig muligheten for avlytting og overvåkning. Kryptoløsninger for sensitiv og BEGRENSET informasjon vil sterkt bidra til å redusere risiko for at informasjon utilsiktet skal komme på avveie. NSM tar utgangspunkt i at dette behovet kan dekkes av åpne standarder og sertifiserte, kommersielt tilgjengelige produkter.

NSM ser også et behov for en gjennomgående utvikling av nasjonal kryptokompetanse. Det er behov for økt kompetanse innen akademia, industri og offentlig sektor. I en egen rapport i regi av Forsvarsdepartementet beskrives dette behovet nærmere[27].

For å sikre nasjonal suverenitet over nasjonal gradert informasjon, er det nødvendig med en kontinuerlig utvikling av løsninger for kryptografi. Gjennom forsvarssektorens investeringsportefølje samarbeider NSM og Forsvaret om å utvikle nye, digitaliserte løsninger for kryptosikkerhet. Disse initiativene skal støtte behovene for høygraderte kryptoløsninger i forsvarssektoren og i sivil sektor.

Det er et stort potensial for å øke sikkerheten i tjenester som skal behandle sensitive data, gjennom kommersielle løsninger som sikker http (https)[28], sikker epost og PKI[29].

På bakgrunn av dette anbefaler NSM følgende tiltak:

33. Justis- og beredskapsdepartementet og Forsvarsdepartementet bør ta initiativ til at det stilles krav til bruk av godkjente krypteringsløsninger for beskyttelse av sensitiv informasjon. NSM bør gis et slikt oppdrag.
34. Justis- og beredskapsdepartementet og Forsvarsdepartementet bør gi NSM i oppdrag å utvikle krav til programvarebaserte krypteringsløsninger som kan godkjennes for beskyttelse av både sensitiv og BEGRENSET informasjon.
35. Alle statlige og kommunale nettsteder bør innføre krypteringsløsninger for bedre sikring av offentlige nettsteder. Dette vil øke sikkerheten i all kommunikasjon mellom innbyggerne og offentlige nettsteder.
36. Forsvarsdepartementet og Justis- og beredskapsdepartementet bør videreutvikle en nasjonal kryptopolitikk for å sikre nødvendig nasjo-

[27] Rapport fra Arbeidsgruppe kryptosystemer i Forsvaret. 2013

[28] http: hyper text transfer protocol (en protokoll som muliggjør å overføre og vise nettsider). https er en sikrere og kryptert utgave av http.

[29] PKI: Public key infrastructure (rammeverk for digitale sertifikater som brukes til identifikasjon, signering, og konfidensialitet)

nal kryptokompetanse og utvikling av kryptoutstyr for høygradert informasjon. En revisjon og videreutvikling av dagens kryptopolitikk er nødvendig for å stimulere til innovasjon og produktutvikling.

37. Det bør initieres et prosjekt for å få frem en ny generasjon av kryptoløsninger innen 2020.

ETABLERING AV NSM SOM NASJONAL SERTIFIKATUTSTEDER. Økt digitalisering av samfunnet vil stille stadig strengere krav til sikker identifisering av brukerne av systemene. IDeALT[30]-programmet er et eksempel på et initiativ som adresserer identifikasjonsutfordringen.

For eksempel vil sikker identifisering av individer kreve digitale sertifikater som er generert på bakgrunn av data fra en tiltrodd tjeneste. NSM er i dag en slik nasjonal sertifikatutsteder for blant annet Forsvarets bruk av digitale sertifikater, hvor NSM gjør Forsvaret i stand til å generere en sikker identifikasjon for den enkelte brukeren og brukerens tilgangsrettigheter i datasystemene.

På bakgrunn av dette anbefaler NSM følgende tiltak:

38. Forsvarsdepartementet og Justis- og beredskapsdepartementet bør styrke og videreutvikle NSM som nasjonal sertifikatutsteder for sikker identifikasjon av individer og deres bruk av IKT-tjenester i samfunnet. NSM kan i en slik rolle kvalifisere kommersielle leverandører gjennom å utstede et sikkert sertifikat for deres leveranse av tiltrodde tjenester.

ØKT BRUK AV INNTRENGNINGSTESTING. Mange norske virksomheter har store, digitale sårbarheter, ofte i kombinasjon med manglende fysisk sikkerhet. Sårbarhetene gjør det i mange tilfeller enkelt å gjøre digitale innbrudd i datasystemer, stjele informasjon eller ødelegge systemer. Inntrengningstesting er et svært effektivt virkemiddel til å få kunnskap om den faktiske sårbarheten i IKT-systemer, slik at sårbarhetsreduserende tiltak kan målrettes bedre. NSM har evne til å gjennomføre inntrengningstesting, og har gjennom dette avdekket en rekke alvorlige sårbarheter innenfor ulike samfunnssektorer.

Det er få krav til inntrengningstesting, og virkemidlet brukes i for liten grad. Det bør stilles krav til inntrengningstesting av systemer som er kritiske eller som behandler sensitiv informasjon, og det er behov for å utvikle en nasjonal evne i forvaltningen og næringslivet til å foreta slik testing. Det bør utvikles en akkrediteringsordning for virksomheter som kan gjennomføre inntrengningstesting. Formålet er å sikre at disse virksomhetene har nødvendig kompetanse til å gjennomføre slike tester på en forsvarlig måte, og at personvernhensyn blir ivaretatt i gjennomføringen. NSM vil se på muligheten for å gjennomføre en pilotordning. En permanent akkrediteringsordning bør forvaltes av NSM.

NSM kan teste systemer som behandler sikkerhetsgradert informasjon, men dette krever samtykke fra virksomheten som eier slike systemer. I enkelte tilfeller ser NSM behovet for å foreta slike tester uten samtykke. NSM bør gis en slik mulighet.

På bakgrunn av dette anbefaler NSM følgende tiltak:

39. Eiere av kritisk infrastruktur og systemer som behandler sensitiv informasjon bør jevnlig gjennomføre inntrengningstesting av sine IKT-systemer som et sårbarhetsreduserende tiltak.
40. Forsvarsdepartementet og Justis- og beredskapsdepartementet bør ta initiativ til at det stilles krav til inntrengingstesting av IKT-systemer som behandler sensitiv informasjon. Hvordan dette kan innrettes bør utredes nærmere, herunder innretningen av en permanent akkrediteringsordning. Departementene bør gi NSM et slikt utredningsoppdrag.
41. Sikkerhetsutvalget bør vurdere å gi NSM utvidet hjemmel til inntrengingstesting etter sikkerhetsloven til å omfatte også nasjonal kritisk IKT-infrastruktur, og oppdraget bør utvides til å omfatte testing av logiske, tekniske, administrative, menneskelige og fysiske sårbarheter, da disse er vevet tett sammen. NSM bør gis hjemmel til å gjennomføre inntrengningstesting uten forutgående samtykke fra virksomheten.

[30] IDeALT-programmet har ansvar for ID-utstedelse som pass og ID-kort, ID-kontroll på grensen og på territoriet, og teknisk og taktisk ID-kriminalitet.

HENDELSESHÅNDTERING

STYRKING OG VIDEREUTVIKLING AV DEN NASJONALE CERT-FUNKSJONEN (NSM NORCERT)[31]. Med den økte avhengigheten Forsvaret og eiere av annen kritisk IKT-infrastruktur får til internett som bærer av informasjon, vil NSM NorCERT ha behov for en betydelig kapasitetsøkning for å kunne bistå eiere av kritisk IKT-infrastruktur i årene fremover. NSM NorCERT har i dag rollen som den nasjonale CERT-funksjonen. Det innebærer at NSM NorCERT er nasjonalt IKT-responsmiljø, og skal koordinere håndteringen av alvorlige IKT-hendelser mot samfunnskritisk infrastruktur og informasjon. Det innebærer også rollen som nasjonal evne for å detektere hendelser, koordinere og bistå i hendelseshåndteringen, foreta tekniske analyser, dele informasjon og gi råd. I tillegg gir NSM NorCERT et særlig viktig underlag for å utarbeide et nasjonalt IKT-risikobilde. Denne kombinasjonen av egenevne til å detektere og koordinere håndteringen av hendelser og dataangrep er unik i europeisk sammenheng og danner et godt grunnlag for en videreutvikling av NSM NorCERT. Utfordringene har endret seg betydelig de siste årene.

NSM har i løpet av 2015 gjennomført en større strategiprosess for bedre å være i stand til å skalere i tråd med økningen i antallet IKT-hendelser. Den nye modellen, som innebærer at NSM NorCERT skal løse mer av det nasjonale oppdraget gjennom ulike sektorvise responsmiljøer, er under etablering. Modellen vil til en viss grad møte økningen i antall dataangrep, men det er fortsatt et tydelig behov for en styrking av kapasitet.

Satsingsområder vil være aktiv informasjonsformidling av trusselbildet, formidling av anonymisert teknisk informasjon om sikkerhetsrelaterte hendelser, og gi råd om hvilke tiltak som bør benyttes for å redusere risikoen for et fremtidig angrep. Det vil også være behov kontinuerlig videreutvikling av metoder og verktøy for å detektere stadig mer kompetente trusselaktører.

NSM ser behov for å ta initiativ til å etablere et felles bygg, et nasjonalt cybersikkerhetssenter[32], som en del av NSMs ansvar for koordinering av IKT-hendelser. Hensikten er å legge til rette for samhandlingsarenaer for å koordinere og gi støtte til hendelseshåndtering ved dataangrep mot norske interesser. En samlokalisering gir en optimalisering av samhandling og deling av informasjon og ressurser på tvers av sektorene. Dette forenkler koordineringsoppgavene og bidrar samtidig til at samfunnets totale evne til å motstå dataangrep øker. Uavhengig av dette må rutinene for informasjonsdeling mellom aktørene optimaliseres, dog slik at de ivaretar andre hensyn som forholdet til nasjonale og internasjonale samarbeidspartnere, både myndigheter og næringsliv.

Det bør legges til rette for at sektorvise koordineringsmiljøer kan samles i senteret, i tillegg til samarbeidende myndigheter som øvrige EOS-tjenester og politiet. Det bør også legges opp til tilstedeværelse for sentrale infrastruktureiere (som for eksempel Forsvaret og Telenor). Det er et tydelig uttrykt behov hos alle at det er nødvendig å legge fysisk til rette for dette, både i det daglige og i forbindelse med hendelser.

Tiltaket kan gjennomføres alene, men bør primært inngå som en del av styrkingen og videreutviklingen av den overordnede koordinering av sikkerhetsarbeidet gjennom tiltaket om samlokalisering av NSM, jf. tiltak 9 ovenfor.

På bakgrunn av dette anbefaler NSM følgende tiltak:

42. Forsvarsdepartementet og Justis- og beredskapsdepartementet bør styrke den nasjonale CERT-funksjonen, NSM NorCERT, for ytterligere å kunne bedre evnen til bearbeiding og analyse av hendelsesdata, styrke samarbeidet med næringslivet, få økt evne til bistand til håndtering av IKT-hendelser, samt kontinuerlig videreutvikle av metoder og verktøy.
43. Forsvarsdepartementet og Justis- og beredskapsdepartementet bør legge til rette for samarbeid mellom de sektorvise koordineringsmiljøene og andre ved å gi NSM oppdrag om å etablere et nasjonalt cybersikkerhetssenter[33] hos NSM. Senteret omhandles også under anbefaling om samlokalisering av NSM.
44. Forsvarsdepartementet og Justis- og beredskapsdepartementet bør gi NSM i oppdrag å utvikle en portal på internett som sørger for

[31] Iht. NIS-direktivet - artikkel 7

[32] Begrepet «cybersikkerhetssenter» i stedet for «IKT-sikkerhetssenter» blir her brukt for å være sammenlignbart med andre lands oppbygning av slike sentre, for eksempel Nederland og Finland.

effektiv og rask informasjonsdeling under hendelser mellom ulike responsmiljøer, andre offentlige myndigheter, i næringslivet, og mellom myndigheter og næringslivet.

STYRKING OG VIDEREUTVIKLING AV DEN NASJONALE DETEKSJONSEVNEN. Nasjonal sikkerhetsmyndighet drifter i dag Varslingssystem for digital infrastruktur (VDI). Sensorsystemet detekterer og varsler om dataangrep mot kritisk infrastruktur og viktige virksomheter i Norge. Systemet er basert på frivillig deltakelse og delfinansiering av private aktører. Forløperen ble allerede etablert i 1999 og VDI-systemet har, etter å ha gjennomgått flere oppdateringer underveis, vært i drift siden.

VDI er i dag et av de viktigste verktøyene norske myndigheter har til å detektere og stoppe cyberangrep, herunder spionasje fra fremmede statlige aktører, mot norsk infrastruktur. Dette bidro til at NSM NorCERT i 2014 håndterte 5069 hendelser og avdekket 88 alvorlige angrep mot norske bedrifter og myndigheter. Tilliten som i dag er bygget opp mellom norske myndigheter og norsk næringsliv gjennom VDI over ti år er unik i europeisk sammenheng. Styrking og videreutvikling av løsningen vil gi norske myndigheter mulighet for å bygge opp en meget god deteksjonsevne på nasjonalt nivå. Tilknytning av flere aktører til SON, som beskrevet tidligere, vil gi ytterligere deteksjonsevne på nasjonalt nivå.

I dag er deltakelse i VDI delfinansiert av deltakerne. Hver deltager dekker kostnaden for egen sensor, mens NSM finansierer sentral infrastruktur samt utvikling og forvaltning. Situasjonsbildet på internett er dermed avhengig av om viktige selskaper ønsker å være med i samarbeidet eller ikke. VDI bør i stedet for dagens ordning være basert på en risikovurdering, og behovet for å se dataangrep på tvers av sektorer, i stedet for i hvor stor grad systemet kan finansieres av private aktører. Dagens sensor-nettverk (VDI) bør utvikles til å være fullfinansiert av staten. Antallet sensorer bør økes betydelig, alternativt må større sensorer plasseres sentralt hos for eksempel internettleverandører, for å gi en betydelig bedre deteksjonsevne ved samfunnsviktige funksjoner.

På bakgrunn av dette anbefaler NSM følgende tiltak:

45. Forsvarsdepartementet og Justis- og beredskapsdepartementet bør tildele NSM ressurser for å styrke og videreutvikle VDI-løsningen til et robust sensornettverk for å sikre en best mulig nasjonal deteksjonsevne.
46. Forsvarsdepartementet og Justis- og beredskapsdepartementet bør ta initiativ til at deltakelse i VDI-samarbeidet fullfinansieres av staten. Deltakelse bør gjøres obligatorisk for virksomheter med samfunnsviktig IKT-infrastruktur og samfunnsviktige funksjoner, etter en risikovurdering. En slik deltakelse må hjemles i lov.

ETABLERE OG STYRKE SEKTORVISE RESPONSMILJØER. NSM har over tid anbefalt at det etableres sektorvise responsmiljøer. Hensikten er å analysere og dele informasjon om hendelser i egen sektor, mellom andre sektorer, og med NSM på nasjonalt nivå. For NSM er det viktig å ha slike miljøer som kontaktpunkt i den enkelte sektor. Sektorvise responsmiljøer er etablert i Forsvaret (ved Cyberforsvaret/Avdeling for beskyttelse av kritisk infrastruktur - BKI), helsesektoren (HelseCSIRT), finanssektoren (FinansCERT), kraftsektoren (KraftCERT), og universitets- og høyskolesektoren (UNINETT CERT). NSM mener det er viktig å styrke og videreutvikle disse, samtidig som det etableres tilsvarende miljøer i andre sektorer. Sektorenes ulikhet tilsier at løsningene kan være noe forskjellige. NSM har en viktig rolle med å binde disse miljøene sammen, og koordinere aktiviteten. De sektorvise miljøene må ha evne og kompetanse til å dele informasjon med virksomheter innenfor sektoren, mellom sektorer og med NSM NorCERT. Miljøene må også ha evne og kompetanse til å analysere informasjon om hendelser i sektoren. NSM må spille en rolle for å bidra til kompetansen i de sektorvise miljøene og gjøre dem i stand til å ivareta sin rolle på det operative nivået. NSM må håndtere grensesnittet mellom strategisk og operativt nivå og sørger for tilstrekkelig koordinering.

[33] Begrepet «cybersikkerhetssenter» i stedet for «IKT-sikkerhetssenter» blir her brukt for å være sammenlignbart med andre lands oppbygning av slike sentre, for eksempel Nederland og Finland.

På bakgrunn av dette anbefaler NSM følgende tiltak:

47. Justis- og beredskapsdepartementet og Forsvarsdepartementet bør oppfordre til at sektorene etablerer, videreutvikler og styrker responsmiljøene i sektorene.
48. Justis- og beredskapsdepartementet og Forsvarsdepartementet bør gi NSM i oppdrag å koordinere nasjonalt og til sektorene samt bidra til kompetanseoverføring til disse miljøene.

KONTROLL

STYRKE TILSYNET MED IKT-SIKKERHET. Tilsyn med IKT-sikkerhet i norske virksomheter er spredt på en rekke tilsynsorganer. De fleste av disse mangler kompetanse til å føre tilsyn med den tekniske siden av IKT-sikkerheten innen sitt ansvarsområde.

Ettersom NSM er det nasjonale fagmiljøet for IKT-sikkerhet, er det hensiktsmessig å utnytte potensialet som ligger her i stedet for at de enkelte sektortilsyn skal bygge opp egen kompetanse innen IKT-sikkerhet.

På bakgrunn av dette anbefaler NSM følgende tiltak:

49. Justis- og beredskapsdepartementet bør ta initiativ til at ulike tilsyn, herunder i sektorene, sørger for at det blir ført tilsyn med tekniske IKT-sikkerhetstiltak på eget ansvarsområde.
50. Justis- og beredskapsdepartementet bør tildele NSM ressurser for å øke kapasiteten til å føre tilsyn med tekniske IKT-sikkerhetstiltak. Herunder å etablere en evne for å kunne gi støtte til tilsyn til andre tilsyn for å kunne realisere tiltak 49 på en kosteffektiv måte.

17. Tiltak innen personellsikkerhet

KOMPETANSE OG KVALITET I FAGMYNDIGHETEN FOR PERSONELLSIKKERHET. Sikkerhetsklarering av personer som skal håndtere sensitiv informasjon er utfordrende.

Det er et betydelig behov for å styrke evnen i hele personellsikkerhetskjeden[34]. Spesielt viktig er økt spesialisering og akademisk kompetanse innen psykologfaglige vurderinger, lojalitetsforhold, tilknytningsutfordringer, samtale- og intervjuteknikk, og forsvar mot sosial manipulasjon. Det bør i tillegg bygges kompetanse innen risiko- og trusselanalyse relatert til personellsikkerhetsrisiko. Behovet har økt i takt med internasjonaliseringen og mer kompliserte vurderingstemaer.

Den gjeldende desentraliserte modellen med svært mange små klareringsmyndigheter er ineffektiv og gir ikke nødvendig kompetanse til likebehandling av klareringssaker. Forsvarsdepartementet har i forslag til endringer i sikkerhetsloven nylig foreslått at antall klareringsmyndigheter reduseres til en sivil og en militær klareringsmyndighet, i tillegg til at EOS-tjenestene sikkerhetsklarerer egne ansatte. Dersom endringen blir vedtatt, vil det være et meget viktig tiltak for å skape klareringsmyndigheter med økt effektivitet, kompetanse og kvalitet i saksbehandlingen.

Der det er mulig med felles kapasiteter og behov for spesialisert kompetanse i ulike deler av personellsikkerhetskjeden, bør disse samles hos NSM i egenskap av fagmyndighet. For at hele personellsikkerhetskjeden skal få tilgang på god nok kompetanse og verktøy, må imidlertid fagmyndighetsoppgavene styrkes[35]. I tillegg er det, for å heve kvaliteten, behov for økt tilsyn med området.

På bakgrunn av dette anbefaler NSM følgende tiltak:

51. Forsvarsdepartementet bør legge til rette for at klareringsmyndighetsstrukturen endres i tråd med foreslått endring i sikkerhetsloven som er til behandling.
52. Forsvarsdepartementet bør legge til rette for at NSMs fag- og tilsynsmyndighet innen personellsikkerhet styrkes. Styrkingen muliggjøres ved at ressursene i NSM som frigjøres etter endret klareringsmyndighetsstruktur innrettes mot oppgaver innen fag- og tilsynsmyndighet.

[34] Personellsikkerhetskjeden består av den nasjonale fagmyndigheten og personkontrollfunksjonen i NSM – klareringsmyndighetene for sektorene – autorisasjonsmyndighetene og utøvelse av daglig sikkerhetsmessig ledelse i virksomhetene.

EFFEKTIVISERING AV KLARERINGSPROSESSEN. Saksbehandlingstiden i klareringssaker er for lang. Det fører til store samfunnsøkonomiske tap ved at personell ikke kan benyttes rettidig av arbeids- eller oppdragsgivere, i tillegg til personlig belastning for personellet det gjelder. Sikkerhetsloven gir hjemmel for å innhente opplysninger fra en lang rekke registre, men tidkrevende manuelle prosesser er en utfordring både for den sentrale personkontrollen og de enkelte klareringsmyndigheter.

Et automatisert system for innhenting av opplysninger fra kilderegistre i forbindelse med klarering, og regelmessig kildekontroll av personell med gyldig klarering, vil øke effektiviteten og redusere risikoen for at sårbarheter ikke blir håndtert. Samtidig vil det redusere ressursbehovet i forbindelse med klarering og reklarering. I tillegg vil et automatisert system for vurdering i saker uten ufordelaktige personkontrollopplysninger gjøre at slike saker kan behandles meget hurtig.

Det tar ofte lang tid å innhente opplysninger fra kilderegistre fra andre land, og tiden varierer betydelig mellom ulike land. NSM er kjent med at NATO har etablert ordninger som imøtekommer sine behov, men for rent nasjonale behov er situasjonen utilfredsstillende.

På bakgrunn av dette anbefaler NSM følgende tiltak:

53. Forsvarsdepartementet bør fremme et forslag til lovfesting av at NSM som hovedregel kan kreve automatisert innhenting fra kilderegistre, herunder regelmessig kildekontroll i klareringens gyldighetstid.
54. Forsvarsdepartementet bør styrke NSMs evne til å effektivisere klareringsprosessen i form av et materiellprosjekt finansiert av Forsvarsdepartementet. Prosjektet bør blant annet omfatte elektronisk og automatisert kildeinnhenting og vurdering, innføring av nye kilder, videreutvikling av funksjonaliteten i saksbehandlerverktøyet og overgang til elektroniske varsler og bevis om klarering.

Forsvarsdepartementet bør legge til rette for at NSMs kapasitet til å etablere og videreutvikle bilaterale kontaktnett styrkes. Vi bør få andre land til å forplikte seg til en mer effektiv prosess for å innhente opplysninger fra deres kildregistre.

NY TVERRSEKTORIELL ORDNING FOR BAKGRUNNSKONTROLL. De ulike ordningene og hjemlene for bakgrunnskontroll (utover sikkerhetsklarering etter sikkerhetsloven) er fragmenterte, dekker ikke alle legitime behov, og har få rettigheter for den som kontrolleres. Der bakgrunnskontroll er hjemlet, er det som oftest avgrenset til vandelskontroll etter politiregisterloven, som for mange virksomheter ikke er tilstrekkelig.

Etablering av en ny, tverrsektoriell hjemmel for bakgrunnskontroll bør utredes. Kontrollen bør gjelde personell som kan bli utsatt for trusler ved at de får tilgang til samfunnsviktig informasjon, infrastruktur eller objekt, eller tilgang til farlig materiell eller farlige stoffer. Ordningen bør ta sikte på å innhente færre opplysninger enn i klareringssaker etter sikkerhetsloven, men flere opplysninger enn ved vandelskontroll etter politiregisterloven. Flere sektorer har signalisert overfor NSM at de har behov for dette. Lignende ordninger er innført i blant annet USA og Storbritannia, der kontrollen utføres på sentralt nivå av egne forvaltningsorganer. Hjemmelen kan tilpasses det reelle behovet for slik kontroll og dermed ikke være mer inngripende enn nødvendig. Bakgrunnskontrollen kan benyttes tverrsektorielt og ivareta hensynet til likebehandling og den enkeltes rettssikkerhet. Den kan gjennomføres på en måte som er effektiv og lett å kontrollere.

En annen viktig gevinst ved å innføre en hjemmel for slik bakgrunnskontroll er å få redusert antallet klareringer etter sikkerhetsloven.

På bakgrunn av dette anbefaler NSM følgende tiltak:

55. Justis- og beredskapsdepartementet bør få utredet en ny tverrsektoriell hjemmel og ordning for bakgrunnskontroll av personell med sikte på å ivareta legitime behov som vandelsattest ikke dekker eller alene er utilstrekkelig for.

REDUSERE RISIKOEN FOR INNSIDERE OG UTRO TJENERE. Ny teknologi og en ny sikkerhetspolitisk

[35] Med fagmyndighetsoppgaver menes her rådgivning, veiledning, undervisning og utvikling innen fagområdet.

situasjon øker behovet for å motvirke innsidetrusselen i årene fremover. Slik oppfølging bør bestå av en kombinasjon av tiltak innen ulike fagområder, herunder linjeledelse, personellsikkerhet og IKT-sikkerhet internt i virksomheter. I tillegg er det behov for at PST kan følge opp virksomheter som benytter sikkerhetsklarert personell med tilknytning til stater som utgjør en høy etterretningstrussel mot Norge og norske interesser.

NSM anbefaler at det gjennomføres et utredningsoppdrag om hvordan innsidetrusselen kan motvirkes både innenfor eksisterende lovverk og ved eventuelle lovendringer eller andre virkemidler. Videre bør det gjøres en endring av formålsbegrensningen i sikkerhetsloven § 20 sjette ledd, slik at den ikke er til hinder for at NSM kan gi informasjon fra klareringssaker til PST som er relevant for at PST skal kunne ivareta sitt ansvar for å forebygge og motvirke trusler mot rikets sikkerhet eller andre grunnleggende nasjonale interesser.

På bakgrunn av dette anbefaler NSM følgende tiltak:

56. Sikkerhetsutvalget bør utrede virksomheters rettslige rammer og andre virkemidler for å motvirke innsidetrusselen.
57. Forsvarsdepartementet bør fremme forslag om endring av sikkerhetsloven § 20 sjette ledd, slik at NSM kan gi informasjon fra klareringssaker til PST som er relevant for at PST skal kunne ivareta sitt ansvar for å forebygge og motvirke trusler mot rikets sikkerhet eller andre grunnleggende nasjonale interesser.

SIKKER IDENTIFIKASJON I PERSONKONTROLLEN.

Sikker identifisering av personell er viktig i hele personellsikkerhetskjeden. Det er i dag svakheter i denne kontrollen. Slike sikrere kontrollmekanismer må implementeres i samarbeid med andre relevante virksomheter. Hvordan dette kan gjennomføres bør utredes nærmere i samarbeid med Nasjonalt ID-senter.

På bakgrunn av dette anbefaler NSM følgende tiltak:

58. Forsvarsdepartementet bør gi NSM i oppdrag å utrede hvordan kontrollmekanismene for identifikasjon av personell i hele personellsikkerhetskjeden kan bli sikrere.

18. Tiltak innen fysisk sikkerhet

GRUNNLAG FOR PRIORITERING AV STATLIGE SIKRINGSSTYRKER.

Flere ulike ordninger for klassifisering av ulike typer objekter og infrastruktur vanskeliggjør i dag en prioritering av knappe statlige sikringsstyrker som er felles for sektorene. Eksempler er sikringsstyrker fra politiet og Forsvaret. Flere ordninger er i praksis konkurrenter om de samme fellesressursene, uten at det fremgår hvilke som skal prioriteres først.

På bakgrunn av dette anbefaler NSM følgende tiltak:

59. Det bør sikres at objekter klassifisert etter sikkerhetsloven gis prioritet på statlige sikringsstyrker, fremfor objekter utvalgt kun etter sektorregelverk. Om nødvendig, bør dette fastsettes gjennom Kgl.res. Dette bør vurderes av Sikkerhetsutvalget.

RÅD OG VEILEDNING OM FYSISK SIKKERHET.

Det er behov for råd og veiledning om fysisk sikkerhet til virksomheter omfattet av sikkerhetsloven, slik at disse kan oppfylle kravene i loven. NSM har en veiledningsplikt etter sikkerhetsloven og forvaltningsloven om hvordan sikkerhetslovens krav er å forstå. Det er også behov for å heve kompetansen hos virksomheter som skal kjøpe tjenester innen fysisk sikkerhet.

Etterspørselen etter råd og veiledning er større enn det NSM kan imøtekomme. Fagmiljøet er lite robust og bør styrkes. Samtidig er det også andre miljøer med kompetanse og kapasitet innen fysisk

sikring, som PST, Forsvarsbygg og Statsbygg. Det kan være muligheter for bedre ressursutnyttelse, men også bedre rollefordeling, mellom disse.

På bakgrunn av dette anbefaler NSM følgende tiltak:

60. Forsvarsdepartementet bør styrke NSM for å øke evnen til å gi råd og veiledning innen fysisk sikkerhet etter sikkerhetsloven.
61. Forsvarsdepartementet, Justis- og beredskapsdepartementet og Kommunal- og moderniseringsdepartementet bør utrede hvordan roller, ansvar og evner innen fysisk sikkerhet bør være for relevante fagmiljøer på området. I denne sammenheng bør det vurderes om det bør etableres et felles rådgivingssenter for å samle og utnytte samfunnets ressurser på best mulig måte.

SIKKERHETSDESIGN I BYPLANLEGGING OG BYGGEPROSJEKTER. Det er behov for å øke bevisstheten og kunnskapen om god sikkerhetsdesign i det offentlige rom og for bygg. Også næringslivets aktører i prosessene er en sentral målgruppe for å oppnå dette. Et kompetanseprogram om sikkerhetsdesign med ulike incentiver kan gi god effekt. Programmet kan gjerne sees som en forlengelse av gjeldende felles veileder i sikrings- og beredskapstiltak mot terrorhandlinger.

På bakgrunn av dette anbefaler NSM følgende tiltak:

62. Justis- og beredskapsdepartementet bør gi NSM, Politiets sikkerhetstjeneste og Politidirektoratet i oppdrag å utarbeide et kompetanseprogram om sikkerhetsdesign for aktørene i byplanlegging og byggeprosjekter.

19. Tiltak innen samarbeid med næringslivet

AKKREDITERING AV VIRKSOMHETER. For mange er det i dag vanskelig å velge sikre løsninger, produkter og tjenester, og kunnskapen om slike er begrenset. NSM vil etablere en ordning der en tredjepart kan akkrediteres for å utføre oppgaver eller oppdrag innen enkelte av NSMs ansvarsområder. Med tredjepart menes private bedrifter eller offentlige forvaltningsorganer. En slik ordning vil organiseres og ledes av NSM. Dette muliggjør en effektiv og strukturert utnyttelse av eksisterende kompetanse som en tredjepart besitter, og anses som en kosteffektiv måte å heve det generelle sikkerhetsnivået i samfunnet på.

NSM opprettholder sitt ansvar, evne og nødvendig kapasitet på området.

Tredjepart vil ha en supplerende rolle til NSM, og dette vil gi økt totalkapasitet til å håndtere sikkerhetsutfordringer i samfunnet. Bedrifter og institusjoner i samfunnet for øvrig vil samtidig få kvalitetssikrede aktører, i tillegg til NSM, som de kan benytte ved behov.

NSM har igangsatt et pilotprosjekt for å etablere akkreditering av tredjeparter på enkelte områder. NSM samarbeider med Norsk Akkreditering om utviklingen av en slik ordning. Å etablere og forvalte en slik ordning i full skala på flere områder vil kreve ytterligere kapasitet. En slik styrking vil gi en betydelig effekt på totalkapasiteten innen sikkerhetstjenester i samfunnet.

På bakgrunn av dette anbefaler NSM følgende tiltak:

63. Forsvarsdepartmentet bør styrke NSM for å etablere og forvalte en ordning for akkreditering av virksomheter for utøvelse av sikkerhetstjenester.

ANSVAR FOR OG FORENKLING AV LEVERANDØRKLARERINGER. Det er et stort behov for å styrke fagmyndighetsrollen i NSM, for å sikre at prosessene rundt sikkerhetsgraderte anskaffelser er gode og sikre nok. NSM bruker i dag mesteparten av sine ressurser på området til å fatte vedtak om leverandørklareringer. Sikkerhetsloven åpner ikke for at andre enn NSM i dag kan fatte vedtak om leverandørklarering. Både nåværende fagmiljøer for sikkerhetsgraderte anskaffelser i Forsvaret og Forsvarsbygg, samt de foreslått opprettede klareringsmyndighetene på militær og sivil side, kan være aktuelle med tanke på utøvelse av myndighet til å gi leverandørklareringer. Ressursene i NSM som frigjøres ved en slik omlegging bør refokuseres til kontroll og utvikling innen området, herunder utvikle regelverk og veiledninger.

På bakgrunn av dette anbefaler NSM følgende tiltak:

64. Forsvarsdepartementet bør fremme et forslag om at sikkerhetsloven endres slik at Kongen kan utpeke klareringsmyndigheter og klageinstans for saker om leverandørklarering og andre myndighetsavgjørelser på området.

TIDLIG INFORMASJON OM FREMTIDIGE MARKEDSMULIGHETER. Næringslivet vil være en viktig aktør i å bedre sikkerhetstilstanden ved å utvikle og produsere nye varer og tjenester innenfor sikkerhet. For at leverandører skal kunne ta risiko i utvikling av fremtidige produkter og tjenester trenger de tidlig informasjon om hva som er fremtidige behov hos det offentlige som kunde. Slik informasjon bidrar til å skape en høyere grad av forutsigbarhet i markedet.

På bakgrunn av dette anbefaler NSM følgende tiltak:

65. Forsvarsdepartementet og Justis- og beredskapsdepartementet bør etablere eller videreutvikle allerede eksisterende arenaer for informasjonsutveksling mellom det offentlige som kunde og leverandører.

FLEKSIBEL BRUK AV DET OFFENTLIGE ANSKAFFELSESREGELVERKET. Forskrift om offentlige anskaffelser (FOA) gir et begrenset handlingsrom når det gjelder dialog med leverandører. Anbud er den grunnleggende anskaffelsesmetoden i FOA. Dette innebærer at det er begrenset mulighet til dialog mellom leverandører og innkjøpere i anskaffelsesprosessen. Mangelen på en slik dialog kan begrense evnen til å utvikle innovative løsninger. For sikkerhetsrelaterte anskaffelser er det et alternativ å benytte forskrift om sikkerhetsanskaffelser (FOSA). Den grunnleggende anskaffelsesmetoden i FOSA er kjøp med forhandlinger som er en mer fleksibel metode enn anbud. Alle offentlige oppdragsgivere kan bruke dette regelverket. Etter hva NSM kjenner til er dette regelverket i begrenset grad tatt i bruk. Økt bruk av regelverket kan bidra til økt innovasjon av sikkerhetsprodukter.

På bakgrunn av dette anbefaler NSM følgende tiltak:

66. Forsvarsdepartementet bør som regelverksforvalter forsterke sitt informasjonsarbeid om forskrift om sikkerhetsanskaffelser, for å bidra til hensiktsmessig bruk av det.

20. Tiltak innen kompetanse

STIMULERE TIL ØKT SATSING PÅ IKT-SIKKERHET PÅ HØGSKOLER OG UNIVERSITETER. Det er mangel på personer med relevant kunnskap i IKT-sikkerhet innenfor kritiske samfunnsfunksjoner. Norske høgskoler og universiteter bør satse mer på slik utdanning i årene fremover.

På bakgrunn av dette anbefaler NSM følgende tiltak:

67. Justis- og beredskapsdepartementet bør ta initiativ overfor Kunnskapsdepartementet for å vurdere hvordan det kan stimuleres til en sterkere satsning på IKT-sikkerhet som fag. Vurderingen bør blant annet se på mulighetene for etablering av egne bachelor- og mastergrader i IKT-sikkerhet, og muligheten for å gjøre IKT-sikkerhet til et obligatorisk fag eller kurs for alle som utdanner seg innenfor IT-området.

68. Forsvarsdepartementet bør legge til rette for at kapasiteten økes slik at det kan opprettes sivile plasser ved Forsvarets ingeniørhøyskole.

INNFØRE IKT-SIKKERHET SOM FAG I LÆRERUTDANNINGEN. Nettvett står i dag som kompetansemål i barneskolen. Men opplæringen i IKT-sikkerhet i grunnskolen og videregående skole er ofte tilfeldig, basert på hva lærere kan fra før av om temaet[36].

På bakgrunn av dette anbefaler NSM følgende tiltak:

69. Justis- og beredskapsdepartementet bør ta initiativ overfor Kunnskapsdepartementet for å vurdere hvordan IKT-sikkerhet kan innarbeides i lærerutdanningen.

VIDEREUTVIKLING AV NSMS KURSSENTER FOR FOREBYGGENDE SIKKERHET. Tilgjengelige undervisningsressurser ved kurssenteret er en knapphetsfaktor, både til eksisterende kursportefølje og til planlagt utvidelse. Etterspørselen etter kurstilbudet er i dag høyere enn leveransekapasiteten. Undervisningsressursene hentes fra NSMs fagavdelinger, som allerede har en høy belastning. Forsvaret og NSM arbeider med å samordne kursporteføljen der det er hensiktsmessig og hvor det er mulig å oppnå gevinster.

Et verktøy som kan gi kursporteføljen et bredere nedslagsfelt er å etablere profesjonell e-læring innen forebyggende sikkerhet. Det bør etableres et godt tilbud innen e-læring som både supplerer og erstatter hele eller deler av kurs.

Prinsippet om brukerfinansiering av kurssenterets drift bør videreføres. Det er imidlertid avgjørende med en grunnfinansiering som sikrer en videreutvikling av kurssentret.

Når aktuelle kurs er samordnet og det er realisert flere gevinster ved kurssenterets drift, vil NSM bygge ut tilbudets akademiske profil. Gjennom avtaler med høgskoler eller universitet kan kursene gi sertifisering eller være poenggivende for høyere utdanning.

På bakgrunn av dette anbefaler NSM følgende tiltak:

70. Forsvarsdepartementet bør styrke NSM med undervisningsressurser og nødvendig grunnfinansiering.
71. Forsvarsdepartementet bør tilføre NSM midler til utviklingen av et profesjonelt tilbud innen e-læring som gjør det mulig å skape en felles faglig plattform og skalere tilbudet slik at det kan nå langt flere med færre dager i kurssenteret.
72. Forsvarsdepartementet bør gi NSM i oppdrag å finne løsninger sammen med høgskoler og universiteter med tanke på å tilby poenggivende utdanninger, kurs eller sertifisering.

21. Tiltakenes relevans for Forsvarets operative evne

NSMs evner innen forebygging, håndtering og kontroll bidrar til å styrke Forsvarets operative evne gjennom direkte leveranser til Forsvaret. NSM bidrar gjennom dette også til å øke samfunnssikkerheten generelt. Dette medfører at Forsvaret kan fokusere på sin kjernevirksomhet, samt sikre leveranser fra sivile aktører. Et mer robust sivilsamfunn som i større grad ivaretar egen sikkerhet vil redusere behov for støtte fra Forsvaret i fredstid og i en krisesituasjon.

Flere av tiltakene i SFR vil bidra til økt operativ evne. De konkrete bidragene som følge av tiltakene er beskrevet under. Noen av disse punktene omfatter flere enkelttiltak.

Styrking av nasjonal hendelseshåndtering og samlokalisering av denne, vil kunne bidra til ytterligere økt evne til å detektere og håndtere trusler som kan påvirke Forsvarets operative evne.

Styrking av NSM og Forsvarets evne til personellkontroll og kildefangst vil kunne gi økt tilgang til klarert personell som kan anvendes i operativ tjeneste.

[36] «Opplæring i informasjonssikkerhet», Nina Hoddø Bakås, Universitetet i Oslo, 2015

Et nasjonalt rammeverk for etablering og drift av sikre IKT-løsninger vil kunne redusere tiden Forsvaret bruker for å implementere og få godkjent operative systemer. Dette sammenholdt med forsterket fokus på standardiserte IKT-løsninger (ugradert, lav- og høygradert) vil kunne øke Forsvarets evne til å samhandle effektivt med totalforsvaret og sivil sektor i fred, krise og krig.

FoU og materiellinvesteringer innen kryptografi som NSM foreslår i SFR vil bidra til økt operativ evne gjennom økt sikkerhet (konfidensialitet, integritet og tilgjengelighet) i Forsvarets IKT-systemer. Ny generasjon kryptoløsninger vil gi en substansiell økning av operativ evne, både gjennom effektivisering og forsterket sikring.

Økt evne hos NSM til å utøve inntrengningstesting vil bidra til økt sikkerhet i systemene som skal understøtte operasjoner i Forsvaret.

Ytterligere fokus på korrekt utvelgelse av skjermingsverdige objekter, sikringstiltak, samt tverrsektoriell prioritering av sikringsressurser, vil bidra til effektivisering og optimal bruk av Forsvarets operative ressurser i beredskapssituasjoner samt i krise og krig.

NSM bidrar til en rekke ulike prosjekter i forsvarssektorens portefølje. I tillegg har også NSM gjennomføringsansvar for noen av disse. Sentrale elementer i disse investeringene er nye systemer for person- og virksomhetskontroll, graderte plattformer, ulike virksomhetskritiske verktøy samt kryptoprosjekter. Flere av disse aktivitetene er sentrale for å styrke Forsvarets operative evne, særlig innen sikring av informasjon.

Disse tiltakene vil ha særlig påvirkning på Forsvarets operative evne. I tillegg kommer de andre tiltakene, som vil være relevante for alle sektorer, herunder forsvarssektoren.

22. Styrking og videreutvikling av NSM

BAKGRUNN. NSM skal utvikle nasjonale krav og anbefalinger innenfor sine fagområder, og kontrollere og sikre at disse følges. Vi foreslår å bygge på og styrke disse rollene, fremfor å foreslå nye organisatoriske tiltak.

Generelt for NSMs oppgaver innen forebygging, håndtering og kontroll ser vi at det er krevende å kunne gi god nok støtte til virksomheter og aktører i forsvarssektoren og i sivil sektor. Til tross for refokusering av virksomheten, erfarer NSM at det er et gap mellom behovet for støtte og det vi er i stand til å yte. Både virksomheter og statlige organ som har vært utsatt for hendelser, og virksomheter der NSM har vært på tilsyn, har et stort behov for oppfølgende rådgivning og kompetansebygging. Dette behovet er NSM per i dag ikke i stand til å møte.

NSM erfarer at både Forsvarsdepartementet og Justis- og beredskapsdepartementet har behov for substansielle bidrag til støtte for sin politikkutforming innenfor samfunnssikkerhet og beredskap. Behovet er større enn det NSM er i stand til å etterkomme på en forsvarlig måte.

NSM er gitt i oppdrag å utrede videre utvikling av NSMs drift gitt at dagens budsjettramme på kapittel 1723, post 01 holdes på 2015-nivå, alternativt en økning av rammen med 0,5 prosent. Dette vil utgjøre en økning på drøyt 1 million kroner, eller cirka ett årsverk. En økning av budsjettrammen på 0,5 prosent anses ikke som vesentlig, og utredes ikke nærmere da konsekvensene vil være de samme som ved uendret budsjettnivå.

I denne rapporten er det beskrevet tiltak som kan gjennomføres med og uten rammeøkning. Alle tiltakene vil medføre redusert sårbarhet. Det er imidlertid lagt til grunn at de som gir mest effekt, gjennomføres først. Hvor mange tiltak og i hvilket omfang de lar seg gjennomføre bestemmes av størrelsen på budsjettet.

Nedenfor følger først en beskrivelse av konsekvensene for NSMs virksomhet ved henholdsvis

reell videreføring av driftsmidlene i forhold til saldert budsjett for 2015, inkludert 0,5% økning. Deretter følger en overordnet beskrivelse av tiltak som NSM mener krever økte driftsmidler for å kunne la seg realisere. Deretter kommer en omtale av realisering av de foreslåtte tiltak gjennom henholdsvis FoU, store materiellinvesteringsprosjekter i forsvarssektoren og en særlig avsetning av materiellinvesteringsmidler for NSM.

Innretning av NSMs virksomhet ved reell videreføring av driftsmidler ift. saldert budsjett 2015 (inkludert 0,5% økning).

NSM har små og sårbare fagmiljøer, og dette er en kritisk utfordring. NSM er nå kommet til et punkt der effektivisering og mindre justeringer ikke lenger er tilstrekkelig for å tilfredsstille leveransebehovet i samfunnet. Gapet mellom samfunnets behov og NSMs leveranseevne øker. NSMs driftsbudsjett har i de senere år blitt økt for først og fremst å bedre IKT-sikkerheten. Dette er midler som nå begynner å få effekt. Utfordringene på dette området øker likevel mer enn budsjettøkningene.

NSM har videre mange daglige driftsoppgaver som vanskelig kan overføres til andre da de er en vesentlig del av kjernevirksomheten. Dette gjelder for eksempel produksjon og distribusjon av kryptonøkler, gjennomføring av tilsyn, fastsetting av krav til IKT-systemer og funksjonen som klageinstans for klareringssaker. Dette er noen av oppgavene som ikke er nærmere beskrevet i rapporten, men som utgjør en vesentlig del av den virksomheten som finansieres av NSMs driftsbudsjett. Store deler av NSMs driftsbudsjett er derfor bundet opp.

Som nevnt tidligere i rapporten har NSM over tid tatt ut effektiviseringsgevinster. Det kan imidlertid være rom for effektivisering av interne støttefunksjoner. Skulle andre i forsvarssektoren kunne tilby bedre og billigere tjenester når det gjelder IKT-tjenester, innkjøp, økonomi- og HR-forvaltning, vil dette være en effektivisering som kan bidra til at midler til prioriterte tiltak utenfor rammen kan realiseres.

Det er behov for å utrede nærmere hvilke tiltak som kan iverksettes ved videreføring av rammen ift. saldert budsjett for 2015 (inkludert 0,5 prosent økning av driftsrammen). I det følgende vil vi likevel antyde hvilke tiltak det kan være mulig å se nærmere på:

- Flere av tiltakene innenfor organisering, styring og koordinering kan implementeres, som for eksempel avklaring av roller og ansvar, juridiske avklaringer som grunnlag for eventuelle nye lovhjemler, rapporteringsoppdrag med mer.
- Noen av tiltakene under IKT-sikkerhet kan påbegynnes. Gis NSM oppdrag som skissert under tiltakene kan NSM påbegynne arbeid med rammeverk med tanke på kravstilling og anbefalinger. Uten ressurstilførsel vil flere av tiltakene som medfører utredninger kunne ta lang tid.
- Antallet alvorlige IKT-hendelser har økt med 40 prosent hvert år de seneste årene. Om ikke denne økningen besvares med en økt tilgang på ressurser vil flere alvorlige saker måtte nedprioriteres. Tiltak innenfor styrking av deteksjonsevne, tilsyn og hendelseshåndtering må derfor tilleggsfinansieres.
- Noen av tiltakene under personellsikkerhet kan iverksettes. Mer substansielle utfordringer innenfor personellsikkerhet, som beskrevet i rapporten, bør løses ved å styrke NSM som fagmyndighet. Dette kan realiseres dersom forslag til ny klareringsstruktur blir fremmet og vedtatt, og ressursene prioriteres til å styrke fagmyndighetsoppgavene.
- Noen av tiltakene under fysisk sikkerhet kan iverksettes. Styrking av NSMs rolle innen veiledning, rådgivning og større utredninger på området må tilleggsfinansieres.
- Et fåtall av tiltakene innen kompetanse kan iverksettes. Dette dreier seg primært om samordning og utredninger. NSMs kurssenter i forebyggende sikkerhet er forutsatt å være selvfinansiert gjennom brukerbetalinger. Dette vil også gjelde en eventuell utvidelse av senteret. Et økt kursomfang vil imidlertid medføre at det vil bli behov for mer fagpersonell i NSM for å kunne gjennomføre kurs. Dette er personell som må forutsettes å ha sitt daglige virke i fagavdelingene i NSM. Dagens personelloppsetning i NSM vil ikke tillate et økt kursomfang da undervisning i for stor grad vil gå på bekostning av oppgaver i fagavdelingene. Utvidelse av

undervisningsressurser og læringstilbudet må tilleggsfinaniseres.
- Gitt at tiltaket om å overføre leverandørklareringsmyndigheten iverksettes, kan ressursene til dette reallokeres til kontroll og utvikling av ordningen med sikkerhetsgraderte anskaffelser.

Enkelte av de foreslåtte tiltakene som krever NSMs involvering kan altså startes opp eller implementeres uten økte rammer. Dette er primært tiltak relatert til utredninger om driftsøkonomi og kapabiliteter. I det alt vesentlige vil tiltakene vedrørende styrking og videreutvikling av NSM forutsette økte driftstildelinger og investeringer.

STYRKING AV NSMS DRIFTSBUDSJETT. Som det fremgår av første del av dette kapittelet, er det behov for substansiell økning av NSMs driftsbudsjett for å kunne forsterke og videreutvikle NSMs samfunnsleveranser. Forebygging og håndtering av IKT-hendelser er området hvor utfordringene er store, og hvor ekstra innsats vil gi størst risikoreduserende effekt. Økt tildeling vil kunne redusere gapet mellom behovet for støtte og det NSM p.t er i stand til å yte betydelig. I det følgende beskrives tiltak som bare kan løses fullt ut ved en økning av NSMs driftsbudsjett. Flere av disse vil dessuten kreve investeringer, herunder innen eiendom, bygg og anlegg (EBA). Prioriteringen og detaljbudsjetteringen av disse skjer i en egen prosess:

- Tydeliggjøre organisering, ledelse og koordinering
  - Gjennomføring av årlige nasjonale øvelser i IKT-sikkerhet og hendelseshåndtering
  - Samlokalisering av NSM
  - Etablere attachéordning for sikkerhetsteknologi
- Styrke IKT-sikkerheten
  - Styrke nasjonalt samarbeid og informasjonsdeling vedrørende IKT-sikkerhet
  - Utvikling av et nasjonalt rammeverk innenfor IKT-sikkerhet
  - Utredning av behov og løsninger for nasjonale skytjenester og annen sensitiv informasjon
  - Utvikling av en godkjenningsordning for programvarebaserte kryptoløsninger for beskyttelse av lavgradert og annen sensitiv informasjon
  - Styrking og videreutvikling av NSM som nasjonal sertifikatutsteder for sikker identifikasjon av individer og deres bruk av IKT-tjenester i samfunnet
  - Kapasitet til å føre tilsyn med tekniske IKT-sikkerhetstiltak, herunder å etablere tilsynsstøtte for andre sektortilsyn.
- Styrke håndteringen av cyberangrep
  - Styrke den nasjonale CERT-funksjonen,
  - Samlokalisering av og sentral tilstedeværelse fra håndteringsmiljøer, myndigheter, m.fl.
  - Etablering av portal på internett for effektiv og rask informasjonsdeling
  - Styrking og videreutvikling av VDI-løsningen til et robust sensornettverk
  - Statlig fullfinansiering av VDI-samarbeidet.
- Styrke personellsikkerheten
  - Effektivisering av klareringsprosessen,
  - Styrking av NSM for å gjennomføre bilaterale prosesser å skape forutsigbarhet i personkontrollen
  - Utredning av hvordan kontrollmekanismene for identifikasjon av personell i hele personellsikkerhetskjeden kan bli sikrere
- Styrke arbeidet med fysisk sikkerhet:
  - Styrke NSMs evne til å gi råd og veiledning,
  - Etablere et felles rådgivingssenter
  - Sammen med PST og POD utarbeide kompetanseprogram om sikkerhetsdesign
- Samarbeid og informasjonsdeling med næringslivet
  - Etablere og forvalte ordning for akkreditering av private selskaper eller offentlige forvaltningsorganer for sikkerhetstjenester
- Styrke kompetansen om sikkerhet
  - Undervisningsressurser og nødvendig grunnfinansiering av NSMs kurssenter for forebyggende sikkerhet
  - Utvikling av et profesjonelt tilbud innen e-læring

En rekke av tiltakene som foreslås i SFR forutsetter utredninger i NSM, som vil kreve økte driftsmidler. Det antas at både FD og JD vil ha behov for substansielle bidrag fra NSM til støtte til de foreslåtte tiltak for politikkutforming på sikkerhetsområdet. Samlet sett er dette utredningsbehovet større enn det NSM i dag er i stand til å overkomme.

STYRKING AV NSMS RAMME FOR FORSKNING OG UTVIKLING (FOU). NSM utfører til enhver tid en betydelig mengde forsknings- og utviklingsaktiviteter. Disse prosjektene understøtter NSMs arbeid med å styrke kompetanse, utvikle forebyggende sikkerhetstiltak, bidra til effektiv hendelseshåndtering, styrket objektsikkerhet, personellsikkerhet og andre sentrale aspekter innen NSMs samfunnsoppdrag. FoU-aktivitetene er også en del av NSMs bidrag til å styrke Forsvarets operative evne.

FoU-arbeidet bidrar til at relevante sikkerhetstiltak kommer på plass så tidlig som mulig for samfunnet. FoU-porteføljen tilfører organisasjonen og samfunnet kompetanse om materiell og teknologi som deretter kan realiseres gjennom råd og veiledning, tiltak og materiellinvesteringer. FoU-porteføljens økonomiske ramme og innretning er viktig for NSM.

FoU-porteføljen gir vesentlig merverdi i NSMs arbeid og leveranser til samfunnet. I tiden fremover ønsker NSM å fokusere ytterligere på FoU-aktiviteter relatert til risikoreduserende tiltak. Det er i dag flere nødvendige aktiviteter som det ikke finnes økonomisk handlingsrom for å håndtere. Økning av FoU-rammen vil styrke NSMs evner innen både forebygging, håndtering og kontroll. Det konkrete behov vil fremkomme av Plan for FoU-tiltak.

ETABLERING AV EN EGEN BUDSJETTPOST FOR NSMS INTERNE MATERIELLINVESTERINGER. Materiellinvesteringer av betydelig art (ikke driftsanskaffelser) realiseres gjennom forsvarssektorens investeringsportefølje. Forsvarsdepartementet har gjennom den overordnede forsvarsplanleggingen ansvar for planleggingen av Forsvarets materiellinvesteringer. Basert på forsvarssektorens behov skal strategien for de næringspolitiske aspekter ved forsvarssektorens anskaffelser bidra til økt nasjonal verdiskapning og utvikling av et konkurransedyktig næringsliv, samt sikre forsvarssektoren nødvendig tilgang til kompetanse, materiell og tjenester. NSM har ikke et eget investeringsprogram for store sikkerhetsrelaterte prosjekter, men deltar i forsvarssektorens portefølje.

Prosjektene NSM har gjennomføringsansvar for er viktige prosjekter både for NSM og aktører i militær og sivil sektor.

Som deltaker i forsvarssektorens investeringsportefølje, er NSM kun en av mange aktører som til enhver tid fremmer behov. Investeringsbehov innenfor NSMs virkeområde kan være tidskritiske å gjennomføre. Særlig i perioder med store investeringer i Forsvaret, kan det være utfordrende å sikre at nye prosjekter av betydning for sikkerheten opprettes og gjennomføres i tide. Til tross for positiv utvikling i senere tid, ønsker NSM større forutsigbarhet i forhold til behov for investeringer. Andelen av materiellporteføljen som går til store sikkerhetsrelaterte prosjekter bør følgelig utvides. Disse tiltakene bør realiseres utenfor budsjettrammen til NSM.

NSM har betydelige materiellinvesteringsbehov. Det er også betydelige investeringsbehov relatert til eiendom, bygg og anlegg (EBA). Under følger noen utvalgte elementer av NSMs investeringsbehov. Disse er nødvendige for å styrke samtlige eksternt rettede kjerneevner i NSM. Disse evnene skal understøtte samfunnet. Beskrivelsene er ikke uttømmende.

- NSM har behov for å investere for ytterligere å styrke sikkerhetstiltak, deteksjonsevne og kommunikasjonsløsningene internt i NSMs IKT-systemer. Dette er nødvendig for å styrke robusthet og tilgjengeligheten til nødvendig IKT infrastruktur. Dette prosjektet kommer i tillegg til andre pågående prosjekter.
- NSM har behov for et prosjekt som skal utvikle systemer for å understøtte NSMs kjerneoppgaver innen forebygging, håndtering og kontroll. Dette innebærer områdespesifikke applikasjoner og annen systemunderstøttelse, samt materiell. Denne aktiviteten kommer i tillegg til andre pågående prosjekter.
- NSM anbefaler at det iverksettes et prosjekt

for å isolere og utføre tiltak for styrket grunnsikring i NSM. Dette er nødvendig for å styrke robustheten i NSMs evne til å levere samfunnskritiske funksjoner.

- NSM har i de senere år blitt tilført en rekke nye og sentrale oppgaver i samfunnet. Dette medfører at organisasjonen er i vekst når det gjelder personell og kompetanse. I tillegg kommer tiltak som foreslått i SFR. Det er i denne anledning nødvendig med investeringer relatert til fasiliteter og bygningsmasse. Særlig viktige i den forbindelse er forslagene om samlokalisering av NSM, og samlokalisering av de sektorvise responsmiljøene med NSM NorCERT.

VIDEREUTVIKLING AV RAMMEVERK FOR NSMS KAPASITETER OG KAPABILITETER. Som nevnt i del I og II har NSM utarbeidet en oversikt over evnene organisasjonen besitter, og hvilke utfordringer som er forbundet med dette. Oppdrag, regelverk og samfunnsutviklingen legger føringer på hvilke evner NSM skal besitte. Nye eller endrede evner medfører behov for å endre og investere i organisasjonen, som igjen kan utløse behov for økte ressursrammer. Med bakgrunn i forslagene til tiltak i SFR er det nå formålstjenlig å videreutvikle rammeverket for evner som et verktøy for utvikling av organisasjonen, dialog om innretning av organisasjonen og dialog om ressursrammer. En strukturert prosess for utvikling av evner og mengden av disse evnene er viktig for at NSM kan løse sitt samfunnsoppdrag. Det er i den forbindelse behov for at NSM utvikler en helhetlig plan for utvikling av evnene (kapabilitetsutviklingsplan), som blant annet kan legges til grunn for dialogen med Forsvarsdepartementet og Justis- og beredskapsdepartementet om den videre utvikling og innretning av NSM.

Vedlegg

Vedlegg A

INSTRUKS FOR SJEF NASJONAL SIKKERHETSMYNDIGHET
Gitt av Forsvarsdepartementet 5. desember 2014.

KAPITTEL I INSTRUKSENS FORMÅL

1. Formålet med instruksen er å angi ansvar, myndighet, roller og oppgaver til Sjef NSM. Instruksen skal tydeliggjøre forventinger og sikre god styring og ledelse av NSM, herunder en effektiv og forsvarlig forvaltning av tildelte ressurser.

KAPITTEL II NSMS MYNDIGHETSOMRÅDE

2. NSM skal utøve sitt ansvar i tråd med Lov om forebyggende sikkerhetstjeneste (sikkerhetsloven), lov om oppfinnelser av betydning for rikets forsvar og forskrift om fotografering mv. fra luften og kontroll av luftfotografier og opptaksmateriale fra luftbårne sensorsystemer. NSM skal utøve sertifiseringsmyndighet for IT-sikkerhet i produkter og systemer (SERTIT). NSM skal også, som det nasjonale fagmiljøet for IKT-sikkerhet, understøtte og bidra til utøvelsen av Forsvarsdepartementets (FD) og Justis- og beredskapsdepartementets (JD) ansvar på IKT-sikkerhetsområdet. JD har samordningsansvaret for forebyggende IKT-sikkerhet i sivil sektor ved kgl.res. 22. mars 2013.

3. NSM er underlagt FD. JD har instruksjonsmyndighet overfor NSM i saker innenfor JDs ansvarsområde.

4. FD utsteder i samarbeid med JD iverksettingsbrev (IVB) med tilhørende presiseringer, rettelser og tillegg (PET) til NSM, og gjennomfører styringsdialog med NSM. Oppdrag som av tidshensyn ikke gis i IVB eller PET, koordineres mellom JD og FD.

KAPITTEL III SJEF NSMS ANSVAR, MYNDIGHET, ROLLER OG OPPGAVER

5. Sjef NSM skal, på vegne av forsvarsministeren og justis- og beredskapsministeren, utøve et overordnet og sektorovergripende ansvar for forebyggende sikkerhetstjeneste i henhold til sikkerhetsloven.

6. Sjef NSM skal nå de fastsatte mål, og har ansvar for å utvikle NSM i henhold til de til enhver tid gjeldende styringsdokumenter.

7. Sjef NSM rapporterer til FD for oppgaveløsning i forsvarssektoren og til JD for oppgaveløsning i sivil sektor.

8. Sjef NSM skal på eget initiativ og uten unødig opphold informere FD og JD om saker av særlig viktighet, eller av prinsipiell eller politisk karakter innenfor sitt ansvarsområde.

9. Sjef NSM er forsvarsministerens og justis- og beredskapsministerens nærmeste rådgiver i spørsmål om forebyggende tiltak mot sikkerhetstruende virksomhet som kan ramme nasjonale og samfunnsmessige verdier.

10. Sjef NSM skal etablere og vedlikeholde et helhetlig risikobilde innen forebyggende sikkerhet og produsere en årlig rapport om sikkerhetstilstanden, blant annet basert på trusselvurderinger fra Etterretningstjenesten og Politiets sikkerhetstjeneste. Sjef NSM skal foreslå tiltak for å bedre sikkerhetstilstanden.

11. Sjef NSM skal etablere og vedlikeholde et IKT-risikobilde som omfatter statssikkerhet, samfunnssikkerhet og individsikkerhet, og skal foreslå tiltak, gi anbefalinger og fremme forslag til krav innen IKT-sikkerhet i samfunnet, samt følge opp med råd og veiledning.

12. Sjef NSM er ansvarlig for å koordinere håndteringen av alvorlige IKT-angrep mot samfunnskritisk infrastruktur eller andre viktige samfunnsfunksjoner.

13. Sjef NSM er ansvarlig for å organisere og drifte et nasjonalt varslingssystem for digital infrastruktur.

14. Sjef NSM skal ved behov iverksette nødvendige beredskapsmessige tiltak innenfor gitte fullmakter, herunder i sikkerhetsloven og Nasjonalt beredskapssystem (NBS). I en situasjon der et annet departement enn FD eller JD får ansvar for kriseledelse, rapporterer sjef NSM faglig om situasjonen også til dette departement, med siderapportering til FD og JD.

15. Sjef NSM skal koordinere arbeidet mellom myndigheter som har en rolle innenfor forebyggende IKT-sikkerhet, og skal legge til rette for hensiktsmessig samhandling mellom disse. Til dette ansvaret hører bl.a. koordinering av forskning og utvikling, herunder kompetanseutvikling og internasjonalt arbeid på området.

16. Sjef NSM er Norges representant i internasjonale fora innen forebyggende sikkerhet, og i bi- og multilateralt samarbeid på fagområdet. Sjef NSM representerer Norge i NATOs sikkerhetskomité.

17. Sjef NSM skal legge til rette for hensiktsmessig informasjonsutveksling med relevante samarbeidspartnere, særlig Etterretningstjenesten og Politiets sikkerhetstjeneste.

18. Sjef NSM skal innen eget ansvarsområde bidra til å understøtte Forsvarets operative evne iht. gjeldende krav og føringer.

19. Sjef NSM skal gi støtte til norsk kryptoindustri.

20. Sjef NSM skal samarbeide med andre relevante aktører innenfor forebyggende sikkerhet. Sjef NSM skal medvirke til at ansvarsforhold er avklart. Det skal særlig søkes å unngå overlapping i myndighetsutøvelse.

21. Dersom det ikke oppnås hensiktsmessig avklaring av ansvarsforhold eller det er andre forhold av betydning vedrørende samarbeid med andre relevante aktører, skal saken forelegges FD og JD.

KAPITTEL IV INTERN STYRING OG LEDELSE

22. Sjef NSM skal sikre god styring og ledelse av virksomheten i NSM.

23. Sjef NSM skal ivareta arbeidsgiveransvaret for ansatte i NSM og sikre at virksomheten evner å rekruttere, anvende, utvikle og beholde medarbeidere med riktig kompetanse.

24. Sjef NSM skal definere myndighet og ansvar internt i NSM. Delegering av myndighet skal dokumenteres.

25. Sjef NSM skal fastsette direktiver og instrukser innenfor eget myndighetsområde, med utgangspunkt i denne instruks.

26. Sjef NSM skal innenfor gitte rammer utarbeide forslag til budsjett for NSM, føre kontroll med at tildelte midler blir effektivt utnyttet, gjennomføre løpende mål-, resultat- og risikostyring og rapportere i henhold til fastsatte krav.

27. Sjef NSM skal sikre at virksomheten har evne til å føre effektiv internkontroll i egen virksomhet. Sjef NSM er ansvarlig for at eventuelle regnskaps- og forvaltningsmessige avvik blir raskt utbedret.

28. Når sjef NSM er forhindret fra å utøve sine embetsplikter, fungerer assisterende sjef for NSM som sjef NSM.

KAPITTEL V UTADRETTET VIRKSOMHET

29. Sjef NSM er ansvarlig for presse- og informasjonsvirksomhet knyttet til egen virksomhet. Sjef NSM skal utad fremstå som en synlig sjef for etaten og delta i det offentlige ordskiftet om NSM og forebyggende sikkerhet.

30. Sjef NSM skal bidra til å styrke samfunnets kunnskap, forståelse, motivasjon og evne til å ivareta forebyggende sikkerhet, herunder IKT-sikkerhet på en best mulig måte.

31. Sjef NSM skal bidra til at de enkelte myndigheter og virksomheter settes bedre i stand til å ivareta sitt ansvar iht. sikkerhetsloven.

32. Sjef NSM skal gi selvstendige høringsuttalelser i spørsmål om forebyggende sikkerhet generelt og IKT-sikkerhet også ut over det som er regulert i sikkerhetsloven.

KAPITTEL VI AVSLUTTENDE BESTEMMELSER

33. Instruksen her trer i kraft umiddelbart.

Vedlegg B

Liste over tiltak i Sikkerhetsfaglig råd som antas å ha særlig relevans for arbeidet i Sikkerhetsutvalget

En rekke tiltak som beskrives i Sikkerhetsfagligråd vil ha relevans for arbeidet som skal foreslå nytt lovgrunnlag for forebyggende nasjonal sikkerhet gjennom Sikkerhetsutvalget. Utvalget skal levere en rapport med lovforslag i form av en NOU (Norges offentlige utredninger) i løpet av høsten 2016. Listen referer til tiltaksnummer og tekst fra Sikkerhetsfaglig råd del III Tiltak.

TILTAK NR. 9 Justis- og beredskapsdepartementet og Forsvarsdepartementet må klargjøre hvilke private aktører som har en rolle i krise- og beredskapssituasjoner. Aktørene må bli satt i stand til, og ha nødvendig kompetanse til, å motta nødvendig sikkerhetsgradert informasjon. En nødvendig forutsetning for dette er at aktørene blir omfattet av sikkerhetsloven.

TILTAK NR. 13 Med utgangspunkt i Instruks for Sjef NSM bør det fastsettes en kgl.res. for å gi NSM et tydelig tverrsektorielt mandat og styrke rollen som den nasjonale myndigheten for IKT-sikkerhet også utover sikkerhetsloven, og være strategisk IKT-sikkerhetsrådgiver i hele krisespennet. En kgl.res. vil også tydeliggjøre sjef NSM sin rolle som nasjonal og tverrsektoriell koordinator for håndtering av IKT-sikkerhetshendelser.

TILTAK NR. 18 Skisse til lovforslag om sikring av sensitiv informasjon og informasjonsinfrastruktur, som er til behandling i Justis- og beredskapsdepartementet, bør konkretiseres gjennom arbeidet i Sikkerhetsutvalget.

TILTAK NR. 41 Sikkerhetsutvalget bør vurdere å gi NSM utvidet hjemmel til inntrengingstesting etter sikkerhetsloven til å omfatte også nasjonal kritisk IKT-infrastruktur, og oppdraget bør utvides til å omfatte testing av logiske, tekniske, administrative, menneskelige og fysiske sårbarheter, da disse er vevet tett sammen. NSM bør gis hjemmel til å gjennomføre inntrengningstesting uten forutgående samtykke fra virksomheten.

TILTAK NR. 44 Forsvarsdepartementet bør fremme et forslag til lovfesting av at NSM som hovedregel kan kreve automatisert innhenting fra kilderegistre, herunder regelmessig kildekontroll i klareringens gyldighetstid.

TILTAK NR. 46 Forsvarsdepartementet og Justis- og beredskapsdepartementet bør ta initiativ til at deltakelse i VDI-samarbeidet fullfinansieres av staten. Deltakelse bør gjøres obligatorisk for virksomheter med samfunnsviktig IKT-infrastruktur og samfunnsviktige funksjoner, etter en risikovurdering. En slik deltakelse må hjemles i lov.

TILTAK NR. 51 Forsvarsdepartementet bør legge til rette for at klareringsmyndighetsstrukturen endres i tråd med foreslått endring i sikkerhetsloven som er til behandling.

TILTAK NR. 55 Justis- og beredskapsdepartementet bør få utredet en ny tverrsektoriell hjemmel og ordning for bakgrunnskontroll av personell med sikte på å ivareta legitime behov som vandelsattest ikke dekker eller alene er utilstrekkelig for.

TILTAK NR. 48 Sikkerhetsutvalget bør utrede virksomheters rettslige rammer og andre virkemidler for å motvirke innsidetrusselen.

TILTAK NR. 57 Forsvarsdepartementet bør fremme forslag om endring av sikkerhetsloven § 20 sjette ledd, slik at NSM kan gi informasjon fra klareringssaker til Politiets sikkerhetstjeneste (PST) som er relevant for at PST skal kunne ivareta sitt ansvar for å forebygge og motvirke trusler mot rikets sikkerhet eller andre grunnleggende nasjonale interesser.

TILTAK NR. 59 Det bør sikres at objekter klassifisert etter sikkerhetsloven gis prioritet på statlige sikringsstyrker, fremfor objekter utvalgt kun etter sektorregelverk. Om nødvendig, bør dette fastsettes gjennom Kgl.res. Dette bør vurderes av Sikkerhetsutvalget.

TILTAK NR. 64 Forsvarsdepartementet bør fremme et forslag om at sikkerhetsloven endres slik at Kongen kan utpeke klareringsmyndigheter og klageinstans for saker om leverandørklarering og andre myndighetsavgjørelser på området.

NASJONAL SIKKERHETSMYNDIGHET

Postboks 814, 1306 Sandvika

Tlf. 67 86 40 00
post@nsm.stat.no
www.nsm.stat.no