Nasjonal sikkerhetsmyndighet – oppgaver og styring

Nasjonal sikkerhetsmyndighet – oppgaver og styring

Under er en forklaring på forkortelser som er brukt i kapittel 1 i utredningen. I vedlegg 2 er det en lengre liste med forkortelser som brukes også ellers i utredningen.

Institusjoner:

DFD	Digitaliserings- og forvaltningsdepartementet
DEKSA	Direktoratet for eksportkontroll og sanksjoner
DSB	Direktoratet for samfunnssikkerhet og beredskap
FCKS	Felles cyberkoordineringssenter
NATO	Den nordatlantiske traktats organisasjon
NC3	Nasjonalt cyberkrimsenter
NCSC	Nasjonalt cybersikkerhetssenter
NorSIS	Norsk senter for informasjonssikring
NSM	Nasjonal sikkerhetsmyndighet
PST	Politiets sikkerhetstjeneste

Begreper i arbeid med forebyggende sikkerhet:

GNF	Grunnleggende nasjonale funksjoner
KIKS	Kritisk infrastruktur og kritiske samfunnsfunksjoner
SERTIT	Den offentlige sertifiseringsmyndigheten for IT-sikkerhet i Norge
TSU	Tekniske sikkerhetsundersøkelser
VDI	Varslingssystem for digital infrastruktur

Innhold

Oversikt over bokser

Viktige begreper

En lengre liste med mer utdypende forklaringer er beskrevet i boks 3.1.

Statssikkerhet er å ivareta statens eksistens, suverenitet, territorielle integritet og politiske handlefrihet.

Nasjonal sikkerhet defineres som statssikkerhet og en avgrenset del av samfunnssikkerhet som er av vesentlig betydning for statssikkerheten.

Samfunnssikkerhet handler om samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare.

Nasjonale sikkerhetsinteresser er landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser.

Grunnleggende nasjonale funksjoner er tjenester eller produksjon mv. der helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.

Informasjon, objekter, infrastruktur og **informasjonssystemer** er **skjermingsverdige** dersom de er av betydning for nasjonale sikkerhetsinteresser.

Skjermingsverdige verdier brukes som en samlebetegnelse på disse.

Kritiske samfunnsfunksjoner er funksjoner som er nødvendige for å ivareta befolkningens og samfunnets grunnleggende behov, som mat, vann, varme, og trygghet.

Kritisk infrastruktur er anlegg og systemer som er nødvendige for å opprettholde kritiske samfunnsfunksjoner.

Forebyggende sikkerhetsarbeid er å planlegge, tilrettelegge, gjennomføre og kontrollere forebyggende tiltak mot sikkerhetstruende virksomhet og følger av slik virksomhet.

1 Sammendrag

Utvalget er bedt om å vurdere oppgavene til Nasjonal sikkerhetsmyndighet (NSM). Den sentrale problemstillingen er hvordan NSM best kan bidra i arbeidet med forebyggende nasjonal sikkerhet.[1] Ifølge mandatet skal utvalget vurdere om det er oppgaver som ikke følger direkte av loven, som bør overføres til andre myndigheter. Viktige premisser har vært at Norges internasjonale forpliktelser må ivaretas og at forslagene skal være budsjettnøytrale. Utvalgets mandat omhandler NSMs oppgaver, men vurderingene vil berøre delingen av ansvar mellom departementene i arbeidet med å forebygge digitale hendelser og trusler.

For å svare ut mandatet er flere temaer belyst. Disse er omtalt i ulike kapitler i utredningen. Vi gir en beskrivelse av hvordan arbeid med forebyggende sikkerhet i Norge er organisert og utføres i dag. NSMs historie og sikkerhetslovens formål og virkeområde er beskrevet. NSM ble opprettet i 2003 med Forsvarsdepartementet som administrativt ansvarlig departement, men der også Justis- og beredskapsdepartementet hadde et fagansvar. I 2019 ble det administrative ansvaret overført til Justis- og beredskapsdepartementet. Videre følger en omtale av NSMs oppgaver, hvilke som følger av sikkerhetsloven og hvilke som er gitt på annet grunnlag. Styringen og finansieringen av NSM er også beskrevet. I tråd med mandatet har vi omtalt de mest sentrale statlige myndigheter som har grenseflater mot NSM. Vi beskriver hvordan de er tilgrenset, om oppgavene glir over i hverandre og hvordan arbeidsdelingen er regulert. Norges internasjonale forpliktelser er deretter beskrevet og også hvordan arbeidet med forebyggende sikkerhet er organisert i utvalgte andre land. Vi har sett nærmere på organiseringen i Sverige, Danmark, Finland, Nederland, USA og Storbritannia. En vurdering av trusler framover utarbeidet av Justis- og beredskapsdepartementet og Forsvarsdepartementet etter anmodning fra utvalget, følger deretter. Denne legges til grunn av utvalget.

NSMs kjerne bør være de oppgavene som følger av sikkerhetsloven. Loven stiller krav til det nasjonale sikkerhetsarbeidet. NSM bør konsentrere seg om disse oppgavene og være i stand til å løse dem med høy kvalitet. Dette er også i tråd med utvalgets mandat som sier at den sikkerhetspolitiske utviklingen og utviklingen i risikobildet for nasjonal sikkerhet skal være førende for vurderingene.

Norge står overfor komplekse trusler som utfordrer den nasjonale sikkerheten. Arbeidet med digital sikkerhet har fått økt betydning, og skillet mellom den tradisjonelle statssikkerheten og samfunnssikkerheten er mindre tydelig.[2] En koordinert innsats fra en rekke aktører er derfor nødvendig. NSM har her viktige oppgaver.

[1] Se side 9 for definisjon av «nasjonal sikkerhet».

[2] Se side 9 for definisjoner av «statssikkerhet» og «samfunnssikkerhet».

Oppgaveporteføljen til NSM har over tid blitt for bred. Særlig har oppgavene innen digital sikkerhet økt i omfang. For mange og for omfattende oppgaver kan svekke evnen til å løse kjerneoppgavene på en god måte. Omfanget av oppgaver bør derfor reduseres.

NSM er en organisasjon med dyktige medarbeidere. Men organisasjonen har også fått svekket ry etter svikt i den interne økonomiske styringen, kamp for utvidet revir, interne siloer med ulike budskap og lange saksbehandlingstider. Viktige oppgaver etter sikkerhetsloven er forsømt, samtidig som direktoratet er blitt pålagt stadig nye oppgaver utenfor loven. Det ryddes nå opp i styringen av økonomien, organisasjonen utvikles og det samarbeides bedre internt og eksternt.

Modellen med én sikkerhetslov og én sikkerhetsmyndighet bør videreføres. NSM fyller som nevnt rollen som sikkerhetsmyndighet etter sikkerhetsloven. Sikkerhetsmyndigheten skal påse at såkalte skjermingsverdige verdier har forsvarlig sikkerhet både i militær og sivil sektor.[3] Fagområdene i arbeidet med forebyggende sikkerhet omfatter fysisk og digital sikkerhet, personellsikkerhet og sikkerhetsstyring. Sikkerhetsstyring omfatter blant annet saker om eierskapskontroll. Det har verdi og er riktig å legge disse oppgavene til én myndighet. Som fag- og tilsynsmyndighet for forebyggende sikkerhet gir NSM råd og veiledning og får kunnskap og kan spre den bredt. Det er en styrke i lys av dagens risiko- og trusselbilde. I andre land synes organiseringen av arbeidet med forebyggende sikkerhet gjennomgående å være mer fragmentert.

NSMs oppgaver etter sikkerhetsloven bør bli klarere. Sikkerhetsloven § 2-2 gir sikkerhetsmyndigheten «det sektorovergripende ansvaret for at forebyggende sikkerhetsarbeid i virksomhetene utføres i samsvar med loven» og det «overordnede ansvaret for at sikkerhetstilstanden i alle sektorer kontrolleres […]». Ansvaret som beskrives er omfattende og gir grunnlag for ulike tolkninger.

Generelt bør begreper som brukes, gi en presis beskrivelse av NSMs oppdrag. Ord som «overordnet», «sektorovergripende ansvar» og «nasjonal responsfunksjon» kan gi inntrykk av at NSM skal lede, gripe inn og gi alle sikkerhet. Ansvar for sikkerheten ligger hos de enkelte departementene og virksomhetene som er underlagt sikkerhetsloven. NSM skal bistå de ansvarlige blant annet ved å gi råd, veilede og å føre tilsyn. Justis- og beredskapsdepartementet og Forsvarsdepartementet bør presisere i hovedinstruksen hva NSMs oppgaver etter sikkerhetsloven er.

NSM har og bør ha viktige oppgaver innen digital sikkerhet etter sikkerhetsloven. NSM skal drifte og utvikle «Varslingssystem for digital infrastruktur (VDI)», være «nasjonal responsfunksjon» ved alvorlige digitale angrep og formidle informasjon til virksomheter og etablere nødvendige arenaer for informasjons- og erfaringsutveksling. Felles cyberkoordineringssenter (FCKS) og Nasjonalt cybersikkerhetssenter (NCSC) er her viktige arenaer.

Som nasjonal responsfunksjon bidrar NSM i håndtering av digitale hendelser i samfunnskritiske funksjoner, men virksomheter som rammes har selv ansvar for sik-

[3] Se side 9 for definisjon av «skjermingsverdige verdier».

kerheten og er som regel i det vesentlige avhengige av egne ressurser eller hjelp fra private tjenesteleverandører for å gjenopprette ordinær drift. NSM mottar varsler, koordinerer og varsler videre ved behov til regjeringen, relevante myndigheter og til virksomheter. Ugradert informasjon kan enkelt spres raskt. Det er samtidig viktig å sørge for en godt utbygget infrastruktur for å dele gradert informasjon.

Omfanget av NSMs oppgaver innen digital sikkerhet utenfor sikkerhetsloven bør reduseres. NSM betegnes i hovedinstruksen som «det nasjonale fagmiljøet for digital sikkerhet». Med et slikt utgangspunkt har det trolig vært lett å legge nye oppgaver på dette området til NSM. Men instruksen overvurderer direktoratets rolle; NSM er ett blant flere digitale fagmiljøer. Direktoratets oppgaver er nå for mange, og de favner for bredt. Det svekker NSMs kapasitet til å fylle funksjonen som sikkerhetsmyndighet etter sikkerhetsloven.

Oppgaver innen digital sikkerhet utenfor sikkerhetsloven bør overføres til andre. NSM bør fortsatt bidra, men ikke ha ansvaret for oppgavene. Kunnskap som NSM tilegner seg i arbeidet med oppgaver etter sikkerhetsloven, bør fortsatt tilflyte samfunnet.

NSM bør for eksempel ikke ha som oppgave å gi informasjon, råd og veiledning til statlig og kommunal sektor, private virksomheter og enkeltpersoner utenfor sikkerhetslovens virkeområde, drifte Norsk senter for informasjonssikring (NorSIS) eller vedlikeholde grunnprinsipper for IKT-sikkerhet. NSM bør heller ikke ha et hovedansvar for å koordinere aktiviteter som faller utenfor sikkerhetsloven.

Tilsvarende anbefaler utvalget at den frivillige ordningen for sertifisering av IT-sikkerhet i produkter og systemer (SERTIT) og oppgaven med å drifte deteksjonssystemet for falske basestasjoner tas ut av NSMs oppgaveportefølje og overføres til andre.

Det nye Digitaliserings- og forvaltningsdepartementet (DFD) bør ha et større ansvar for digital sikkerhet utenfor sikkerhetsloven. NSMs mange oppgaver innen digital sikkerhet har sammenheng med at Justis- og beredskapsdepartementet i 2013 fikk ansvaret for å samordne IKT-sikkerhet på sivil side. I samme år ble det samtidig vist til at ansvarsdelingen bør gås gjennom jevnlig i lys av den økende betydningen digital sikkerhet har i samfunnet. Vi mener tiden nå er inne for en slik gjennomgang.

DFD skal bidra til å styrke statens og samfunnets evne til å bruke potensialet og håndtere utfordringene som digital teknologi skaper. Departementet skal være en pådriver og samordne regjeringens politikk, også innen kunstig intelligens. Oppgaven DFD har med å vurdere hvilke muligheter digitalisering kan gi, bør ikke være løsrevet fra oppgaven med å vurdere hvilke konsekvenser disse mulighetene kan ha for den digitale sikkerheten. Det vil derfor etter utvalgets syn være riktig at dette departementet får som oppgave å samordne regjeringens arbeid med digital sikkerhet utenfor sikkerhetsloven. De oppgavene som utvalget foreslår tatt ut av NSM, bør legges til en eller flere etater under dette departementet.

NSM må prioritere ressursene riktig, ha god kommunikasjon internt og arbeide effektivt. På noen områder har aktører uttrykt misnøye med NSMs tjenester. Det er pekt

på at NSM bruker for lang tid på å gjennomføre tekniske sikkerhetsundersøkelser (TSU) og at NSM ikke har godkjent skjermingsverdige informasjonssystemer til tross for at direktoratets råd og veiledning var fulgt. Det siste kan skyldes for dårlig kommunikasjon mellom ulike avdelinger i NSM. Også behandling av klager på avslag om sikkerhetsklarering av personell har tatt for lang tid. For klagesaker innen personellsikkerhet er kravet fra Justis- og beredskapsdepartementet at minst 85 prosent av sakene skal behandles innen 90–120 dager. Det er for lenge å vente for de som berøres, og målet bør skjerpes.

NSM bør sette ut flere oppgaver til andre. Direktoratet er fagmyndighet, men utfører også selv flere oppgaver. Sikkerhetsloven og forskrifter åpner for at flere av oppgavene som NSM selv utfører, kan settes ut til andre. Denne muligheten bør brukes mer enn i dag.

Dette gjelder blant annet oppgaven med å gjennomføre tekniske sikkerhetsundersøkelser (TSU) som vist til ovenfor. Et system der NSM også godkjenner andre virksomheter som kan gi råd om slike undersøkelser, bør vurderes. Når NSM gjennomfører TSU selv, bør oppgavene prioriteres tilstrekkelig, og det må kunne tas betaling for full kostnad for arbeidet. Det vil gi brukere insentiv til nøye å vurdere behovet og slik også styrke sikkerheten. Egenbetaling vil kreve hjemmelsgrunnlag.

Ordningen for godkjenning av skjermingsverdige informasjonssystemer bør også vurderes. Slik godkjenning krever system- eller virksomhetsspesifikk kompetanse som kan være krevende for NSM å ha på alle områder. Framfor å godkjenne systemet, kan NSM vurdere om virksomheten er skikket etter kriterier som departementene har fastsatt. Det er viktig at NATO-krav ivaretas i et slikt revidert opplegg. NSM må fortsatt føre tilsyn i ettertid.

Også på flere andre områder bør de mulighetene som sikkerhetsloven og forskrifter gir til å sette ut oppgaver, nyttes mer enn i dag.

Flere tilsynsmyndigheter bør føre tilsyn etter sikkerhetsloven. NSM fører tilsyn med at sikkerhetsloven blir fulgt opp, både med departementene, etater, lokale myndigheter og virksomheter. I fem sektorer hittil har ansvarlig departement gitt oppgaven med å føre tilsyn etter sikkerhetsloven til myndigheten som fører tilsyn i sektoren. Dette er en god ordning som bør brukes i flere sektorer. Blant annet finanssektoren og helsesektoren er her egnede kandidater. NSM vil bli avlastet, og ansvarlig departement og etater vil få større bevissthet om arbeidet med forebyggende sikkerhet etter sikkerhetsloven.

Grensesnittet mot Direktoratet for samfunnssikkerhet og beredskap (DSB) *må bli klarere.* DSB bistår Justis- og beredskapsdepartementet med å koordinere arbeidet med samfunnssikkerhet og beredskap og har ledet arbeidet med å identifisere kritiske samfunnsfunksjoner. Det er et nasjonalt planleggingsgrunnlag for departementenes arbeid med samfunnssikkerhet og beredskap. Totalberedskapskommisjonen foreslo å slå sammen rammeverkene DSB og NSM arbeider etter, det vil si de kritiske samfunnsfunksjonene (KIKS) og de grunnleggende nasjonale

funksjonene (GNF), se nærmere omtale i boks 6.2.[4] Kommisjonen anbefalte også «å gjennomgå porteføljene til DSB og NSM for å avklare eventuelle uklare grensesnitt og oppgavefordeling».

Utvalget er enig i at det er overlapp mellom arbeidet med kritiske samfunnsfunksjoner og arbeidet med grunnleggende nasjonale funksjoner etter sikkerhetsloven. Sikkerhetstilstanden for GNF-ene vil påvirkes av sikkerhetstilstanden for de kritiske samfunnsfunksjonene. Rammeverkene bør likevel ikke slås sammen. De har både ulike formål og virkeområder, der arbeidet med kritiske samfunnsfunksjoner favner vesentlig videre enn sikkerhetsloven. Utvalget mener sikkerhetslovens formål og virkeområde i dag er hensiktsmessig og fungerer etter intensjonen.

Det er likevel behov for at formål og virkeområde og grensesnitt mellom rammeverkene gjøres klarere og formidles på en pedagogisk måte. Videre må oppgavefordeling og grensesnitt generelt mellom DSB og NSM avklares og gjøres tydelig i direktoratenes hovedinstrukser.

Arbeidet med nasjonal sikkerhet og arbeidet med samfunnssikkerhet vil overlappe også framover. Samarbeidet mellom NSM og DSB må derfor styrkes. De må være samstemte når de informerer og veileder om hvordan myndigheter og virksomheter skal håndtere ulike sårbarheter, hendelser og kriser.

Justis- og beredskapsdepartementet bør stille tydelige krav og gi retningslinjer for samhandling der oppgaver overlapper. Begge direktoratene må benytte etablerte arenaer for arbeidet med samfunnssikkerhet på nasjonalt, regionalt- og kommunalt nivå.

Klare grensesnitt er også viktig overfor andre myndigheter. Det gjelder blant annet i forholdet til Etterretningstjenesten og Politiets sikkerhetstjeneste (PST) og Forsvaret. Ansvarsdelingen mellom disse synes nå avklart.

Nasjonalt sikkerhetssenter (NCSC) i NSM og Nasjonalt cyberkrimsenter (NC3) i Kripos er begge sentrale i håndteringen av alvorlige IKT-sikkerhetshendelser. Samtidig har de til dels ulike roller. NSM bidrar til å gjenopprette berørte systemer og informerer andre virksomheter for å motvirke smitteeffekt. Kripos etterforsker hendelser for å avdekke hvem som står bak og informerer utad ved behov. Her kan det være ulike hensyn som kan krysse hverandre. Mens de berørte virksomhetene og NSM som oftest er opptatt av å få systemene raskt opp, kan Kripos ha behov for å avvente gjenoppretting for å etterforske og sikre bevis. Ulike hensyn vil avveies i «Felles cyberkoordineringssenter» (FCKS) der representanter fra NSM, Etterretningstjenesten, PST og Kripos deltar. Det er viktig at det er god kommunikasjon mellom aktørene og at de respekterer at hver av dem har ulike samfunnsoppdrag som skal ivaretas. En slik samhandling må ikke føre til at det kan stilles spørsmål ved om påtalemyndighetens uavhengighet hva gjelder etterforsking og påtaleavgjørelser, er ivaretatt eller utfordret.

[4] Se side 9 for definisjoner av «kritiske samfunnsfunksjoner» og «grunnleggende nasjonale funksjoner (GNF)».

NSMs funksjon som National Security Authority (NSA) overfor NATO, bør videreføres. Denne oppgaven må ses i sammenheng med oppgaven NSM har som sikkerhetsmyndighet etter sikkerhetsloven. I kontakten med NATO bør NSM trekke andre berørte etater og virksomheter med i forberedelsene og behandlingen av saker som følger av kontaktpunktfunksjonen. Direktoratet må dele informasjon fra møter i NATO med andre myndigheter som bør ha den. I den utstrekning det er hensiktsmessig og mulig, bør det åpnes for at andre deltar sammen med NSM på møter eller andre relevante fora i NATO-sammenheng.

Departementene må styre og finansiere NSM samordnet, helhetlig og langsiktig. Styringen av NSM synes i dag å være kortsiktig med nye oppdrag gjennom året i supplerende tildelingsbrev. Ulike hasteoppdrag til støtte for departementet i rollen som politisk sekretariat har også økt. Det gjør det mer krevende for NSM å planlegge og prioritere oppgaver og ressurser.

Departementene må være avholdne med å gi NSM flere oppgaver. Tildeling, oppdrag og styringsrammer bør med få unntak komme i de årlige tildelingsbrevene som sendes ut i desember og ikke spredt over året. Instrukser bør komme fra ett departement og være samordnet.

Dagens detaljerte hovedinstruks med en rekke «skal-punkter» gir lite rom for ledelsen til å planlegge og prioritere. En større vekt på mål og resultater vil legge et bedre grunnlag både for å kunne utvikle en kompetent organisasjon og for departementenes styringsdialog med etaten. Økonomireglementets krav om langsiktighet og planlegging må tillegges mer vekt i instruksen og i etterlevelsen av den.

NSM får nå orden på økonomien, men organisasjonen må utvikles planmessig med flerårig perspektiv. Direktoratets innspill til departementene om de årlige bevilgningene bør ta utgangspunkt i planer for fire til fem år fram i tid for hvordan organisasjonen skal utvikles. NSM bør være tidlig i inngrep med Forsvarets investeringsplaner slik at leveranser til ulike prosjekter kan planlegges i tid og omfang.

I en vurdering av departementstilhørighet for NSM må ulike hensyn avveies. Det er argumenter både for og mot dagens arbeidsfordeling mellom departementene. En faglig linje fra begge med ett som administrativt ansvarlig departement, bør videreføres. Justis- og beredskapsdepartementet har denne oppgaven i dag. Sivil sektor har fått økt betydning for nasjonal sikkerhet, samtidig som den sikkerhetspolitiske utviklingen kan tilsi at oppgavene framover i stor grad vil være på militær side. Forsvaret er allerede en stor bruker av tjenester fra NSM. Styringen fra departementene må være godt samordnet mellom dem uavhengig av hvor det administrative ansvaret ligger. Oppgavene må samsvare med tildelingene som gis, i tråd med bevilgningsreglement og økonomiregelverk. Samfunnsoppdraget og organisasjonen må utvikles videre ut fra et oppdatert risikobilde.

Utvalgets anbefalinger er budsjettnøytrale for staten samlet. Forslagene bidrar samtidig til å styrke det forebyggende arbeidet med nasjonal sikkerhet. Ved å konsentrere seg om sine kjerneoppgaver som fagmyndighet og tilsynsmyndighet etter sikkerhetsloven vil NSM lettere kunne planlegge og tilpasse ressursene der behovene forventes å bli størst. Dette vil også legge grunnlag for en mer effektiv virksomhet innenfor en realistisk budsjettering.

Overføring av oppgaver til andre vil gi redusert ressursbruk i NSM og tilsvarende økt arbeidsmengde hos de som overtar. Oppgaver som settes ut til markedsaktører eller som finansieres gjennom brukerbetaling, fører til mindre statlige utgifter. Utvalget antar at departementenes og etatenes arbeid med å fremme bruk av digitale verktøy og kunstig intelligens i offentlig sektor og næringsliv og avveie mot digital risiko, vil kunne kreve økte bevilgninger over tid.

Utvalgets anbefalinger kan oppsummeres på følgende måte:

Utvalget har tre hovedbudskap: i) Det bør fortsatt være én sikkerhetslov og én sikkerhetsmyndighet, ii) NSMs kjerneoppgaver bør være de som følger av sikkerhetsloven, og iii) NSM bør i større grad enn i dag nytte de mulighetene loven gir til å la andre utføre oppgaver.

I en usikker verden er behovet for forebyggende sikkerhetsarbeid blitt enda tydeligere. En koordinert innsats fra en rekke aktører er derfor nødvendig, der Nasjonal sikkerhetsmyndighet (NSM) har en plass.

Modellen med én sikkerhetslov og én sikkerhetsmyndighet bør videreføres.

NSMs kjerne bør være nasjonal sikkerhet etter sikkerhetsloven. Det nyopprettede Digitaliserings- og forvaltningsdepartementet med tilhørende etater bør få ansvar for å samordne arbeidet med digital sikkerhet utenfor sikkerhetsloven.

NSMs oppgaver etter sikkerhetsloven bør bli klarere.

NSM bør sette ut flere oppgaver som direktoratet i dag selv utfører.

Grensesnittet mot Direktoratet for samfunnssikkerhet og beredskap (DSB) må bli klarere. Departementet bør utforme retningslinjer for samhandlingen mellom dem. Hovedinstruksene må oppdateres og trekke grenser mellom direktoratene.

NSM og Nasjonalt cyberkrimsenter (NC3) må arbeide godt sammen, og Justis- og beredskapsdepartementet bør her stille klare krav om dette i instruksene.

Departementenes styring av NSM må være forutsigbar og langsiktig. NSM må følge kravene i statens økonomireglement om langsiktig planlegging.

2 Utvalgets mandat, sammensetning og arbeid

2.1 Mandat og sammensetning

Utvalget ble oppnevnt ved kongelig resolusjon 27. september 2024. Mandatet er gjengitt i boks 2.1.

Boks 2.1 **Mandat for ekstern gjennomgang av Nasjonal sikkerhetsmyndighets oppgaveportefølje**

1. Rustet for å håndtere fremtidens utfordringer?
Den sikkerhetspolitiske utviklingen, økningen i digitale angrep og en hurtig digital transformasjon har endret rammebetingelsene for arbeidet med forebyggende nasjonal sikkerhet. Er forvaltningen rustet for å håndtere det fremtidige risikobildet?

Justis- og beredskapsdepartementet og Forsvarsdepartementet starter derfor en ekstern gjennomgang for å vurdere om oppgaveporteføljen som ligger under NSMs ansvarsområde er organisert hensiktsmessig for å svare på fremtidens utfordringer. Et viktig resultat av en slik gjennomgang skal være å sikre at vi bruker nasjonens samlede ressurser effektivt for å ivareta forsvarlig sikkerhet på nasjonalt nivå, som svarer på fremtiden behov og en forventet økning i oppgavemengde.

2. Utgangspunkt i dagens oppgaver delegert til Nasjonal sikkerhetsmyndighet
Nasjonal sikkerhetsmyndighet (NSM) er faglig underlagt Justis- og beredskapsdepartementet (JD) og Forsvarsdepartementet (FD). JD har det administrative etatsstyringsansvaret. NSM har et tverrsektorielt ansvar og oppgaver på flere områder innen forebyggende nasjonal sikkerhet og øvrig digital sikkerhet, både på sivil side og for forsvarssektoren. Også andre statlige virksomheter har viktige roller innen områdene. Med utgangspunkt i oppgavene som i dag ivaretas av NSM, skal utvalget gjøre sine vurderinger. NSM har siden opprettelsen fått tilført nye oppgaver, fått utvidet ansvarsområdet blant annet gjennom et utvidet virkeområde på sikkerhetsloven, fått økte krav og forventninger og har betydelig dybde på enkelte fagområder i form av løpende produksjon. NSM er det nasjonale fagmiljøet for digital sikkerhet i sivil sektor.

Boks 2.1 forts.

3. Har vi en hensiktsmessig organisering av oppgaver, roller og ansvar?
NSMs viktige rolle i arbeidet med nasjonal sikkerhet gjør det nødvendig å foreta en helhetlig gjennomgang av oppgavene som er gitt til direktoratet i dag, samt en vurdering av om oppgavene er hensiktsmessige for å håndtere det fremtidige utfordringsbildet. NSM leverer viktige tjenester for både forsvarssektoren og sivil side, og ivaretar internasjonale krav og forventninger til Norge. Det er viktig at disse behovene også ivaretas i fremtiden. Forsvarssektoren står fremfor en stor økning i budsjetter og NSMs understøttelse i denne styrkingen er viktig. Sivile sektorers betydning for nasjonal sikkerhet er økende, og NSM har en nøkkelrolle i blant annet implementeringen av sikkerhetsloven og koordinerer håndteringen av digitale angrep.

4. Hva er fremtidens hensiktsmessige organisering av oppgaver, roller og ansvar?
Den sikkerhetspolitiske utviklingen, utviklingen i risikobildet med særlig betydning for nasjonal sikkerhet og ivaretagelsen av nasjonale sikkerhetsinteresser skal være førende for vurderingen.

Gitt denne bakgrunnen skal utvalget svare på følgende problemstillinger:
1. Etablere en oversikt over NSMs samlede portefølje og oppgaver.
2. Er dagens organisering av NSMs oppgaveportefølje hensiktsmessig innrettet?

   Herunder om:
   a. grensesnitt mot andre tilgrensede statlige virksomheter er tilstrekkelig avklart og ressurseffektivt organisert,
   b. oppgaveporteføljen er hensiktsmessig innrettet med tanke på at den er faglig underlagt både JD og FD.
   c. departementenes tverrsektorielle behov i arbeidet med nasjonal sikkerhet godt nok ivaretatt
   d. oppgaveporteføljen er fremtidsrettet, robust og ressurseffektivt innrettet
3. Hvordan bør oppgaveporteføljen lagt til NSM være organisert for å være fremtidsrettet, robust og ressurseffektivt innrettet i arbeidet med nasjonal sikkerhet?

5. Premisser og krav for arbeidet:
Gjennomgangen må ta utgangspunkt i sikkerhetslovens kapittel 2 om ansvar og myndighet for forebyggende sikkerhetsarbeid, herunder oppgaver som er beskrevet i tilhørende forskrifter og annet regelverks beskrivelser av oppgavene tillagt sikkerhetsmyndigheten, samt direktoratets hovedinstruks, slik at det vurdere av hvem, og hvordan, disse best kan ivaretas. Det er ikke et mål i seg selv å skille ut oppgaver fra NSM, men der noen av dagens oppgaver dupliseres eller av andre grunner kan utføres av andre på en mer hensiktsmessig og effektiv måte, så bør disse vurderes overført. Utvalget skal konsentrere opp-

Boks 2.1 forts.

merksomheten sin om de mest tilgrensede og eventuelt overlappene oppgavene med andre statlige virksomheter. Oppgaver som NSM gjør i dag, og som ikke kan relateres direkte til sikkerhetsloven skal også identifiseres, og vurderes overført til andre myndigheter. Det kan også være oppgaver som utføres av andre virksomheter som kan vurderes overført til NSM der dette vil bidra til å kraftsamle nasjonal innsats på viktige områder. Videre kan det være oppgaver som kan vurderes løst i partnerskap med næringslivet.

6. Arbeidet må videre hensynta at:

- Forslag til løsninger må hensynta at oppgaver, roller og ansvar for cybersikkerhet ivaretas tilstrekkelig,
- Det pågår en prosess for overføring av ansvar for klareringssaker i sivil sektor herunder fagmyndighetsoppgaver, fra NSM til Sivil klareringsmyndighet. Denne prosessen skal fortsette uavhengig av dette arbeidet.
- Det pågår et arbeid ledet av Digitalisering- og forvaltningsdepartementet, sammen med Justis- og beredskapsdepartementet, hvor regjeringen vil kartlegge brukerbehov og erfaringer med dagens organisering av veiledning innen digital sikkerhet. Dette for å vurdere oppgaver, ansvar og organisering, og om en kraftsamling av veiledningsmiljøer vil kunne gi effektiviseringsgevinster (iht Meld. St. 9 (2022–2023) s. 26). Denne prosessen skal fortsette uavhengig av dette arbeidet, og utvalget kan se hen til dette.
- Ivaretar forpliktelsene en nasjonal sikkerhetsmyndighet har overfor andre land og internasjonale organisasjoner, spesielt Norges forpliktelser til NATO må ivaretas i alle forslag til løsninger, samt en vurdering av hva som inngår i kontaktpunktfunksjonen til NATO og hvem som er nærmest til å ivareta denne,
- Gjennomgangen må sikre at behovet for samarbeid med andre land og internasjonale organisasjoner (særlig NATO og EU), med relevans for nasjonal sikkerhet, blir tilstrekkelig ivaretatt.
- Se hen til andre sammenlignbare lands organisering av arbeidet med forebyggende nasjonal sikkerhet,
- Være budsjettnøytral (skal ikke medføre økte drifts- eller investeringsutgifter)
- Synliggjøre eventuelle behov for justeringer i forskriftene til sikkerhetsloven og kgl. res som følge av eventuelle endringer i oppgavefordelingen,
- Arbeidet skal gjennomføres i tråd med utredningsinstruksen og følge veileder for utvalgsarbeid i staten.

Arbeidet gjennomføres av et eksternt utvalg ledet av Svein Gjedrem, med et lite sekretariat. JD og FD inngår i sekretariatsfunksjonen. Det skal legges opp til tett dialog med, og involvering av berørte aktører.

Arbeidet fra ekspertutvalget skal resultere i en ugradert rapport. Eventuelt gradert materiale utarbeides i separat(e) vedlegg. Rapporten skal leveres innen utgangen av mars 2025.

På forespørsel fra utvalget ble fristen endret til 9. april 2025.

Utvalget har hatt følgende sammensetning:

– Svein Gjedrem (leder), tidligere finansråd og sentralbanksjef
– Maria Bartnes, forskningssjef
– Tor-Aksel Busch, tidligere riksadvokat
– Haakon Bruun-Hanssen, tidligere forsvarssjef

Assisterende nasjonal sikkerhetsrådgiver i Sverige, Annika Brändström, var med i utvalget fram til den 30. januar 2025 da hun ble konstituert som nasjonal sikkerhetsrådgiver av den svenske regjeringen og derfor ikke lenger hadde mulighet til å delta. På dette tidspunktet var utvalget kommet så langt i sitt arbeid at det ble vurdert som uhensiktsmessig å anmode om oppnevnelse av et nytt medlem.

Sekretariatet har bestått av Yngvar Tveit (leder), Anders Bjønnes, Bente Lund Michaelsen, Njaal Segaard og Christina Smith-Erichsen.

2.2 Arbeidet i utvalget

2.2.1 Merknader til mandatet

Utvalgets mandat er gjengitt i boks 2.1. Utvalget skal vurdere om NSMs oppgaveportefølje er hensiktsmessig innrettet og hvordan NSM best kan bidra til arbeidet med forebyggende nasjonal sikkerhet. Oppgaveporteføljen skal vurderes blant annet i lys av at NSM er faglig underlagt både Justis- og beredskapsdepartementet og Forsvarsdepartementet.

I gjennomgangen av oppgaveporteføljen skal utvalget ta utgangspunkt i sikkerhetsloven kapittel 2 og vurdere om det er oppgaver som ikke følger direkte av loven som bør overføres til andre myndigheter eller løses i partnerskap med næringslivet. Utvalget skal vurdere om det er oppgaver som bør overføres fra andre til NSM. Grensesnittet mot andre myndigheter er her sentralt.

Norges internasjonale forpliktelser og samarbeid med andre land og organisasjoner må ivaretas. Utvalget skal beskrive hva som inngår i kontaktpunktfunksjonen til NATO og hvem som er nærmest til å ivareta denne oppgaven.

Utvalget skal synliggjøre eventuelle behov for justeringer i forskriftene til sikkerhetsloven som følge av utvalgets forslag. Forslagene skal være budsjettnøytrale.

I utvalgets mandat vises det til at det pågår en prosess for overføring av ansvar for klareringssaker i sivil sektor fra NSM til Sivil klareringsmyndighet, og at denne skal fortsette uavhengig av utvalgets arbeid. Personellsikkerhet er en sentral del av sikkerhetsmyndighetens ansvar etter sikkerhetsloven, og utvalget kan ikke unnlate å komme inn på denne problemstillingen i vurderingene.

I utvalgets mandat står det videre at det pågår et arbeid for å kartlegge brukerbehov og erfaringer med dagens organisering av veiledning innen digital sikkerhet. Denne prosessen skal ifølge mandatet fortsette uavhengig av utvalgets arbeid,

og «utvalget kan se hen til dette». Etter det utvalget erfarer har ikke arbeidet med denne kartleggingen kommet ordentlig i gang. Utvalget berører også dette området i våre forslag.

Utvalgets mandat omhandler NSMs oppgaver. Men oppgaver som foreslås tatt ut av NSM, må noen andre overta dersom de ikke skal opphøre. Utvalgets vurderinger kan ikke ses uavhengig av delingen av ansvar mellom departementene i arbeidet med å utvikle bruk av digitale verktøy og kunstig intelligens i det norske samfunn og forebygge risiko.

2.2.2 Utvalgets møter

Utvalget har hatt 15 møter i perioden 15. oktober 2024 til 3. april 2025, hvorav med en rekke aktører med berøringspunkter til NSM. Det var representanter for departementer, direktorater og tilsynsmyndigheter, næringslivsaktører, arbeidslivsorganisasjoner og akademikere som forsker på fagområdet. Utvalget har også møtt direktør for NSM og ledere av de ulike fagavdelingene i NSM.

Justis- og beredskapsdepartementet har det administrative ansvaret for NSM, mens ansvaret for den faglige etatsstyringen er delt mellom Justis- og beredskapsdepartementet og Forsvarsdepartementet. Utvalget har hatt møter med representanter fra begge.

Alle departementene er ansvarlige for forebyggende sikkerhetsarbeid innenfor egen sektor. Utvalget har hatt møter med representanter fra Digitaliserings- og forvaltningsdepartementet, Energidepartementet og Utenriksdepartementet.

NSM er en av Etterretnings-, overvåknings- og sikkerhetstjenestene (EOS-tjenestene). Utvalget har hatt møter med lederne av Etterretningstjenesten og Politiets sikkerhetstjeneste (PST) som utgjør de øvrige EOS-tjenestene ved siden av NSM. Utvalget har også møtt daværende leder av Stortingets Kontrollutvalg for EOS-tjenestene (EOS-utvalget) og direktøren for sekretariatet.

NSM var del av Forsvaret før det ble et eget direktorat i 2003. Forsvaret er fortsatt en stor bruker av NSMs tjenester. Utvalget har møtt Forsvaret ved forsvarssjefen.

Videre har utvalget møtt daværende leder i Politidirektoratet og ledelsen i Kripos. Både NSM og Kripos ved Nasjonalt cyberkrimsenter (NC3) har oppgaver blant annet i håndteringen av digitale hendelser.

NSM har grenseflater til flere andre direktorater og tilsynsmyndigheter i arbeidet med forebyggende sikkerhet. Utvalget har møtt representanter fra Direktoratet for samfunnssikkerhet og beredskap (DSB), Direktoratet for eksportkontroll og sanksjoner (DEKSA), Digitaliseringsdirektoratet (Digdir), Norges vassdrags- og energidirektorat (NVE), Havindustritilsynet (Havtil), Nasjonal kommunikasjonsmyndighet (Nkom) og Finanstilsynet. Alle de ovennevnte myndighetene bortsett fra Finanstilsynet er pekt ut som tilsynsmyndighet for å følge opp sikkerhetsloven. Det er ansvarlig departement som peker ut sektortilsyn etter sikkerhetsloven i egen sektor.

Departementene er også ansvarlige for å peke ut virksomheter som skal underlegges sikkerhetsloven. Dette er virksomheter som har vesentlig betydning for

såkalte grunnleggende nasjonale funksjoner eller som har aktiviteter eller råder over informasjon, infrastruktur el. som har avgjørende betydning for nasjonale sikkerhetsinteresser. Utvalget har møtt representanter fra Equinor, Gassco, Telenor Norge og BITS AS. Utvalget har også møtt representanter fra Norges Bank.

Innen digital sikkerhet er både NSM og andre myndigheter og virksomheter avhengige av tjenester fra private sikkerhetsleverandører, både i det forebyggende sikkerhetsarbeidet og ved håndtering av hendelser som oppstår. Utvalget har møtt leder av selskapet mnemonic. Utvalget har også hatt møte med ledelsen av Norwegian Cybersecurity Cluster som er et samarbeidsorgan for norske foretak som tilbyr tjenester innen digital sikkerhet til offentlig og privat næringsliv, akademia og offentlig forvaltning.

Utvalget har videre hatt møter med arbeidslivsrepresentanter både på arbeidsgiver- og arbeidstakersiden. Fra arbeidstakersiden har utvalget møtt fagforeninger i NSM, samt Politiets Fellesforbund og Flygeledernes forening. Fra arbeidsgiversiden har utvalget møtt leder av Næringslivets sikkerhetsråd (NSR).

Fra akademia har utvalget hatt møte med to professorer ved Institutt for sikkerhet, økonomi og planlegging ved Universitetet i Stavanger.

Videre har utvalget møtt med tidligere direktør Frode Forfang som i oppdrag fra Justis- og beredskapsdepartementet utreder oppgavefordelingen innenfor personellsikkerhet.

I vedlegg 3 er representantene fra de ulike institusjonene som utvalget har møtt, listet opp.

2.2.3 Utredningens videre oppbygging

Utvalget beskriver hvordan det forebyggende sikkerhetsarbeidet er organisert og utføres i dag.

I kapittel 3 beskrives NSMs historie, hvor direktoratet kommer fra og hva som var bakgrunnen for opprettelsen i 2003. NSMs historie sammenfaller i stor grad i tid med sikkerhetslovens historie. Gjeldende sikkerhetslov er en lov om nasjonal sikkerhet som omfatter statssikkerhet og delen av samfunnssikkerheten, jf. boks 3.1.

I kapittel 4 omtaler vi NSMs oppgaver i dag. Vi identifiserer hvilke av oppgavene som følger av sikkerhetsloven og hvilke som faller utenfor denne loven.

NSM er administrativt underlagt Justis- og beredskapsdepartementet, men faglig underlagt både Justis- og beredskapsdepartementet og Forsvarsdepartementet. Utvalget har i kapittel 5 beskrevet hvordan styringen av NSM er innrettet og hvordan NSM finansieres.

Videre har utvalget i kapittel 6 omtalt andre statlige myndigheter som har grenseflater mot NSM. Vi beskriver hvordan de er tilgrenset, om oppgavene glir over i hverandre og hvordan arbeidsdelingen er regulert.

I kapittel 7 er Norges internasjonale forpliktelser og hva som inngår i kontaktfunksjonen til NATO beskrevet. Arbeid med forebyggende sikkerhet i utvalgte andre land omtales deretter i kapittel 8. Utvalget har sett nærmere på organiseringen i Sverige, Danmark, Finland, Nederland, USA og Storbritannia.

Utvalgets anbefalinger skal ifølge mandatet ivareta at NSMs oppgaver er «fremtidsrettet, robust og ressurseffektivt innrettet i arbeidet med nasjonal sikkerhet». Utvalget har mottatt en beskrivelse av risikobildet og mulige trusler fremover fra Justis- og beredskapsdepartementet og Forsvarsdepartementet som er gjengitt i kapittel 9.

Utvalgets vurderinger følger så i kapittel 10.

3 Nasjonal sikkerhetsmyndighet – bakgrunn og historie

Vi kan skille mellom funksjonen nasjonal sikkerhetsmyndighet og direktoratet Nasjonal sikkerhetsmyndighet.[5] Funksjonen nasjonal sikkerhetsmyndighet fulgte blant annet av NATOs krav overfor medlemslandene om å ha en såkalt *National Security Authority* (NSA) med ansvar for å ivareta sikkerheten for NATO-gradert informasjon.[6] Denne funksjonen ble tidligere ivaretatt av Forsvarssjefens Sikkerhetsstab ved Forsvarets Overkommando (FO/S). Da direktoratet Nasjonal sikkerhetsmyndighet (NSM) ble opprettet 1. januar 2003, ble denne funksjonen overført til det nye direktoratet.

Oppgavene som inngår i funksjonen nasjonal sikkerhetsmyndighet, følger av sikkerhetsloven og forskrifter med hjemmel i loven. Direktoratet Nasjonal sikkerhetsmyndighet har i tillegg fått flere andre oppgaver, dels ved etableringen i 2003 og dels senere. Utvalgets mandat har vært å vurdere oppgavene til direktoratet. Når vi i utredningen skriver Nasjonal sikkerhetsmyndighet eller NSM, mener vi derfor direktoratet.

Dette kapittelet gir et kort overblikk over NSMs historie.[7] I senere kapitler blir ulike sider ved NSM beskrevet mer utdypende.

3.1 Defensivt sikkerhetsarbeid

Før andre verdenskrig var det ikke et defensivt forebyggende sikkerhetsarbeid som dekket flere sektorer i Norge. Det begynte først å ta form under andre verdenskrig da Forsvarets ledelse i London utviklet en etterretnings- og sikkerhetstjeneste. Her inngikk også den nasjonale chiffertjenesten, eller dagens kryptotjeneste, som så vidt var startet opp før krigsutbruddet. Det var viktig både å verne mot fiendtlig infiltrasjon fra flyktningestrømmer og å opprettholde diskresjon som deltakere i de alliertes krigsplanlegging.

Etter krigen ga medlemskapet i NATO i 1949 forpliktelser i det forebyggende sikkerhetsarbeidet, blant annet ved at NATOs hemmeligheter måtte vernes om. Kort tid etter ble det fastsatt en sikkerhetsinstruks for å beskytte sikkerhetsgradert informasjon. Denne var gjeldende for både Forsvaret og enkelte sivile sektorer som

[5] Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet (sikkerhetsloven),* side 166.

[6] NATO Security Policy C-M, (2002) 49. Dette er beskrevet i blant annet NOU 2016: 19 *Samhandling for sikkerhet — Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid,* side 138–140.

[7] Historien før opprettelsen i 2003 er beskrevet i doktoravhandlingen til Hans Morten Synstnes fra 2015 *«Den innerste sirkel. Den militære sikkerhetstjenesten 1945–2002»*. Denne ble utgitt som bok med samme tittel året etter.

det var forventet at skulle støtte Forsvaret i sikkerhetspolitiske konflikter og krig. Slik gjensidig støtte mellom forsvarssektoren og det sivile samfunnet i fred, krise og krig betegnes gjerne som totalforsvaret.[8] Forsvarets sikkerhetsmiljø ble gitt i oppgave å veilede om instruksen og føre tilsyn med at den ble fulgt opp. Det ble også opprettet en egen stilling som sikkerhetsinspektør som skulle følge opp den nye instruksen.

Sikkerhetsinstruksen ble revidert i 1962. Virkeområdet ble da noe utvidet ved at den ble gjort gjeldende for hele statsforvaltningen. I 1965 ble Forsvarets sentrale sikkerhetsledd og oppgaven med å følge opp sikkerhetsinstruksen plassert i en selvstendig sikkerhetsstab i Forsvarsstaben. Denne staben ble i 1970 en del av Forsvarets overkommando med forkortelsen FO/S.

Perioden 1965-1990 var en tid preget av faglig og regelverksteknisk utvikling innenfor ulike fagdisipliner. Kjernen i regelverket var sikkerhetsinstruksen med graderingsnivåene BEGRENSET, KONFIDENSIELT, HEMMELIG og STRENGT HEMMELIG. I 1972 ble det i tillegg til sikkerhetsinstruksen formulert en egen beskyttelsesinstruks som ga regler for sikring av informasjon som skulle beskyttes av andre grunner enn de som var dekket av sikkerhetsinstruksen og med graderingene FORTROLIG og STRENGT FORTROLIG. FO/S fulgte opp også denne. Det ble etter hvert gitt supplerende direktiver innen datasikkerhet til støtte for begge instruksene.

I 1996 ble Forsvarets ansvar for sikkerhetsarbeidet i FO/S vurdert i lys av arbeidet som pågikk med ny sikkerhetslov. Det ble lagt opp til at loven ikke lenger bare skulle handle om å motvirke spionasje gjennom hemmelighold av gradert informasjon på tvers av sektorene, men også legge til rette for å motvirke sabotasje og terrorhandlinger ved å beskytte såkalte skjermingsverdige objekter. Dette ville gi et utvidet nedslagsfelt for loven, særlig på sivil side av samfunnet. Det var også et ønske at kompetansen som var blitt utviklet i FO/S, i større grad kunne komme også andre deler av samfunnet til gode. Dessuten ble det reist prinsipielle motforestillinger mot at forsvarssjefen kunne fortsette å være ansvarlig for tilsynet med sikkerhetsarbeidet da dette i stor grad var å føre tilsyn med sin egen etat. En solid forbindelse til forsvarssektoren var likevel fortsatt viktig for utviklingen av nye sikkerhetsløsninger.

3.2 Nasjonal sikkerhetsmyndighet opprettes

Regjeringen Stoltenberg foreslo i 2000 at Nasjonal sikkerhetsmyndighet (NSM) skulle opprettes som et eget direktorat direkte underlagt Forsvarsdepartementet.[9] Det ble blant annet vist til at ansvaret som sikkerhetsloven la til nasjonal sikkerhetsmyndighet, kunne tilsi at funksjonen ble organisert utenfor Forsvarets militære organisasjon. En overføring av ressurser fra sikkerhetsstaben ved Forsvarets overkommando (FO/S) ville «sikre en effektiv styring og en god kontroll med den forebyggende sikkerhetstjeneste».[10]

[8] Prop. 87 S (2023–2024) *Forsvarsløftet – for Norges trygghet. Langtidsplan for forsvarssektoren 2025–2036*, side 48.

[9] St.prp. nr. 45 (2000–2001) *Omleggingen av Forsvaret i perioden 2002–2005 , side 172–173.*

[10] Ibid, side 173.

Forslaget bygget på anbefalinger både fra interne arbeidsgrupper i Forsvarsdepartementet og utredninger fra henholdsvis Forsvarspolitisk utvalg og Sårbarhetsutvalget.[11] Sistnevnte utvalg foreslo også at det burde opprettes et eget departement med ansvar for sikkerhet og beredskap som blant annet skulle ha ansvar for det nye direktoratet.

Stortingets forsvarskomité ba i sin innstilling regjeringen komme tilbake til saken i den kommende stortingsmeldingen om samfunnssikkerhet.[12]

Regjeringen Bondevik II uttalte i 2002 blant annet følgende til Stortinget:[13]

> «Nasjonal sikkerhetsmyndighet skal ha ansvar for forebyggende sikkerhetstjeneste etter sikkerhetsloven i sivil og militær sektor. Det vil sikre en helhetlig tilnærming til sikkerhetsarbeidet på tvers av militær og sivil sektor, og sikre en effektiv utnyttelse av ressursene innenfor forebyggende sikkerhet. Etter regjeringens oppfatning tilsier imidlertid Nasjonal sikkerhetsmyndighets ansvarsområde, særlig innenfor sivil sektor, at Nasjonal sikkerhetsmyndighet organiseres utenfor Forsvarets militære organisasjon. Det anses i den sammenheng som naturlig og hensiktsmessig at Nasjonal sikkerhetsmyndighet etableres som et direktorat rett under et fagdepartement. Regjeringen går inn for at Nasjonal sikkerhetsmyndighet skal opprettes som et eget direktorat administrativt underlagt Forsvarsdepartementet. Videre legges det opp til at Nasjonal sikkerhetsmyndighet skal rapportere (med faglig ansvarslinje) i militær sektor til Forsvarsdepartementet, og til Justisdepartementet i sivil sektor.»

Flertallet i en sammenslått justis- og forsvarskomite «merket seg at NSM er faglig underlagt Forsvarsdepartementet, men rapporterer til Forsvarsdepartementet i militær sektor og Justisdepartementet i sivil sektor. Flertallet vil påpeke viktigheten av klare kommandolinjer og ansvarsforhold».[14] Mindretallet støttet å opprette direktoratet, men mente at direktoratet administrativt burde legges under Justisdepartementet.

Regjeringen foreslo på denne bakgrunn å opprette Nasjonal sikkerhetsmyndighet (NSM) som eget direktoratet administrativt underlagt Forsvarsdepartementet fra 1. januar 2003. Direktoratet skulle ha en faglig rapporterings- og ansvarslinje til Justisdepartementet i saker på sivil side av samfunnet. Sikkerhetsstaben (FO/S) ved Forsvarets Overkommando ble samtidig foreslått avviklet:[15]

> «Organiseringen av NSM innebærer at FO/S nedlegges, og at hoveddelen av de ressurser som ligger i FO/S i dag overføres til det nye direktoratet. Forsvarets militære organisasjon må imidlertid beholde en egen sikkerhetskompetanse og kapasitet på sentralt nivå, som skal ivareta sikkerhetstjenesten i Forsvaret. Det opprettes derfor en forsvarssjefens sikkerhetsavdeling (FSA). FSA skal være operativ samtidig med opprettelsen av det nye direktoratet.»

[11] NOU 2000: 20 *Et nytt forsvar* og NOU 2000: 24 *Et sårbart samfunn*.

[12] Innst. S. nr. 342 (2000–2001), side 60.

[13] St.meld. nr. 17 (2001–2002) *Samfunnssikkerhet – Veien til et mindre sårbart samfunn*, side 103.

[14] Innst. S nr. 9 (2002–2003), side 44.

[15] St.prp. nr. 1 (2002–2003) for budsjettåret 2003 under Forsvarsdepartement*et*, side 30 og Innst. S. nr. 7 (2002–2003) , side 20.

NSM overtok lokalene til FO/S i Kolsås leir, mens Forsvarets sikkerhetsavdeling (FSA) fikk lokaler på Akershus festning. Ansvar for forebyggende sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet ble nedfelt i en egen forskrift.[16] NSM skulle ivareta de utøvende funksjonene for den forebyggende sikkerhetstjenesten på vegne av justisministeren og forsvarsministeren.

Sikkerhetsloven av 1998 definerte en kjerne for NSMs ansvar og oppgaver. Loven var nokså ny, og NSMs oppgave var å bidra til at den ble fulgt opp. Direktoratet fikk i tillegg også med seg enkelte tilgrensende oppgaver som kunne sies å være av tverrsektoriell karakter, se omtale i kapittel 4. FSA fikk de rent etatsinterne oppgavene som til da hadde ligget i FO/S, herunder å være forsvarssjefens rådgiver og utøvende organ i Forsvarets arbeid med sikkerhet.

Etter 2001 er sikkerhetsloven blitt endret på avgrensede områder i 2005, 2008 og 2016. I 2018 ble loven revidert fullt ut, blant annet på bakgrunn av anbefalinger fra Sikkerhetsutvalget.[17] Revisjonene av sikkerhetsloven ble i lovproposisjonen begrunnet med blant annet følgende:[18]

> «Risiko- og trusselbildet er mer sammensatt enn tidligere, med store teknologiske, demografiske og sikkerhetsmessige endringer. Begrepet samfunnssikkerhet er derfor tatt i bruk og har de siste årene fått stadig større fokus i samfunnsplanleggingen. Samfunnssikkerhet må ses i nær sammenheng med statssikkerhetsbegrepet. Dette har gitt behov for en helhetlig vurdering og nytenkning med hensyn til lovregulering av forebyggende nasjonalt sikkerhetsarbeid.»

Ny sikkerhetslov skulle legge grunnlag for at «vi har de virkemidlene som er nødvendige for å ivareta nasjonale sikkerhetsinteresser og forebygge mot sikkerhetstruende virksomhet».[19] Lovens virkeområde er å ivareta «nasjonal sikkerhet», som omfatter den tradisjonelle statssikkerheten og den delen av samfunnssikkerhet som er av vesentlig betydning for statens evne til å ivareta nasjonale sikkerhetsinteresser, se avsnitt 3.3 og boks 3.1. Loven trådte i kraft 1. januar 2019.

Like etter at ny lov trådte i kraft, overførte regjeringen Solberg det administrative ansvaret for NSM fra Forsvarsdepartementet til Justis- og beredskapsdepartementet. Det ble lagt opp til at NSM fortsatt skulle ha en faglig linje til Forsvarsdepartementet, og dette departementet har fortsatt instruksjonsmyndighet i saker som direktoratet arbeider med for forsvarssektoren.

NSM har også oppgaver utenfor sikkerhetsloven, og disse har økt i omfang over tid. Dette er nærmere omtalt i kapittel 4. Oppgaven med å følge opp beskyttelsesinstruksen falt bort ved etableringen av direktoratet.

---

[16] Kronprinsregentens resolusjon 4. juli 2003 nr. 900, *Fordeling av ansvar for forebyggende sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet*.

[17] NOU 2016: 19 *Samhandling for sikkerhet*.

[18] Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)*, side 10.

[19] Ibid, side 10.

Boks 3.1 Definisjoner av viktige begreper

Definisjonene er hentet fra sikkerhetsloven og Meld. St. 5 (2020–2021) *Samfunnssikkerhet i en usikker verden*.

Nasjonal sikkerhet defineres som statssikkerhet og en avgrenset del av samfunnssikkerhet som er av vesentlig betydning for statens evne til å ivareta nasjonale sikkerhetsinteresser.

Statssikkerhet er å ivareta statens eksistens, suverenitet, territorielle integritet og politiske handlefrihet.

Samfunnssikkerhet handler om samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slike hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil eller bevisste handlinger.

De nasjonale sikkerhetsinteressene er i sikkerhetsloven § 1-5 definert som «landets suverenitet, territorielle integritet og demokratiske styreform og overordnede sikkerhetspolitiske interesser knyttet til

a. de øverste statsorganers virksomhet, sikkerhet og handlefrihet
b. forsvar, sikkerhet og beredskap
c. forholdet til andre stater og internasjonale organisasjoner
d. økonomisk stabilitet og handlefrihet
e. samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet».

Grunnleggende nasjonale funksjoner er i henhold til sikkerhetslovens § 1-5 tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser.

Skjermingsverdige objekter og infrastruktur er ifølge sikkerhetsloven § 7-1 skjermingsverdige dersom det kan skade grunnleggende nasjonale funksjoner om de får redusert funksjonalitet eller blir utsatt for skadeverk, ødeleggelse eller rettsstridig overtakelse, eller kan skade nasjonale sikkerhetsinteresser på annen måte. Følgende klassifiseringsgrader skal benyttes; MEGET KRITISK, KRITISK og VIKTIG.

Skjermingsverdige informasjonssystemer er ifølge sikkerhetsloven § 6-1 skjermingsverdige dersom de behandler skjermingsverdig informasjon, eller dersom det i seg selv har avgjørende betydning for grunnleggende nasjonale funksjoner eller for nasjonale sikkerhetsinteresser.

Skjermingsverdige verdier brukes som en samlebetegnelse på skjermingsverdige objekter, infrastruktur og eller informasjonssystemer.

Boks 3.1 forts

Informasjon er ifølge sikkerhetsloven § 5-1 **skjermingsverdig** dersom det kan skade nasjonale sikkerhetsinteresser hvis informasjon blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.

Informasjon er ifølge sikkerhetsloven § 5-3 **sikkerhetsgradert** dersom det kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende. Følgende sikkerhetsgrader skal benyttes: STRENGT HEMMELIG, HEMMELIG, KONFIDENSIELT og BEGRENSET.

Kritiske samfunnsfunksjoner er funksjoner som er nødvendige for å ivareta befolkningens og samfunnets grunnleggende behov og befolkningens trygghetsfølelse. Grunnleggende behov er definert som «mat, vann, varme, trygghet og lignende». Kritiske samfunnsfunksjoner konkretiseres i såkalte «kapabiliteter».

Kapabilitet med tilhørende definert funksjonsevne uttrykker hvilke tjenester og leveranser som må opprettholdes for at grunnleggende behov skal være ivaretatt.

Kritisk infrastruktur er anlegg og systemer som er nødvendige for å opprettholde kritiske samfunnsfunksjoner.

Sikkerhetstruende virksomhet er i sikkerhetslovens § 1-5 definert som tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser.

Forebyggende sikkerhetsarbeid er i henhold til sikkerhetslovens § 1-5 å planlegge, tilrettelegge, gjennomføre og kontrollere forebyggende tiltak mot sikkerhetstruende virksomhet og følger av slik virksomhet.

3.3 Sikkerhetsloven 2018 og begrepet nasjonal sikkerhet

Sikkerhetsloven 1998 omhandlet i hovedsak statssikkerhet, det vil si beskyttelse av rikets selvstendighet og sikkerhet. I lovproposisjonen til gjeldende sikkerhetslov er det vist til at endringene i samfunnet siden 1998 har gjort det stadig vanskeligere å trekke en klar grense mellom statssikkerhet og samfunnssikkerhet.[20] Blant annet bidrar såkalte hybride trusler til at det er vanskelig å spore og dokumentere hvilke aktører som står bak et angrep. I tillegg er det vist til at grenselinjene mellom stats- og samfunnssikkerhet viskes ut i takt med at virksomhetene i de ulike samfunnssektorene er blitt mer og mer avhengige av hverandre. Videre står det i lovproposisjonen:

> «Som en konsekvens av disse forholdene er det etter departementets vurdering nødvendig å tilpasse lovens nedslagsfelt til den virkeligheten vi befinner oss i. I lovproposisjonen foreslås det derfor at lovens formål bør være å trygge *nasjonale sikkerhetsinteresser*. Dette vil i praksis innebære en utvidelse av lovens formål til å gjelde mer enn bare statssikkerhet i snever forstand. Samtidig vil departementet understreke at loven ikke skal være en bred samfunnssikkerhetslov.»

Det understrekes i proposisjonen at lovendringene «innebærer en begrenset utvidelse av lovens virkeområde». Sikkerhetslovens formål er etter § 1-1 å «å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser» og å «forebygge, avdekke og motvirke sikkerhetstruende virksomhet […]».

De tre sikkerhetsinteressene «Norges suverenitet, territorielle integritet og demokratiske styreform» utgjør ifølge lovproposisjonen ikke en uttømmende liste, og ved å innføre begrepet «nasjonale sikkerhetsinteresser» mente departementet å gjøre dette tydeligere.

Disse kategoriene er så i lovens § 1-5 delt inn i fem underkategorier, der punktene a. – c. ifølge departementet faller innenfor begrepet «statssikkerhet»:

a. de øverste statsorganers virksomhet, sikkerhet og handlefrihet
b. forsvar, sikkerhet og beredskap
c. forholdet til andre stater og internasjonale organisasjoner
d. økonomisk stabilitet og handlefrihet
e. samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet

Departementet understreket at totalforsvaret er grunnleggende for «nasjonens evne til militær respons» og at Forsvaret er «direkte avhengig av sivile innsatsfaktorer som elektronisk kommunikasjon (ekom), kraftforsyning, transport, drivstofforsyning, helse og tilførsel av vann og mat». Til § 1-5 punkt 1 bokstav e står det blant annet i proposisjonen:

[20] Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)*, side 32 og 33.

> «Sikkerhetsloven skal trygge nasjonale sikkerhetsinteresser, mens det er andre lover som skal sikre den sivile samfunnssikkerheten. Etter departementets vurdering vil det likevel også være behov for å omfatte infrastruktur og tjenester som anses som avgjørende for at sivilsamfunnet skal kunne fungere på en slik måte at øvrige nasjonale sikkerhetsinteresser kan ivaretas. Særlig vil dette kunne gjelde infrastruktur og tjenester som ikke anses å understøtte Forsvaret direkte, jf. bokstav b, men som likevel er viktig for nasjonens samlede beredskap og forsvarsevne. […]»

Loven gjelder i henhold til sikkerhetsloven § 1-3 for statlige, fylkeskommunale og kommunale organer, leverandører av sikkerhetsgraderte anskaffelser og virksomheter som har vesentlig betydning for grunnleggende nasjonale funksjoner, eller har aktiviteter eller råder over informasjon, infrastruktur el. som har avgjørende betydning for nasjonale sikkerhetsinteresser. Grunnleggende nasjonale funksjoner er i sikkerhetsloven § 1-5 punkt 2 definert som «tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser».

Det er de enkelte departementene som er ansvarlige for forebyggende sikkerhetsarbeid innenfor sine ansvarsområder. Departementene skal identifisere hva som er grunnleggende nasjonale funksjoner (GNF) og hvilke virksomheter som har vesentlig betydning for slike funksjoner. Det er videre departementenes oppgave å fatte vedtak etter sikkerhetsloven § 1-3 om hvilke virksomheter som skal underlegges sikkerhetsloven. Lovens virkeområde er på denne måten «ment å kunne utøves fleksibelt og dynamisk».

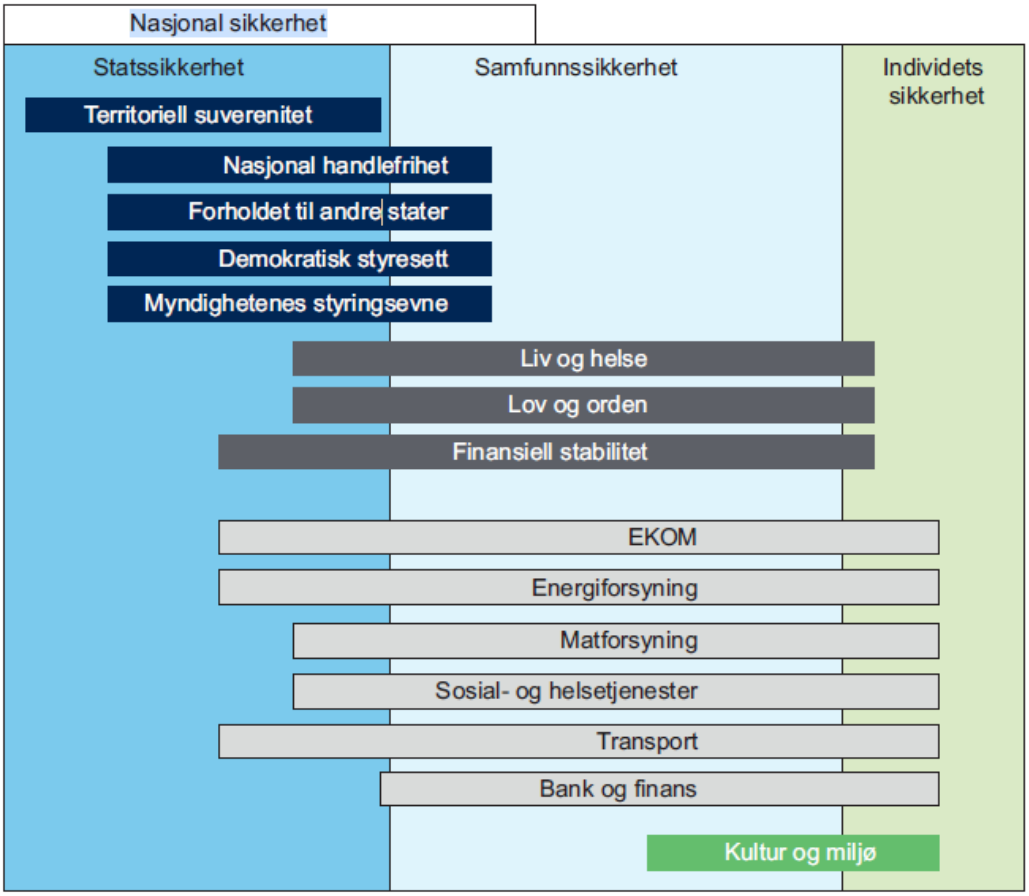
Sikkerhetsloven ble i 2023 endret på enkelte punkter.[21] Lovens virkeområde ble utvidet slik at også virksomheter som er av avgjørende betydning for nasjonale sikkerhetsinteresser skal underlegges hele eller deler av loven, selv om virksomheten ikke understøtter en grunnleggende nasjonal funksjon. Utvidelsen var ifølge lovproposisjonen ment å fange opp «de unntaksvise tilfellene der en virksomhet driver en aktivitet eller råder over verdier som har avgjørende betydning for nasjonale sikkerhetsinteresser, men ikke direkte understøtter en identifisert grunnleggende nasjonal funksjon.»[22] Som eksempler vises det til virksomheter som har rettigheter til eller arbeider med forskning og utvikling innen områder som kan utnyttes til sikkerhetstruende virksomhet av fremmede stater, som for eksempel kunstig intelligens eller avansert overvåkningsteknologi.

Figur 3.1 er hentet fra forarbeidene til sikkerhetsloven og skal illustrere at nasjonal sikkerhet omfatter statssikkerhet og deler av samfunnssikkerheten. Figuren skal videre illustrerer hvorvidt utvalgte sentrale nasjonale funksjoner og interesser understøtter statssikkerhet eller samfunnssikkerhet. Det understrekes i proposisjonen at det er krevende å plassere de enkelte funksjonene og at de fleste vil kunne berøre både stats- og samfunnssikkerheten.

[21] Prop. 95 L (2022–2023) *Endringer i sikkerhetsloven (eierskapskontroll og lovens virkeområde)*.

[22] Ibid., side 32 og 58.

Figur 3.1 Nasjonal sikkerhet, statssikkerhet og samfunnssikkerhet



Kilde: Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)*, Figur 6.2, side 38.

Figuren er en forenkling, men kan bidra til forståelse dersom den tolkes med varsomhet. Figuren kan trolig raffineres ved for eksempel å inkludere «virksomheters sikkerhet» i tillegg til «individets sikkerhet» som en kategori. Videre kan det alltid stilles spørsmål ved om det bør tas med flere kategorier eller om plasseringene av dem. Noen vil kunne mene at bank og finans burde strekke seg like langt inn i statssikkerhet som transport, mens andre vil kunne mene at kultur og miljø har fått for liten betydning. Dette bildet vil være å forvente at endres da arbeidet med å identifisere de grunnleggende nasjonale funksjoner har kommet lenger og at det senere er gjort endringer i definisjonen av hva som skal til for å kunne utpekes som skjermingsverdig.

Boks 3.2 Begreper om sikkerhet

Det finnes mange begreper om sikkerhet. Begrepene kan med sikkerhetsloven som utgangspunkt inndeles i ulike kategorier.

Den første kategorien er begreper utledet av hvilke **verdier** som skal sikres. Innen rammen av sikkerhetsloven snakker vi da om informasjonssikkerhet, informasjonssystemsikkerhet og objekt- og infrastruktursikkerhet.

Den andre kategorien er begreper utledet av hvilke **sårbarheter** som skal reduseres gjennom tiltak. Her er ikke sikkerhetsloven like dekkende, og flere av begrepene stammer fra fagmiljøenes tradisjonelle bruk. Dette kan være fysisk sikkerhet, personellsikkerhet, sikkerhetsstyring eller organisatorisk sikkerhet, og digital sikkerhet. Digital sikkerhet kan igjen være delt i systemsikkerhet, kommunikasjonssikkerhet, kryptosikkerhet, avlyttingssikkerhet og strålingssikkerhet (TEMPEST). Innen sikkerhetsstyring har vi dokumentsikkerhet, administrativ kryptosikkerhet og eierskapssikkerhet.

De enkelte områdene i denne andre kategorien kan gå litt over i hverandre. Avlyttingssikkerhet kan for eksempel ha en digital dimensjon, men også en fysisk dimensjon. Begreper kan også endre seg over tid. Digital sikkerhet har gjennom årene hatt mange betegnelser: EDB-sikkerhet, Datasikkerhet, IT-sikkerhet og IKT-sikkerhet. Vi har også begreper som er sammensatt av engelsk og norsk, som for eksempel cybersikkerhet. Det brukes som synonym til digital sikkerhet.

I tillegg til disse to hovedkategoriene kommer en tredje litt løseligere forankret kategori som omfatter samlebegreper som ikke lar seg innpasse i de to ovenfor. Det gjelder for eksempel industrisikkerhet som i sikkerhetsloven er omtalt som sikkerhetsgraderte anskaffelser. Det handler om tiltak for å redusere sårbarheter ved oppdrag til private som får tilgang til skjermingsverdige verdier. Kategorien omfatter personellsikkerhet, eierskapssikkerhet, fysisk sikkerhet, dokumentsikkerhet mv. Et annet eksempel er romsikkerhet. Begrepet betegner alt sikkerhetsarbeid som brukes for å ivareta sikkerheten i romrelatert virksomhet.

Boks 3.3 Om offensivt og defensivt sikkerhetsarbeid

NSMs oppdrag er på nasjonalt nivå å legge forholdene til rette og følge opp arbeidet med «defensiv forebyggende sikkerhet». Defensiv sikkerhet i henhold til sikkerhetsloven er å beskytte nasjonale sikkerhetsinteresser mot tilsiktede ondsinnede handlinger. Loven definerer ikke hva slike handlinger kan være, men tradisjonelt inkluderes spionasje, sabotasje, terrorhandlinger og undergraving. Slike handlinger inngår i det som gjerne betegnes som «sammensatte trusler» eller «hybride virkemidler». Under den kalde krigen ble slike trusler omtalt som «den skjulte krigen» eller «krigen i fredstid». Dette er trusler som kan gå forut for, eller gli over i, krigshandlinger. Handlinger innen disse kategoriene kan også være straffbare. Fellesnevner for sikkerhetstruslene er at de gjennom hemmelighold søker å overraske eller helt unngå å bli oppdaget.

Arbeidet med defensiv, forebyggende sikkerhet går ut på å identifisere hva som kan være mulige mål for trusselaktører. Deretter må det vurderes hvor stor skade trusselen kan medføre dersom et angrep er vellykket eller vi ikke lenger har kontroll over disse målene. Når målene er identifisert og vurdert, må det bygges barrierer for å forhindre anslag, men også motvirke at vi gjennom ulike sårbarheter svikter fra innsiden. Det må også etableres mekanismer for å kunne avdekke og håndtere mistenkelige hendelser. Styrken i tiltakene må vurderes i lys av trussel- og sårbarhetsbildet.

Begrepet «grunnleggende nasjonale funksjoner (GNF)» kom inn i sikkerhetsloven av 2018.[23] Disse funksjonene skal hjelpe til med å identifisere hva som kan tenkes å være mål for trusselaktører, altså «skjermingsverdige verdier». Slike verdier kan i henhold til en endring i sikkerhetsloven i 2023 også utledes direkte fra hva som vurderes som nasjonale sikkerhetsinteresser uten å gå veien om de grunnleggende nasjonale funksjonene. Tiltakene grupperes i fagområdene fysisk sikkerhet, personellsikkerhet, digital sikkerhet og sikkerhetsstyring.

Det defensive, forebyggende sikkerhetsarbeidet virker sammen med det offensive sikkerhetsarbeidet. Offensivt sikkerhetsarbeid er å drive etterretning for å identifisere og innhente informasjon om trusselaktører for å oppdage og avskjære trusselaktiviteter. Dette omtales gjerne som kontraetterretning og kan deles opp i kontraspionasje, kontrasabotasje, kontraterror og kontrasubversjon. I Norge er det Politiets sikkerhetstjeneste (PST) som driver det offensive sikkerhetsarbeidet etter særskilte fullmakter.

Det er virksomhetene selv som etter sikkerhetsloven er ansvarlige for å gjennomføre de forebyggende, defensive sikkerhetstiltakene som må til for å gi et forsvarlig sikkerhetsnivå. Et forsvarlig sikkerhetsnivå innebærer grunnsikring i en normalsituasjon og at sikkerheten styrkes dersom trusselnivået øker.

[23] Prop. 153 L (2016–2017) Lov om nasjonal sikkerhet (sikkerhetsloven), side 7–8 og 32–39.

Boks 3.3 forts.

Et slikt fleksibelt system for egenbeskyttelse er beskrevet i Nasjonalt beredskapssystem (NBS).[24] I tillegg bidrar politiet og Forsvaret med å sikre objekter og nøkkelpunkter i bestemte situasjoner.

De enkelte departementene er etter sikkerhetsloven ansvarlige for forebyggende, defensiv sikkerhet i egen sektor. Justis- og beredskapsdepartementet har det overordnede ansvaret for det forebyggende sikkerhetsarbeidet i sivil sektor, og, mens Forsvarsdepartementet har et tilsvarende ansvar for forsvarssektoren.[25] NSM ble opprettet i 2003 for å ivareta de utøvende funksjoner for de to statsrådene.[26]

Det må være et godt samspill mellom det defensive og offensive sikkerhetsarbeidet. Forebyggende, defensiv sikkerhet må bygge på et best mulig etterretningsgrunnlag om trusselaktørene, deres kapasiteter, intensjoner og modus operandi. Også Etterretningstjenesten er viktig for det defensive sikkerhetsarbeidet. Dersom trusselnivået øker eller aktørenes modus operandi endres, må de som arbeider med den defensive sikkerheten varsles slik at tiltakene kan justeres. Tilsvarende bør de som arbeider med offensiv sikkerhet, holdes orientert om hvor de mulige målene er og hvilken verdi disse er vurdert å ha. I tillegg er det viktig raskt å orientere PST om mistenkelige hendelser siden de kan være et resultat av trusselaktørers virksomhet.

Så vel det offensive som defensive sikkerhetsarbeidet vil ha nytte av en opplyst og årvåken befolkning. Det er derfor viktig med klar kommunikasjon om trussel- og risikobildet og med en godt forståelig og ensartet begrepsbruk.

[24] Nasjonalt beredskapssystem (NBS) består av Sivilt beredskapssystem (SBS) og Beredskapssystem for forsvarssektoren (BFF). NBS er et redskap for politisk styring og forankring av krisehåndtering. Innholdet i NBS er sikkerhetsgradert.

[25] Jf. kgl.res 20. desember 2018 *Ikraftsetting av lov 1. juni nr. 24 om nasjonal sikkerhet med overgangsregler, fordeling av myndighet, videreføring av forskrifter m.m*, pkt.3, fremmet av Forsvarsdepartementet.

[26] Jf. kronprinsreg.res. 4. juli 2003 *Fordeling av ansvar for forebyggende sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet*, fremmet av Forsvarsdepartementet. Er opphevet ved ovennevnte res. av 20. desember 2018.

4 Nasjonal sikkerhetsmyndighets oppgaver

I mandatet er utvalget bedt om å gi en oversikt over Nasjonal sikkerhetsmyndighets (NSMs) samlede portefølje av oppgaver. Utvalget skal videre, med «utgangspunkt i sikkerhetslovens kapittel 2 om ansvar og myndighet for forebyggende sikkerhetsarbeid», vurdere «om porteføljen er hensiktsmessig innrettet». Deretter skal utvalget vurdere om det er oppgaver «som ikke kan relateres direkte til sikkerhetsloven», som bør overføres til andre myndigheter.

NSM er gitt mange oppgaver med utgangspunkt i flere forskjellige hjemmelsgrunnlag, både etter sikkerhetsloven og enkelte andre lover. I sikkerhetsloven brukes betegnelsen sikkerhetsmyndigheten og ikke Nasjonal sikkerhetsmyndighet eller NSM. I lovproposisjonen står det i merknaden til § 2-2:[27]

> «Bestemmelsen angir sikkerhetsmyndighetens ansvar og myndighet etter loven. I praksis vil funksjonen som sikkerhetsmyndighet ivaretas av den aktøren som blir tildelt myndigheten fra ansvarlig fagdepartement. Ansvaret som tillegges sikkerhetsmyndigheten, er i dag lagt til Nasjonal sikkerhetsmyndighet (NSM). Forslaget innebærer ingen endring av dette.»

Regjeringen har presisert NSMs oppgaver i forskrifter. I forskriftene til sikkerhetsloven brukes gjennomgående benevnelsen «Nasjonal sikkerhetsmyndighet» eller «NSM».

I det videre legger vi i tråd med dette til grunn at oppgaver som i loven er gitt til sikkerhetsmyndigheten, skal håndteres av NSM.

Justis- og beredskapsdepartementet og Forsvarsdepartementet har i en hovedinstruks til NSM gjentatt flere av disse oppgavene og dessuten lagt til flere.[28] Flere av oppgavene i instruksen er oppgaver som ble overført fra daværende Forsvarets sikkerhetstjeneste (FO/S) da NSM ble opprettet i 2003, se omtale i kapittel 3. I tillegg har Justis- og beredskapsdepartementet og Forsvarsdepartementet pålagt NSM ulike oppgaver gjennom iverksettingsbrev, i tildelingsbrev og supplerende tildelingsbrev. Enkelte av oppgavene er omtalt i hovedinstruksen, andre er det ikke.

Det er altså blitt lagt til flere nye oppgaver i porteføljen til NSM i årenes løp, men uten at det er tatt oppgaver ut. NSMs oppgaveportefølje ble ytterligere utvidet så sent som i 2024, da ansvaret for Norsk senter for informasjonssikring (NorSIS) og oppgaver fra det tidligere interkommunale selskapet Kommune-CSIRT ble overført

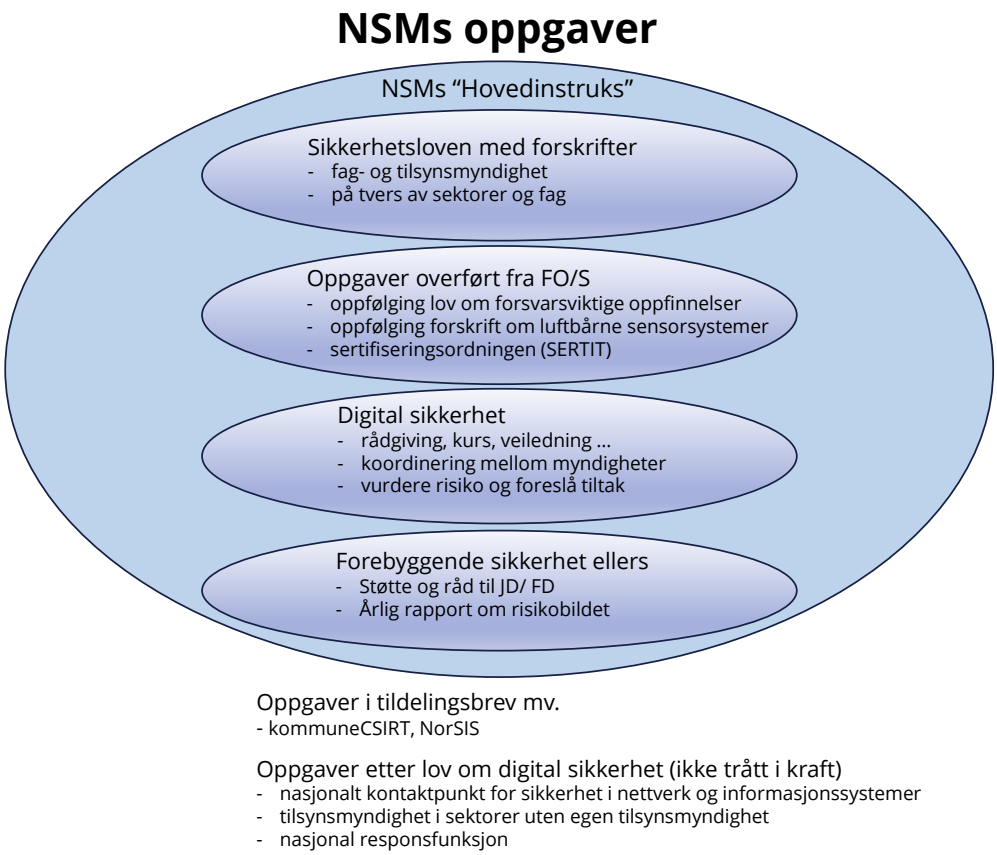
[27] Prop. 153 L (2016 –2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)*, side 166.

[28] Hovedinstruks for Nasjonal sikkerhetsmyndighet av 03.05.2019.

til NSM.[29] Videre er NSM tiltenkt flere nye oppgaver i ny forskrift til digitalsikkerhetsloven som etter planen skal tre i kraft i løpet av 2025.[30] NSMs portefølje av oppgaver kan også bli endret i den nye loven om grunnsikring av virksomheter som ble varslet i Totalberedskapsmeldingen regjeringen la fram i januar 2025.

Alle oppgavene til NSM omhandler forebyggende defensiv sikkerhet, se boks 3.3. I dette kapittelet har utvalget forsøkt å identifisere hvilke oppgaver som er sentrale i NSMs virksomhet, og omtalt bakgrunnen for hvorfor de er lagt til direktoratet. Vi belyser deretter i hvilken grad andre aktører arbeider sammen eller parallelt med NSM for å løse dem. Se også omtale i kapittel 6 om andre myndigheter med grenseflater mot direktoratet. Utvalgets vurderinger av NSMs oppgaver følger i kapittel 10.

Figur 4.1 NSMs oppgaver og hjemmelsgrunnlag [1)]



1) Figuren er ment å illustrere at NSM har oppgaver med ulike hjemmelsgrunnlag. Instruksen favner mange av disse, men ikke alle. Oppgaveporteføljen består av en god del oppgaver som ikke følger direkte av sikkerhetsloven. Figuren er en forenkling og gir ikke et uttømmende bilde.

[29] Prop. 1 S (2024–2025) for budsjettåret 2025 under Justis- og beredskapsdepartementet, side 137. NorSIS arbeider med digital sikkerhet med vekt på allmennheten. NorSIS er nå en ny enhet i NSM lokalisert i Gjøvik. Kommune-CSIRTs oppgaver med å gi råd til kommuner om digital sikkerhet er overført til NSM, mens de operative oppgavene er lagt til Helse CERT.

[30] Høringsbrev 11. september 2024 til forskrift til digitalsikkerhetsloven med frist 11. desember: Høringsbrev – forslag til forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften) (regjeringen.no).

4.1 NSMs oppgaver etter kapittel 2 i sikkerhetsloven

Ifølge utvalgets mandat er oppgavene som NSM har etter sikkerhetsloven, og særlig de som følger av kapittel 2 i loven, viktige i NSMs virksomhet. NSM skal blant annet føre tilsyn, dele informasjon, veilede, drifte digital deteksjon og bistå ved digitale hendelser. I dette avsnittet beskriver vi disse oppgavene.

4.1.1 § 2-2 NSMs ansvar for forebyggende sikkerhetsarbeid

Paragraf 2-2 har overskriften «Sikkerhetsmyndighetens ansvar for forebyggende sikkerhetsarbeid». Dette er dermed en særlig sentral bestemmelse for NSM. Paragrafen lyder:

«§ 2-2. *Sikkerhetsmyndighetens ansvar for forebyggende sikkerhetsarbeid*

Sikkerhetsmyndigheten har det sektorovergripende ansvaret for at forebyggende sikkerhetsarbeid i virksomhetene utføres i samsvar med loven.

Sikkerhetsmyndigheten har det overordnede ansvaret for at sikkerhetstilstanden i alle sektorer kontrolleres, og skal se til at virksomhetene oppfyller sine plikter etter loven. Sikkerhetsmyndigheten skal blant annet

a. se til at det føres tilsyn med at virksomheter oppfyller krav til forebyggende sikkerhetsarbeid
b. utarbeide og vedlikeholde grunnleggende kriterier for tilsyn
c. innhente og vurdere informasjon som har betydning for forebyggende sikkerhetsarbeid
d. gi informasjon, råd og veiledning om forebyggende sikkerhetsarbeid og krav til tiltak
e. holde oversikt over de funksjonene og virksomhetene departementene har identifisert etter § 2-1
f. holde oversikt over virksomheter som det er fattet vedtak om etter § 1-3
g. legge til rette for informasjonsdeling etter § 2-3
h. bidra til å utvikle sikkerhetstiltak og fastsette krav til forebyggende sikkerhetsarbeid
i. holde oversikt over eiendommer av sikkerhetsmessig betydning som det er sendt varsel om etter § 7-6 andre ledd.

Sikkerhetsmyndigheten er nasjonal fagmyndighet overfor andre land og internasjonale organisasjoner.

Så langt det er nødvendig for å gjennomføre oppgavene i eller i medhold av loven, skal sikkerhetsmyndigheten gis uhindret adgang til skjermingsverdig informasjon, informasjonssystem, objekt eller infrastruktur.

Kongen kan gi forskrift om sikkerhetsmyndighetens ansvar for forebyggende sikkerhetsarbeid.»

Loven gir altså NSM det «sektorovergripende ansvaret» for at forebyggende sikkerhetsarbeid i virksomhetene utføres i samsvar med loven. NSM har videre «det overordnede ansvaret for at sikkerhetstilstanden i alle sektorer kontrolleres», og

NSM skal se til at virksomhetene oppfyller sine plikter etter loven. Sikkerhetsloven omfatter etter § 1-2 statlige, fylkeskommunale og kommunale organer, samt private leverandører av varer eller tjenester i forbindelse med sikkerhetsgraderte anskaffelser etter lovens kapittel 9. Den omfatter også andre virksomheter som det er fattet vedtak om etter § 1-3. Særbestemmelser om Stortinget, Stortingets organer, domstolene og regjeringens medlemmer følger av § 1-4.

Ifølge forarbeidene til loven menes det med sektorovergripende ansvar «i første rekke ansvaret for at forebyggende sikkerhetsarbeid etter loven har en helhetlig tilnærming, og at sikkerhetsarbeidet mellom ulike departementer og ulike relevante sektormyndigheter blir koordinert.»[31] NSMs ansvar griper «ikke inn i de enkelte departementenes ansvar innen eget myndighetsområde».

NSMs tilsynsvirksomhet (§ 2-2 … bokstav a og b)

Tilsyn er en del av arbeidet med forebyggende sikkerhet. NSMs tilsynsoppgaver er gitt dels i sikkerhetsloven § 2-2 og dels i kapittel 3. I tillegg er også oppgaver for tilsynsmyndigheten omtalt andre steder i loven og forskrifter. Etter bokstav a skal NSM «se til at det føres tilsyn med at virksomhetene oppfyller de krav som stilles til forebyggende sikkerhetsarbeid.» Kapittel 3 sier i større grad hva NSM selv skal gjøre for å utføre tilsynet. Det er dessuten stilt nærmere krav til NSMs tilsynsvirksomhet i forskrift om virksomheters arbeid med forebyggende sikkerhet kapittel 14, og i forskrift om kryptosikkerhet § 2.

Etter sikkerhetsloven § 3-1 kan ansvarlig departement beslutte at sektortilsyn på departementets fagområde også kan føre tilsyn etter sikkerhetsloven. Etter forarbeidene skal det før slik beslutning fattes «… foretas en helhetsvurdering i samarbeid med sikkerhetsmyndigheten, hvor det skal vurderes om den aktuelle myndigheten har nødvendig sikkerhetsfaglig kompetanse, eller kan opparbeide seg slik kompetanse uten uforholdsmessig høye utgifter …».[32] Det er i dag fem sektortilsyn som er utpekt: Nasjonal kommunikasjonsmyndighet, Norges vassdrags- og energidirektoratet, Havindustritilsynet, Luftfartstilsynet og Jernbanetilsynet. Der det er sektortilsyn, fører som hovedregel ikke NSM tilsyn direkte med virksomheter underlagt sikkerhetsloven, men med at sektortilsynene fører et tilfredsstillende tilsyn med virksomhetene. Sektortilsynene skal rapportere til NSM. I sektorer der det ikke er sektortilsyn med tilsynsansvar etter sikkerhetsloven, fører NSM tilsyn med virksomheter som er underlagt sikkerhetsloven. Benevnelsen «tilsynsmyndighet» viser dermed både i sikkerhetsloven og tilhørende forskrifter enten til NSM eller til sektortilsyn der slike er utpekt. Sektortilsynenes virksomhet er nærmere omtalt i kapittel 6.

Når sikkerhetsmyndigheten etter § 2-2 bokstav b skal «utarbeide og vedlikeholde grunnleggende kriterier for tilsyn», legges det ifølge lovforarbeidene til rette for en nasjonal enhetlig sektorovergripende tilnærming til tilsyn innen forebyggende

[31] Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)*, side 167.

[32] Ibid, side 170.

sikkerhetsarbeid.[33] Dette presiseres i lovens § 3-2 der sikkerhetsmyndigheten også pålegges å legge til rette for felles opplæring av tilsynspersonell.

NSM eller sektortilsynet fører blant annet tilsyn med virksomhetenes beskyttelse av skjermingsverdig informasjon, informasjonssystemer, objekter eller infrastruktur. Etter § 88 i forskrift om virksomheters arbeid med forebyggende sikkerhet fører NSM også tilsyn med leverandører til sikkerhetsgraderte anskaffelser når leverandøren har lokaler innenfor norsk jurisdiksjon, med mindre annet er avtalt med et sektortilsyn.

Selv i sektorer med egne sektortilsyn etter sikkerhetsloven skal sikkerhetsmyndigheten etter sikkerhetsloven § 3-1 føre tilsyn med virksomhetene «dersom det følger av internasjonale forpliktelser eller er tvingende nødvendig». NSM skal i henhold til samme paragraf «føre tilsyn med departementene og myndigheter med tilsynsansvar etter andre ledd». Det er også i forskrift om kryptosikkerhet § 2 lagt til NSM alene å se til at de krav som følger av forskriften, oppfylles. NSM fører også tilsyn med de myndighetene i forvaltningen som klarerer personell i første instans.

NSMs samlede tilsynsvirksomhet drives fra en egen avdeling, Kontrollavdelingen. Kompetansen i øvrige avdelinger kan bli trukket inn i arbeidet. Det utarbeides årlige tilsynsplaner for arbeidet, men disse vil kunne fravikes ved behov. Dersom det oppstår sikkerhetstruende hendelser, vil NSM som del av håndteringen kunne iverksette tilsynssak.

Tilsynsmyndighetene avgir sine tilsynsrapporter til virksomheten som er gjenstand for tilsyn. Sektortilsyn skal etter § 91 i forskrift om virksomheters arbeid med forebyggende sikkerhet i tillegg sende sine rapporter til NSM. NSM kan gjøre tilsynsrapporter tilgjengelige for Politiets sikkerhetstjeneste (PST).

Resultatene fra tilsyn med flere ulike virksomheter omtales i såkalte kontrollmeldinger. Meldingene omhandler ulike tema og kan skrives i samarbeid mellom NSM og ett eller flere sektortilsyn. Meldingene sendes til relevante departementer, og de kan også gis en videre distribusjon.

NSM skal innhente og vurdere informasjon for sikkerhetsarbeidet (§ 2-2 … bokstav c)

NSM har plikt til å hente inn og vurdere informasjon som har betydning for det forebyggende sikkerhetsarbeidet. NSM vurderer i denne sammenhengen hvilken betydning ny informasjon har for nasjonale sikkerhetsinteresser, risikobildet og sikkerhetstilstanden i dag og i fremtiden for utpekte og klassifiserte skjermingsverdige verdier. Slik innhenting og vurdering av informasjon har som formål å forbedre sikkerhetstilstanden på kort og lang sikt. Informasjon om trusselbildet fra Etterretningstjenesten og PST er viktig, men også annen informasjon som kan belyse verdi-, sårbarhets- og tiltaksvurderinger fra et bredt spekter av kilder.

Bestemmelsen må ses i sammenheng med virksomheters varslingsplikt etter sikkerhetsloven § 4-5. I henhold til § 4-5 skal virksomheter varsle sikkerhetsmyndigheten og andre myndigheter som utfører tilsyn, dersom de har blitt rammet

[33] Ibid., side 66.f.

av sikkerhetstruende virksomhet eller de får kunnskap om planer eller aktiviteter som kan gi risiko for at nasjonale sikkerhetsinteresser blir truet. Virksomheter har varslingsplikt og plikt til å melde inn opplysninger til NSM også etter flere andre bestemmelser i sikkerhetsloven og i forskrifter fastsatt med hjemmel i denne.

Innhenting og vurdering av informasjon er et løpende arbeid som gjøres innen alle fagområdene til NSM. Mange av NSMs avdelinger og medarbeidere bidrar derfor i arbeidet, blant annet analysepersonell i fagavdelingene og de som arbeider med teknisk kontroll, tilsyn og rådgiving. NSM har en egen analyseenhet og et situasjonssenter som bidrar i dette arbeidet.

NSM skal gi informasjon, råd og veiledning og legge til rette for informasjonsdeling (§ 2-2 … bokstav d og g)

Med sikkerhetsloven av 2018 ble detaljerte regler om tiltak i stor grad erstattet med funksjonelle krav. Regelverket sier ikke alltid hvilke sikkerhetstiltak en virksomhet skal etablere, men at virksomhetene selv skal vurdere risiko og sette i verk tiltak som gir et forsvarlig sikkerhetsnivå. Lovens formål ble endret blant annet for å legge bedre til rette for beskyttelse mot såkalte hybride eller sammensatte trusler og gi mer fleksibilitet til sektorer og virksomheter.

Det ble samtidig lovfestet i § 2-3 at NSM skulle legge til rette for deling av informasjon som er nødvendig for virksomhetenes forebyggende sikkerhetsarbeid. Dette kom i tillegg til NSMs plikt til å gi informasjon, råd og veiledning.

I lovproposisjonen uttrykkes det en forventning om at NSM skal ha en aktiv rolle med å gi råd til virksomhetene, men at det av ressursmessige og praktiske grunner forutsettes «at slik rådgivning fortrinnsvis gis gjennom generelle veiledere og felles kursopplegg o.l.».[34] Plikten til å gi råd omfatter de virksomhetene som er omfattet av sikkerhetsloven. NSM forsøker i tråd med dette å unngå ressurskrevende rådgiving til enkeltvirksomheter, men heller å nå ut med informasjon, råd og veiledning til flest mulig samtidig – «en til mange». NSM veileder først og fremst gjennom skriftlige veiledninger og håndbøker til regelverket. Det som er ugradert, publiseres på NSMs hjemmeside. Sammen med informasjon om risiko gir dette grunnlag for virksomhetenes arbeid med å etterleve sikkerhetsloven og annet regelverk. Rådgiving til virksomheter vil kunne forekomme i tillegg i enkeltsaker basert på en vurdering av risikoen for nasjonal sikkerhet. Ressurser vil da kunne bli tilført NSM fra virksomheten som skal rådgis. Eksempler på slike rådgivningsoppdrag er IKT-programmene MAST og Mime i forsvarssektoren.[35] NSMs rådgiving til forsvarssektoren følger også av hovedinstruksens bestemmelse om at direktoratet skal «(v)eilede og rådgi ift sikkerhetsfaglige spørsmål knyttet til forsvarssektorens materiellprosjekter».[36]

Etter sikkerhetsloven § 4-2 fjerde ledd skal tilsynsmyndigheten «etter forespørsel gi råd og veiledning» til virksomheters vurdering av risiko. I de sektorene det er utpekt sektortilsyn etter sikkerhetsloven, er det sektortilsynet som skal gi slike råd.

[34] Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)*, side 167.

[35] Forsvarsmateriell har samlet en rekke investeringsprosjekter innen IKT i et program som kalles Mime (kampnær IKT) og et program som heter MAST (militær anvendelse av skytjenester).

[36] Hovedinstruks for Nasjonal sikkerhetsmyndighet, side 4.

I andre sektorer gjelder denne plikten for NSM. Etterspørselen etter råd, veiledning og foredrag er stor og økende.[37]

NSM har etablert et eget kurssenter hvor det tilbys undervisning i ulike sikkerhetsfaglige temaer for å sette virksomheter i stand til å etterleve sikkerhetsloven. Det avholdes kurs om sikkerhet generelt, men også kurs rettet mot spesifikke fagfelt og målgrupper. NSM underviser selv og henter inn eksterne forelesere. Det holdes både kurs med fysisk oppmøte og ulike web-baserte kurs.

NSM publiserer hver uke en gradert sikkerhetsrapport rettet mot departementene og virksomheter som er underlagt sikkerhetsloven. Her gis ulike typer informasjon om risiko og anbefalinger om hva sektorer og virksomheter bør være særlig oppmerksomme på i de ulike fagområdene.

NSM skal holde oversikt over funksjoner, virksomheter og eiendommer (§ 2-2 … bokstav e, f og i)

Bestemmelsen under § 2-2 bokstav e, f og i sier at NSM skal holde oversikt over funksjoner, systemer, virksomheter, eiendommer mv. av betydning for nasjonale sikkerhetsinteresser.

Departementene er ansvarlige for forebyggende sikkerhetsarbeid innenfor sine ansvarsområder. De skal identifisere hva som er grunnleggende nasjonale funksjoner (GNF) og hvilke virksomheter som har vesentlig betydning for slike funksjoner. Departementene fatter også vedtak etter sikkerhetsloven § 1-3 om hvilke virksomheter som skal underlegges sikkerhetsloven. Det er virksomheter som har aktiviteter eller råder over informasjon, informasjonssystemer, objekter eller infrastruktur som har avgjørende betydning for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser, og virksomheter med behov for å behandle sikkerhetsgradert informasjon. Departementene skal i henhold til sikkerhetsloven § 2-1 første ledd bokstav d sende oversikter over de grunnleggende nasjonale funksjonene og virksomhetene til sikkerhetsmyndigheten, og sikkerhetsmyndigheten skal i henhold til § 2-2 andre ledd bokstav e og f holde oversikt over disse.

Også i andre kapitler i sikkerhetsloven og i forskrifter til loven forutsettes det at sikkerhetsmyndigheten skal holde oversikt over ulike forhold av betydning for nasjonale sikkerhetsinteresser. Departementene skal for eksempel i henhold til sikkerhetsloven § 7-1 andre ledd utpeke og klassifisere skjermingsverdige objekter og infrastruktur og melde disse inn til sikkerhetsmyndigheten med angivelse av klassifiseringsgrad. NSM skal etter § 13 i forskrift om virksomheters arbeid med forebyggende sikkerhet også motta oversikt over andre virksomheter som de virksomhetene som er underlagt sikkerhetsloven er avhengige av for å fungere som de skal.

Etter sikkerhetsloven § 7-6 andre ledd skal virksomheter varsle sikkerhetsmyndigheten eller tilsynsmyndigheten dersom en eiendom av sikkerhetsmessig betydning utgjør en risiko for en virksomhets skjermingsverdige objekt eller infrastruktur og det ikke er mulig å opprettholde et forsvarlig sikkerhetsnivå gjennom tiltak. Etter

[37] NSM årsrapport for 2023, side 10, 14, 15, 18 og 22.

§ 2-2, andre ledd bokstav i, skal sikkerhetsmyndigheten holde oversikt over slike eiendommer.

NSM skal videre etter ulike bestemmelser i sikkerhetsloven og forskriftene holdes informert om blant annet personklareringer, informasjonssystemer som er godkjent av andre enn NSM og ulike forhold ved sikkerhetsgraderte anskaffelser. Dette inkluderer årlige oversikter over sikkerhetsgraderte anskaffelser i virksomheter underlagt loven.

I tillegg skal NSM holde oversikt over egne avgjørelser etter sikkerhetsloven og tilhørende forskrifter.

NSMs oppgave med å holde denne typen oversikter er ment å styrke evnen til å følge opp de øvrige oppgavene som følger av § 2-2. Slike oversikter er videre ansett som viktige for at NSM skal kunne ha en god forståelse av situasjonen, bidra i hendelseshåndtering og gi råd til politiske myndigheter om defensive sikkerhetstiltak i situasjoner der det er risiko for sammensatt virkemiddelbruk.

Oversikter over funksjoner, virksomheter, skjermingsverdige verdier mv. holdes ved like i de ulike fagmiljøene i NSM.

Bidra til å utvikle tiltak og sette krav til sikkerhetsarbeidet (§ 2-2 … bokstav h)

Sikkerhetsmyndigheten skal ha oversikt over hva som finnes av regelfestede og anbefalte sikkerhetstiltak i dag, identifisere behov og foreslå nye utviklingsprosjekter og tiltak innenfor de ulike fagområdene. Dette gjelder også behov for regelverksutvikling. NSM utarbeider faglige utredninger selv og i samarbeid med forskningsmiljøer og andre relevante samarbeidspartnere. NSM følger også med på utviklingen av sikkerhetstiltak på mer generelt grunnlag i samfunnet og i andre land.

Nasjonal fagmyndighet overfor andre land og internasjonale organisasjoner (§ 2-2 tredje ledd)

NSM holder oversikt over alle sikkerhetsavtaler som Norge er bundet av. NSM forhandler også om slike avtaler eller bistår Justis- og beredskapsdepartementet, Forsvarsdepartementet, Utenriksdepartementet eller andre når det er disse som står for forhandlingene. De aller fleste av disse handler om gjensidig beskyttelse av sikkerhetsgradert informasjon. NSM påser at forpliktelser følges opp nasjonalt og holder kontakt med de som er oppnevnt som kontaktpunkter i andre land eller internasjonale organisasjoner. NSM deltar i arbeidsgrupper og komiteer i NATO og andre organisasjoner som Norge er medlem av der forebyggende sikkerhet er tema, eller bistår i forberedelsene dersom slike møter er på et høyere nivå. Norge deltar i flere av EUs romprogrammer og NSM har som oppgave å følge opp disse nasjonalt og representere Norge i komiteer og arbeidsgrupper. NSM samarbeider med Norsk romsenter om dette og er kontaktpunkt for hendelseshåndtering overfor EU for satelittnavigasjonssystemene Galileo og EGNOS.[38] NSM har sikker-

[38] Galileo (Global Navigation Satelite System) er etablert av den europeiske romorganisasjonen ESA og EU for nøyaktige posisjons- og tidstjenester. EGNOS (European Geostationary Navigation Overlay Service) er etablert av ESA, EU og luftfartssikkerhetsorganisasjonen EUROCONTROL for å bedre nøyaktigheten og påliteligheten til GPS i Europa.

hetsfaglig dialog med andre lands tilsvarende tjenester. Det vises også til omtale i kapittel 7 om Norges internasjonale forpliktelser.

4.1.2 § 2-3 Utveksling av trusselvurderinger og annen sikkerhetsinformasjon

Sikkerhetsmyndigheten skal etter § 2-3 «legge til rette for at virksomheter som loven gjelder for, får tilgang til informasjon om trusselvurderinger og andre opplysninger som er av betydning for virksomhetenes forebyggende sikkerhetsarbeid». Videre skal sikkerhetsmyndigheten, i samråd med sektormyndigheter og andre relevante myndigheter, «sikre at det etableres nødvendige fora for informasjons- og erfaringsutveksling».

Det er Etterretningstjenesten og Politiets sikkerhetstjeneste (PST) som vurderer truslene, og ikke NSM. Det er opp til disse tjenestene å vurdere om de har anledning til å dele denne informasjonen. Kravet i sikkerhetsloven er at det er virksomhetene selv som skal vurdere risikoen og om sikkerheten er forsvarlig. Trussel- og annen sikkerhetsinformasjon er viktig for at virksomhetene skal vurdere hvilken risiko de er utsatt for.

Til utveksling av informasjon benytter NSM eksisterende, sektorvise fora der dette er hensiktsmessig, for eksempel Sikkerhetsrådet for luftfarten, ekom-sikkerhetsforum eller Forum for sektortilsyn. NSM benytter også eksisterende tverrsektorielle møteplasser som ledes av blant annet Direktoratet for samfunnssikkerhet og beredskap (DSB) eller Forsvarets operative hovedkvarter. Videre orienterer NSM sektordepartementer, sektormyndigheter og virksomheter direkte ved å sende egne rapporter, herunder den ukentlige graderte sikkerhetsrapporten vist til ovenfor. I møter mellom NSMs ledelse og myndigheter og virksomheter er situasjonsbildet for sikkerheten stort sett faste poster på dagsorden. Graderingsnivå på trusselvurderingene og sikkerhetsinformasjonen og prinsippet om å informere om bare det mottaker «trenger å vite» kan legge begrensninger på spredningen av informasjon.

I 2019 ble Nasjonalt cybersikkerhetssenter (NCSC) opprettet som et partnerskap mellom NSM og en rekke både offentlige myndigheter og private virksomheter. NCSC er et viktig forum for NSMs oppfølging av oppgaven med å drifte og utvikle varslingssystemet for digital infrastruktur (VDI) og som nasjonal responsfunksjon etter sikkerhetsloven. NCSC har over tid blitt et nokså stort forum med deltakelse og temaer som strekker seg ut over sikkerhetslovens virkeområde.

4.1.3 § 2-4 Responsfunksjon og varslingssystem for digital infrastruktur

§ 2-4 er en sentral bestemmelse for digital sikkerhet i sikkerhetsloven. NSMs oppgaver kan særlig utledes fra paragrafens innledning og avslutning som lyder:

> «Kongen utpeker en myndighet som skal drive en nasjonal responsfunksjon for alvorlige digitale angrep og et nasjonalt varslingssystem for digital infrastruktur.
>
> […]
>
> Kongen kan gi forskrift om nasjonal responsfunksjon og nasjonalt varslingssystem for digital infrastruktur.»

I § 63 i forskrift om virksomheters arbeid med forebyggende sikkerhet er denne oppgaven gitt til NSM:

> «NSM skal drifte en nasjonal responsfunksjon for alvorlige digitale angrep og et nasjonalt varslingssystem for digital infrastruktur. I forbindelse med dette skal informasjon om digitale angrep innhentes, analyseres og deles».

Varslingssystem for digital infrastruktur (VDI-systemet) ble opprettet i 1999 av EOS-tjenestene som et samarbeidsprosjekt. VDI er et nettverk av sensorer som plasseres på internettforbindelser hos utvalgte offentlige og private virksomheter som har kritisk infrastruktur. Sensorene kan gjøre det mulig for NSM å oppdage og verifisere digitale angrep. VDI-sentralen og ansvaret for å følge opp systemet ble flyttet fra Politiets sikkerhetstjeneste (PST) til NSM i 2003 og hjemlet i sikkerhetsloven i 2016.[39]

Tilgangen på operative data fra VDI-systemet og erfaringer fra samarbeid med VDI-deltakerne gjorde at NSM i 2004 opprettet en nasjonal responsfunksjon under navnet NorCERT (Norwegian Computer Emergency Response Team). NorCERT ble etablert fast i 2006.[40] Oppgaven er å rådgi og bistå virksomheter i Norge i å forebygge og håndtere alvorlige digitale hendelser, og utveksle informasjon med andre land og internasjonale organisasjoner. Også denne nasjonale responsfunksjonen ble lovfestet som en oppgave for NSM i sikkerhetsloven i 2016.

Informasjon fra VDI er ment som en viktig del av hendelseshåndtering og var en del av begrunnelsen for at den nasjonale responsfunksjonen ble lagt til NSM. Deling av informasjon fra VDI og informasjon fra hendelseshåndteringen er i dag nærmere regulert i virksomhetssikkerhetsforskriften § 65. I henhold til denne bestemmelsen kan NSM, når det er innenfor sikkerhetslovens formål, «dele med partene i Felles cyberkoordineringssenter (FCKS) informasjon innhentet fra varslingssystemet for digital infrastruktur eller gjennom den nasjonale responsfunksjonen», se nærmere omtale av FCKS nedenfor. Videre kan NSM, i den utstrekning det er nødvendig for å håndtere en konkret hendelse, dele med andre aktører informasjon som er inn-

[39] Prop. 97 L (2015–2016) *Endringer i sikkerhetsloven (reduksjon av antall klareringsmyndigheter mv.)*, kapittel 6.6. Se også Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet*, kapittel 7.4.4.

[40] St.meld. nr. 17 (2006–2007) *Eit informasjonssamfunn for alle*, se særlig punkt/kapitel 9.4.3 Nasjonal koordinering av varsling, rådgiving og assistanse for informasjonstryggleik.

hentet fra varslingssystemet for digital infrastruktur eller gjennom den nasjonale responsfunksjonen. NSM skal ved fare for alvorlige hendelser «informere berørte nasjonale og internasjonale aktører om trusler, sårbarheter og mulige tiltak».

I lovproposisjonen til sikkerhetsloven er det vist til at både responsfunksjonen og varslingssystemet har et bredere nedslagsfelt enn sikkerhetslovens virkeområde, men at disse funksjonene likevel har en så sterk tilknytning til nasjonalt forebyggende sikkerhetsarbeid at lovfesting av funksjonene passer best i sikkerhetsloven.[41]

I forarbeidene til endringene i sikkerhetsloven i 2017, ble det drøftet om NSMs ansvar for VDI og NorCERT er forenlig med at NSM også er tilsynsmyndighet. Det ble vist til at begge funksjonene allerede hadde vært i NSM i flere år uten at det hadde vært et problem, og at ansvaret for både VDI og NorCERT bør holdes innenfor EOS-tjenestene.[42]

I tillegg til en nasjonal responsfunksjon som NSM er ansvarlig for, er det etablert en ordning med sektorvise responsmiljøer for å støtte opp under effektiv deling av informasjon og håndtering av digitale angrep. De fleste sektorer har etablert slike miljøer eller inngått ulike former for samarbeid om dette. Responsmiljøene er også bindeledd mellom NSM og de enkelte virksomhetene i ulike sektorer. Justis- og beredskapsdepartementet ga i 2017 ut et «Rammeverk for håndtering IKT-sikkerhetshendelser» for å tydeliggjøre hvordan samvirket mellom virksomheter, de sektorvise responsmiljøene og det nasjonale responsmiljøet hos NSM skal være.[43] Krav til samvirke vil bli ytterligere styrket gjennom ny lov om digital sikkerhet.[44]

Digitalsikkerhetsloven ble sanksjonert 20. desember 2023 og vil tre i kraft når forskrift foreligger.[45] Loven gjennomfører EUs NIS-direktiv i norsk rett. Justis- og beredskapsdepartementet varslet i Totalberedskapsmeldingen at NIS2-direktivet sammen med EUs CER-direktiv etter planen skal gjennomføres i norsk rett i en ny lov med felles krav til grunnsikring hos kritiske virksomheter.[46] NIS står for Network & Information Security og stiller krav til digital sikkerhet for virksomheter med særlig betydning for samfunnet. CER står for Critical Entities Resilience og stiller krav til motstandsdyktighet i virksomheter som leverer tjenester som er avgjørende for å opprettholde kritiske samfunnsfunksjoner eller økonomiske aktiviteter. Det vises til nærmere omtale av EUs direktiver i kapittel 7.

Den nasjonale responsfunksjonen og håndtering av digitale hendelser er nærmere forklart i boks 4.1. Se også boks 4.2 der håndteringene av et cyberangrep mot Departementenes sikkerhets- og serviceorganisasjon (DSS) i 2023 er beskrevet. I boks 4.4 er ansvar for digital sikkerhet for ulike aktører omtalt.

---

41 Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)*, side 168.

42 Prop. 97 L (2015–2016) *Endringer i sikkerhetsloven (reduksjon av antall klareringsmyndigheter mv.)*, kapittel 6.6.

43 Rammeverket bygger på et tidligere dokument «Modell for håndtering av IKT-hendelser» utgitt av Justis- og beredskapsdepartementet i 2014. Et forslag til justert rammeverk er nylig sendt fra NSM til Justis- og beredskapsdepartementet.

44 Prop. 109 LS (2022–2023) *Lov om digital sikkerhet (digitalsikkerhetsloven)*, Innst. 78 L (2023–2024).

45 Det er gjennomført høring om forskriften. Fristen for å komme med innspill var 11. desember 2024.

46 Meld. St. 9 (2024–2025) *Totalberedskapsmeldingen – Forberedt på kriser og krig*.

Boks 4.1 Håndtering av digitale sikkerhetshendelser

«Rammeverk for håndtering av IKT-sikkerhetshendelser» ble utgitt av Justis- og beredskapsdepartementet i samråd med Forsvarsdepartementet i 2017, dvs. før gjeldende sikkerhetslov ble vedtatt i 2018. Det beskriver kravene til håndtering av digitale sikkerhetshendelser.[47]

Rammeverket angir hvem som har ansvar for sikkerheten og hvem som kan og skal bidra når det skjer hendelser. Det går gjennom både hva som bør gjøres i forkant, under og etter en hendelse.

Målgruppen for rammeverket
Målgruppen for rammeverket er offentlige og private virksomheter som har betydning for kritisk infrastruktur og kritiske samfunnsfunksjoner. Hva som er kritisk infrastruktur og kritiske samfunnsfunksjoner, er definert i det såkalte KIKS-rammeverket, se boks 6.2. Rammeverket favner dermed videre enn sikkerhetsloven og virksomheter som er underlagt denne. Ifølge rammeverket gjelder det for de sektorvise responsmiljøene (SRM), myndigheter som har en rolle i håndtering av IKT-sikkerhetshendelser og departementene, men det presiseres at det vil kunne ha nytteverdi også for andre.

Ansvar
Digital sikkerhet er virksomhetenes eget ansvar. Dette ansvaret omfatter også å håndtere hendelser som oppstår. Virksomheter skal vurdere risiko og sårbarheter og sørge for en forsvarlig sikkerhet. Det skal være på plass prosedyrer for håndtering av hendelser, varsling og rapportering mv.

Departementene er ansvarlige for å oppnevne såkalte sektorvise responsmiljøer (SRM) i egen sektor. De sektorvise responsmiljøene skal blant annet samle, systematisere, vurdere og dele informasjon om sårbarheter, trusler og hendelser som kan ramme informasjons- og styringssystemer. De skal også informere departementene og NSM. De samarbeider med andre responsmiljøer og er sammen med en rekke myndigheter og private og offentlige virksomheter partnere i Nasjonalt cybersikkerhetssenteret (NCSC) i NSM.

NSM er den nasjonale responsfunksjonen ved alvorlige digitale angrep. Funksjonen er en integrert del av NCSC. Formålet med senteret er å legge til rette for at virksomheter og responsmiljøer kan samarbeide effektivt i arbeidet med digital sikkerhet og når det oppstår hendelser. NCSCs operasjonssenter er døgnbemannet og følger det digitale risikobildet. NCSC informerer om sårbarheter, har kampanjer for å trygge sikkerheten og varsler dersom det avdekkes hendelser for eksempel gjennom det nasjonale varslingssystemet for digital infrastruktur (VDI).

[47] Rammeverket er under revisjon.

Boks 4.1 forts.

Hendelseshåndtering
Hendelseshåndtering kan innebære tiltak for å 1) stanse hendelsen, begrense skadeomfanget og gjenopprette sikker tilstand, 2) sikre tekniske spor og gjøre beslag eller pågripelser og 3) iverksette offensive mottiltak.

Tiltak for å stanse hendelsen, begrense skadeomfanget og gjenopprette sikker tilstand utføres i all hovedsak av virksomheten selv gjennom egen IT-avdeling og eventuelt med bistand fra ekstern partner. NSM har siden 2016 hatt en kvalitetsordning for leverandører som tilbyr tjenester for håndtering av dataangrep. Virksomhetene skal varsle andre virksomheter som kan være rammet og eventuelt det sektorvise responsmiljøet, overordnet myndighet og politiet hvis alvorlighetsgrad tilsier det.

Det sektorvise responsmiljøet (SRM) har primært en koordinerende rolle som innebærer å dele informasjon innad i sektoren, på tvers av sektorer og med NSM. For å kunne drive effektiv informasjonsdeling må SRM ha god oversikt over situasjonen og sårbarheter mv. SRM skal bistå virksomheten med råd og informasjon fra andre virksomheter i sektoren eller fra NSM. Det forutsettes ikke at SRM skal ha kapasitet til å gjennomføre tiltak direkte på virksomheters systemer. De sektorvise responsmiljøene skal varsle NSM om alvorlige hendelser som rammer samfunnskritiske funksjoner, om hendelsen er avansert og kan komme fra aktører med betydelig kapasitet eller om hendelsen kan omfatte flere sektorer.

NSM har en veiledende og koordinerende rolle nasjonalt i hendelseshåndteringen. NSM utfører teknisk skadevareanalyse, opprettholder et nasjonalt situasjonsbilde i det digitale rommet, deler informasjon med sektorvise responsmiljøer og virksomheter, oppretter samarbeidsfora for de sektorvise responsmiljøene og koordinerer aktiviteten mot politiet, PST og Etterretningstjenesten i samråd med de sektorvise responsmiljøene og berørte virksomhetene. NSM rapporterer til departementene og regjeringen.

Ofte pågår etterforskningen av en hendelse samtidig med at det arbeides for å stanse og gjenopprette skaden. Det vil da kunne oppstå motstridende hensyn, for eksempel ved at det i etterforskingen av hvem som står bak en hendelse, er ønskelig å vente med tiltak for å gjenopprette til sikker tilstand. Slike hensyn vil kunne avveies etter en diskusjon i Felles cyberkoordineringssenter (FCKS) der representanter fra NSM, E-tjenesten, PST og Kripos deltar. NSM varsler FCKS om alvorlige IKT-sikkerhetshendelser som rammer kritisk infrastruktur og kritiske samfunnsfunksjoner.

Boks 4.1 forts.

Sektorvise responsmiljøer (SRM) – oversikt pr. januar 2025

SRM	Sektor
BaneCERT	skinnegående transport
Dep CERT	øverste statsorganer, departementene og politiske partier
eduCSC	forskning og kunnskap
EkomCERT	ekom
Helse- og KommuneCERT	helse og kommune
JustisCERT	justis
KraftCERT*	kraft og petroleum
Landbruks- og matCERT	landbruk- og mat
MaritimCERT	sjøfart og kyst
MiljøCERT	klima og miljø
MilCERT	forsvar
NAVCERT	arbeid og velferd
NFCERT**	finans
NSR	små og mellom store bedrifter som ikke er omfattet av annet SRM eller har forhold til NCSC direkte
VegCERT	veitransport

* Støtter Norges vassdrags- og energidirektorat (NVE) og Havindustritilsynet (Havtil) som er myndighets-SRM i respektive sektorer

** Støtter Finanstilsynet som er myndighets-SRM i sektoren.

Private tjenesteleverandører innenfor NSMs kvalitetsordning for hendelseshåndtering (KVO) – oversikt pr. januar 2025

Atea AS, Defendable AS, Fence AS, KPMG AS, mnemonic AS, NetNordic, Netsecurity AS, Orange Cyberdefense, PwC og Sopra Steria.

Boks 4.2 Håndtering av cyberangrep mot Departementenes sikkerhets- og serviceorganisasjon (DSS) i 2023[48]

NSM ble 11. juli 2023 varslet av Departementenes sikkerhets- og serviceorganisasjon (DSS) om mistenkelig aktivitet i deres nettverk. Videre ble det avdekket datainnbrudd hos DSS og 12 norske departementer denne sommeren hvor en aktør hadde fått tilgang til systemene ved å utnytte nulldagssårbarheter i en programvare som DSS benyttet.[49] En nulldagssårbarhet er en svakhet i en programvare som oppdages av angripere før leverandøren av programvaren selv har blitt klar over den. Siden leverandøren ikke vet om den, finnes det – på det tidspunktet – ikke noe tiltak som kan lukke sårbarheten. Selskapet mnemonic avdekket nulldagssårbarhetene i programvaren.

Utnyttelse av nulldagssårbarheter i programvaren muliggjorde at en avansert trusselaktør over tid hadde tilgang til flere deler av departementenes sentrale nettverk og norsk offentlig forvaltning. Tidspunkt er ikke angitt nærmere grunnet sikkerhetsmessige årsaker.

NSM ivaretar et stående oppdrag knyttet til håndtering av alvorlige digitale angrep og har etablerte varslingskanaler. Innenfor NSMs kontaktnett foreligger vide muligheter til informasjonsutveksling og samarbeid med nasjonale og internasjonale partnere. For å ivareta den nasjonale innretningen ved hendelseshåndtering er det også over tid etablert en kvalitetsordning for leverandører som håndterer IKT-hendelser. Her fungerer NSM som et nav og sentralt kontaktpunkt og er avhengig av samarbeid med andre aktører.

Hendelsen mot DSS viste viktigheten av informasjonsdeling og offentlig-privat samarbeid i praksis. Den demonstrerte hvordan aktører fra begge sektorer samlet sin kompetanse for å håndtere en hendelse med betydning for nasjonal sikkerhet.

NSM gav bistand til hendelseshåndteringen som sikkerhetstjenesteleverandøren mnemonic utførte opp mot DSS. mnemonic er medlem av NSMs kvalitetsordning for hendelseshåndtering.[50] NSM gav også bistand gjennom analyser av logger fra DSS, analyser av data fra NSMs varslingssystem for digital infrastruktur (VDI), samt deteksjon og varsling av aktivitet i VDI.

Hendelsen ble avdekket gjennom sikkerhetsteknologi anskaffet av DSS. Data fra VDI var en viktig bidragsyter til å forstå inngangsvektor og omfanget av hendelsen. En inngangsvektor er det aktøren utnytter for å få tilgang til

[48] Omtalen er omforent mellom NSM, DSS og mnemonic.

[49] Programvaren var Ivanti Endpoint Manager.

[50] Kommersielle sikkerhetstjenesteleverandører har en sentral rolle i håndtering av hendelser, og NSM har derfor en godkjenningsordning for slike leverandører. Disse oppfyller NSMs krav til kvalitet innen hendelseshåndtering. Det er tett samarbeid og det utveksles jevnlig informasjon for å sikre en felles situasjonsforståelse.

Boks 4.2 forts.

systemene, i dette tilfelle sårbarheter i programvaren. Analyser identifiserte også trusselaktørs infrastruktur som bestod av kompromitterte hjemmerutere i Norge og utlandet. Dette lot NSM avdekke ytterligere kompromitteringer som kunne spores tilbake i tid, samt sårbare tilfeller av aktuell programvare i Norge som NSM dermed kunne varsle om.

Det var utstrakt samarbeid mellom NSM, DSS og mnemonic gjennom hendelseshåndteringen. NSM håndterte informasjonsdeling mellom nasjonale og internasjonale samarbeidspartnere. mnemonic hadde løpende dialog med programvareleverandøren for å bidra til å lukke nulldagssårbarhetene i leverandørens produkter.

Felles cyberkoordineringssenter (FCKS) ble tidlig varslet, og Kripos ledet politietterforskningen. Samarbeidet med Kripos og felles tekniske analyser med de øvrige partene i FCKS gjorde det mulig å øke forståelsen for hendelsen. Hver av partene håndterte for øvrig saken i henhold til sine mandater, og funn ble fortløpende delt mellom partene. FCKS produserte også felles situasjonsrapporter til Justis- og beredskapsdepartementet, Kommunal- og distriktsdepartementet og Forsvarsdepartementet.

For å sikre god situasjonsforståelse rapporterte NSM hyppig til styrende departement gjennom hendelseshåndteringen. Kommunal- og distriktsdepartementet holdt samtlige departementer informert underveis, i samråd med NSM og DSS.

NSM bistod videre Kommunal- og distriktsdepartementet og DSS, i samråd med Justis- og beredskapsdepartementet, med råd om verdivurderinger av informasjon og risikovurderinger av berørte IKT-systemer, herunder sikkerhetsfaglige råd ved tjenesteutsetting og bruk av skytjenester og råd om skadevurderinger etter bestemmelsene i sikkerhetsloven.

NSM delte informasjon til de sektorvise responsmiljøene (SRM) og internasjonalt om nulldagssårbarhetene og tekniske indikatorer knyttet til hendelsen.[51] Det ble videre gjennomført sårbarhetskoordinering med programvareleverandøren, mnemonic og Cybersecurity & Infrastructure Security Agency (CISA) for å sørge for sikkerhetsoppdateringer som lukket sårbarhetene, samt varsling av kunder.[52] Dette arbeidet ble utført parallelt med at DSS i samråd med NSM utførte tiltak hvor berørte systemer ble utilgjengeliggjort og at det ble avholdt en pressekonferanse hvor DSS informerte om hendelsen.

[51] Internasjonalt ble blant annet European Government CERTs group (EGC) varslet.

[52] Cybersecurity & Infrastructure Security Agency er underlagt Department of Homeland Security i USA.

Boks 4.2 forts.

Rettidig informasjonsutveksling internasjonalt førte også til at NSM utgav et felles varsel med CISA i august 2023 som beskriver hendelsen, sårbarhetene og risikoreduserende tiltak.

Det ble samlet inn og delt mye informasjon i denne saken som har bidratt til å oppdage flere kompromitteringer nasjonalt og internasjonalt. Blant annet ble det koordinert en verdensomfattende sårbarhetskartlegging med den ideelle organisasjonen Shadowserver som gjorde at virksomheter som benyttet den sårbare programvaren ble varslet.[53] Det er sannsynlig at deling av informasjon om nulldagssårbarhetene og analysene gjort i denne hendelsen har bidratt til å avverge sikkerhetshendelser i Norge og internasjonalt.

[53] Shadowserver samler og analyserer mistenkelig aktivitet på internett.

4.1.4 § 2-5 Vedtak ved risiko for skadevirkninger for nasjonale sikkerhetsinteresser

Kongen i statsråd kan i henhold til sikkerhetsloven § 2-5 første ledd fatte vedtak for å hindre sikkerhetstruende virksomhet eller annen planlagt eller pågående aktivitet som kan innebære en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet. Dette gjelder uavhengig av om virksomheten eller aktiviteten er planlagt eller pågår i en virksomhet som er omfattet av sikkerhetsloven eller ikke. Et slikt vedtak kan fattes uten hensyn til begrensningene i forvaltningsloven § 35 om omgjøring av vedtak uten klage og uavhengig av om aktiviteten er tillatt etter annen lov eller annet vedtak. Hjemmelen etter § 2-5 er ment å være en sikkerhetsventil der ikke annet regelverk gir hjemmel til å gripe inn mot en uønsket aktivitet.

Før det fattes vedtak «bør ansvarlig departement» som forbereder saken, innhente rådgivende uttalelse fra relevante organer med kompetanse innenfor det aktuelle fagområdet. I forarbeidene til sikkerhetsloven av 1998 hvor denne bestemmelsen først kom inn, var det forutsatt at alle EOS-tjenestene skulle inngå i kretsen av relevante organer som skulle avgi uttalelse.[54] Dette legges til grunn også i dag. I tillegg kan det være aktuelt å hente inn uttalelser fra andre virksomheter med særlig kompetanse innenfor det aktuelle fagområdet.[55]

Etter sikkerhetsloven §§ 9-4 og 10-2 forutsettes det på tilsvarende måte at departementene skal rådføre seg med EOS-tjenestene ved anskaffelser til skjermingsverdig informasjonssystem, objekt eller infrastruktur, og ved vedtak om stans av erverv av eiendom. NSM ble i 2021 utpekt som Nasjonalt kontaktpunkt for motvirkning av sikkerhetstruende økonomiske virkemiddelbruk for å bidra til en mer effektiv behandling av saker etter sikkerhetslovens §§ 10-3 og 2-5. Kontaktpunktet er nærmere omtalt i boks 4.3 og kapittel 4.3.2 nedenfor.

[54] Prop. 97 L (2015–2016) *Endringer i sikkerhetsloven (reduksjon av antall klareringsmyndigheter mv.)*, side 72.

[55] Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)*, side 169.

Boks 4.3 NSMs rolle i saker om eierskapskontroll

Sikkerhetsloven kapittel 10 har regler om eierskapskontroll. Dersom noen ønsker å erverve en «kvalifisert eierandel» i en virksomhet som er underlagt sikkerhetsloven, må dette i henhold til § 10-1 meldes til departementet med ansvar for sektoren. Der virksomheten ikke er omfattet av noe departements ansvarsområde, skal meldingen sendes til sikkerhetsmyndigheten. Det er etablert en screeninggruppe under ledelse av Justis- og beredskapsdepartementet som skal involveres i slike saker.

Departementet eller sikkerhetsmyndigheten som mottar en ervervsmelding, kan i henhold til sikkerhetsloven § 10-2 be relevante organer uttale seg. Dette gjøres ved at NSM, Etterretningstjenesten og PST uttaler seg om utenlandske aktører, risiko og sårbarhet. I tillegg uttaler den aktuelle sektormyndigheten seg, for eksempel Nasjonal kommunikasjonsmyndighet (Nkom) i saker om elektronisk kommunikasjon (ekom).

Slike saker behandles normalt av regjeringens sikkerhetsutvalg (RSU). Dersom det skal stilles vilkår i forbindelse med ervervet eller ervervet skal nektes, kreves det i henhold til § 10-3 vedtak av Kongen i statsråd. Betingelsen er at ervervet kan medføre «en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet».

I tillegg til sikkerhetsloven kapittel 10 om ervervssaker i virksomheter som er underlagt sikkerhetsloven, omfatter § 2-5 også ervervssaker for virksomheter som *ikke* er underlagt sikkerhetsloven. Denne ble brukt da et forestående salg av selskapet Bergen Engines ble stanset ved kongelig resolusjon 26. mars 2021 begrunnet med at nasjonale sikkerhetsinteresser var truet. Bergen Engines er blant annet leverandør og underleverandør til både forsvarssektoren og virksomheter i sivil sektor.

Justis- og beredskapsdepartementet har også utpekt NSM som såkalt nasjonalt kontaktpunkt for motvirkning av sikkerhetstruende økonomisk aktivitet (screeningsaker). Som kontaktpunkt skal NSM bidra i arbeidet til Justis- og beredskapsdepartementets screeningsgruppe. NSM skal også varsle departementet om enkeltsaker, identifisere relevante organer som bør bes om uttalelse, koordinere og utarbeide fremdriftsplaner i de aktuelle sakene og generelt initiere, koordinere og tilrettelegge for dialog og god informasjonsflyt, samt utarbeide risikovurdering basert på innspill fra blant annet Etterretningstjenesten og PST. NSM har siden 2021 jevnlig sendt erfaringsrapporter om arbeidet som nasjonalt kontaktpunkt til Justis- og beredskapsdepartementet med kopi til Forsvarsdepartementet.

Boks 4.3 forts.

Investeringskontrollutvalget anbefaler i NOU 2023: 28 at saker om investeringskontroll behandles i en egen organisatorisk enhet på etatsnivå. Utvalget mente det er «flere hensyn som taler for at en ny ordning for investeringskontroll legges til en egen, ny myndighet, og at det er relevant å vurdere om denne bør organiseres sammen med den nye etaten for eksportkontroll og sanksjoner.»[56]

Investeringskontrollutvalgets rapport ble levert til Nærings- og fiskeridepartementet (NFD) i desember 2023. NFD skrev i Prop. 1 S (2024–2025) at en hovedprioritering for 2025 vil være å «*Utvikle nytt regelverk for investeringskontroll utenfor sikkerhetsloven som skal ivareta nasjonale sikkerhetsinteresser og bidra til at Norge forblir et attraktivt land for utenlandske investeringer.*»

4.2 Andre oppgaver for NSM i henhold til sikkerhetsloven

De oppgavene som er omtalt i avsnittene over, er oppgaver som følger av eller har en tilknytning til kapittel 2 i sikkerhetsloven. Oppgavene beskrevet i § 2-2, utgjør kjernen i NSMs rolle som fagmyndighet etter loven og gjelder innenfor alle fagområder innen forebyggende sikkerhet. I tillegg er NSM gitt oppgaver i andre kapitler i loven. Det gjelder blant annet arbeid med kryptosikkerhet, kontrollvirksomhet, godkjenning av informasjonssystemer, personellsikkerhet og sikkerhetsgraderte anskaffelser.

Kryptosikkerhet og TEMPEST

Krypto er en kortform for kryptosikkerhet som er prinsipper og teknikker for å skjule informasjon slik at bare de(n) som er autorisert, har mulighet til å lese, endre eller slette innholdet. Krypto handler også om tiltak for å skjerme teknikkene mot uvedkommende.

NSM har en sentral rolle som fagmyndighet innen kryptosikkerhet. Kryptosystemer som skal brukes for å beskytte sikkerhetsgradert informasjon, må etter sikkerhetsloven § 5-6 være godkjent av sikkerhetsmyndigheten. Sikkerhetsmyndigheten skal også godkjenne kryptoalgoritmer som brukes i utstyr som skal eksporteres. Videre er sikkerhetsmyndigheten etter § 5-6 «nasjonal forvalter av kryptomateriell og leverandør av kryptosikkerhetstjenester til virksomheter». Sikkerhetsmyndigheten kan godkjenne andre leverandører av kryptosikkerhetstjenester. Cyberforsvaret (CYFOR), det nyetablerte direktoratet Statens graderte plattformtjenester (SGP) og Thales Norge er godkjent av NSM for dette.

[56] NOU 2023:28 *Investeringskontroll*, side 134.

Med bakgrunn i at NSM er forvalter av kryptomateriell, er NSM i forskrift om kryptosikkerhet § 2 gitt i oppgave å produsere kryptonøkler og utgi kryptodokumenter, samt forestå nasjonal distribusjon av kryptomateriell (NDA). Forskrift om kryptosikkerhet angir også en lang rekke andre oppgaver til NSM.

Oppgavene er lagt til NSM blant annet fordi det har vært ansett som hensiktsmessig av sikkerhetsmessige grunner å ha sentralisert kontroll med hvordan kryptosystemer utvikles, spres og håndteres.

En viktig del av arbeidet med sikkerheten rundt kryptosystemer er å ha kontroll på «sidekanaleffekter». Stråling fra elektronisk utstyr som kan gi tilgang til informasjon, såkalt TEMPEST, kan for eksempel kompromittere sikkerheten for informasjon i kryptosystemer og andre kommunikasjonssystemer. I NSMs arbeid med krypto og sikkerhet rundt skjermingsverdige informasjonssystemer er det derfor viktig å følge opp TEMPEST. Både krypto og TEMPEST er spesialiserte fagfelt hvor informasjonen ofte er høyt gradert og hvor kompetanseutviklingen er avhengig av tillitsfullt samarbeid med andre land.

Kontrollvirksomhet

NSM utøver enkelte kontrolloppgaver. De fleste kontrolloppgavene er av teknisk art og skjer på anmodning fra virksomhetene. NSM kan også foreta noen former for kontroller på eget initiativ. NSMs kontrollvirksomhet er ikke del av NSMs tilsyn.

Sikkerhetsmyndigheten kan i henhold til sikkerhetsloven § 5-5 første ledd «undersøke lokaler, bygninger og andre objekter som en virksomhet alene eller sammen med andre råder over, for å fastslå om uvedkommende kan skaffe seg tilgang til sikkerhetsgradert informasjon ved avlytting, innsyn eller avlesning av signaler». Dette omtales som «tekniske sikkerhetsundersøkelser» eller TSU.

Etter forskrift om virksomheters arbeid med forebyggende sikkerhet § 46 skal virksomheter be NSM vurdere om bruk av TSU er nødvendig før et rom eller lokale tas i bruk for muntlig kommunikasjon gradert KONFIDENSIELT eller høyere. Dersom det gjøres vesentlige endringer i slike rom eller lokaler eller ved mistanke om at informasjon er blitt kjent for uautoriserte eller at uvedkommende har hatt adgang, skal virksomheten be NSM om å gjennomføre TSU. Utvalget er kjent med at det er stor pågang for å få vurdert behov og gjennomført slike undersøkelser. NSM kan etter forskrift om virksomheters arbeid med forebyggende sikkerhet § 48 la andre virksomheter utføre slike tekniske sikkerhetsundersøkelser. Slik tillatelse er gitt i noen få tilfeller til andre offentlige virksomheter.

Sikkerhetsmyndigheten kan videre i henhold til sikkerhetsloven § 6-5 første ledd på anmodning fra virksomheter forsøke å trenge inn i virksomhetens skjermingsverdige informasjonssystemer for å kontrollere om sikkerhetstiltakene er tilstrekkelige. Tilsvarende kan sikkerhetsmyndigheten etter sikkerhetsloven § 7-4 første ledd på anmodning «forsøke å forsere etablerte sikkerhetstiltak for å få tilgang til skjermingsverdige objekter eller infrastruktur» for å kontrollere om sikkerhetstiltakene er tilstrekkelige. De som tester sikkerheten «setter seg i fiendens sted» når de utøver sine forsøk på å trenge gjennom sikkerhetstiltakene. NSM kan i henhold til § 62 i forskrift om virksomheters arbeid med forebyggende sikkerhet la andre

virksomheter utføre slik inntrengningstesting og testing av sikkerhetstiltak. Så langt er én offentlig virksomhet godkjent for dette.

TSU, inntrengningstesting og forsøk på forsering av sikkerhetstiltak, er sensitiv aktivitet som krever tilgang på høyt gradert informasjon, spesiell kompetanse og utstyr. Sikkerhetsloven åpner for at erfaringene fra disse områdene kan brukes «til videreutvikling av sikkerhetsmyndighetens generelle sikkerhetsarbeid».

Sikkerhetslovens § 6-6 sier at sikkerhetsmyndigheten etter anmodning kan kontrollere om en virksomhets informasjonssystemer behandler sikkerhetsgradert informasjon utover det systemets sikkerhetsgodkjenning tillater. Forskrift om virksomheters arbeid med forebyggende sikkerhet § 62 første ledd åpner for at NSM kan la andre gjøre dette, men denne hjemmelen er så langt ikke tatt i bruk.

Godkjenning av informasjonssystemer

Skjermingsverdige informasjonssystemer skal etter sikkerhetsloven § 6-3 «godkjennes av en godkjenningsmyndighet». Kongen kan i forskrift utpeke godkjenningsmyndigheter. NSM er i forskrift om virksomheters arbeid med forebyggende sikkerhet § 51 første og andre ledd pekt ut som godkjenningsmyndighet for de mest kritiske, kompliserte eller høyt graderte informasjonssystemene. En virksomhet som rår over et skjermingsverdig informasjonssystem som ikke er nevnt i første eller andre ledd, skal selv godkjenne systemet. NSM og relevante sektortilsyn skal informeres om dette. Det følger av forskrift om virksomheters arbeid med forebyggende sikkerhet § 51 tredje ledd. Godkjenningsmyndighet som etter første og andre ledd er lagt til NSM, kan delegeres til andre.

Godkjenning av skjermingsverdige informasjonssystemer etter første ledd som har avgjørende betydning for funksjonen til et objekt eller en infrastruktur klassifisert KRITISK eller MEGET KRITISK, kan etter forskriften også gjøres av et sektortilsyn. Det må i så fall besluttes av sektordepartementet etter å ha innhentet NSMs vurdering. Hittil er det besluttet at Nasjonal kommunikasjonsmyndighet (NKOM) og Luftfartstilsynet kan godkjenne slike systemer innen egne sektorer. For andre systemer hvor NSM er godkjenningsmyndighet etter andre ledd, kan NSM bestemme at virksomheten selv eller et sektortilsyn kan godkjenne i stedet for NSM. Dette gjelder informasjonssystemer som behandler sikkerhetsgradert informasjon og som a) skal brukes i utlandet, b) har forbindelse til informasjonssystemer i utlandet eller til andre virksomheters informasjonssystemer, c) brukes eller har forbindelser utenfor områder virksomheten kontrollerer, d) har brukere som ikke er sikkerhetsklarert for det graderingsnivået som behandles i informasjonssystemet eller informasjonssystemer dette har forbindelse til, e) behandler informasjon som er gradert HEMMELIG, og som har brukere som ikke skal ha tilgang til all informasjon i informasjonssystemet eller de informasjonssystemer dette har forbindelse til og f) behandler informasjon som er gradert STRENGT HEMMELIG. I øyeblikket har NSM ikke bestemt at andre kan godkjenne slike systemer. Håndtering av NATO-krav til nasjonale graderte systemer som behandler NATO-informasjon, kompetanse hos andre og behov for avstand mellom den som vurderer sikkerheten og den som utvikler og drifter systemene har vært medvirkende årsaker til at NSM har vært tilbakeholdne med å delegere godkjenningsmyndighet til andre.

Evaluering og sertifisering

Når en virksomhet velger sikkerhetstiltak, skal den bruke evaluerte produkter og tjenester dersom produktet eller tjenestenes funksjon i seg selv er avgjørende for å hindre tilgang til gradert informasjon eller mulighet for å overta eller sette ut av drift skjermingsverdige objekter eller infrastruktur. Dette følger av forskrift om virksomheters arbeid med forebyggende sikkerhet § 16. Slik evaluering skal utføres av NSM eller et akkreditert laboratorium utpekt av NSM. I henhold til samme forskrift § 17 kan kravene til evaluering oppfylles gjennom en sertifisering gitt av NSM eller et akkreditert sertifiseringsorgan utpekt av NSM. Akkreditering og sertifisering skal skje etter ISO- og IEC-standarder. NSM har så langt ikke utpekt akkrediterte laboratorier eller sertifiseringsorganer.

Personellsikkerhet

Sikkerhetsloven § 8-1 stiller krav om sikkerhetsklarering, adgangsklarering og autorisasjon. Etter bestemmelsen skal personer som skal få tilgang til sikkerhetsgradert informasjon, autoriseres. Det gjøres av virksomheten der personen skal arbeide. Det samme gjelder for personer som skal ha adgang til skjermingsverdige objekter og infrastruktur.

Personer som skal autoriseres for tilgang til informasjon gradert KONFIDENSIELT eller høyere, må ha gyldig sikkerhetsklarering. Tilsvarende må personer som skal autoriseres for tilgang til skjermingsverdige objekter og infrastruktur, ha gyldig adgangsklarering når sektordepartementet har fattet vedtak om dette, jf. sikkerhetsloven § 8-3.

I henhold til forskrift om sikkerhetsklarering og annen klarering (klareringsforskriften) § 1 klarerer Forsvaret personell i forsvarssektoren, Etterretningstjenesten, PST, NSM og Statsministerens kontor (SMK) personer i eller tilknyttet egen virksomhet. Sivil klareringsmyndighet (SKM) klarerer nødvendige personer ellers i sivil sektor. I Forsvaret er det Forsvararets sikkerhetsavdeling (FSA) som er klareringsmyndighet. SKM og FSA er nærmere omtalt i kapittel 6. NSM og SMK klarerer ikke i dag eget personell, det gjøres av SKM.

Sikkerhetsmyndigheten skal i henhold til sikkerhetsloven § 8-5 første ledd «gjennomføre en personkontroll av alle som skal klareres». Det innebærer å innhente informasjon som kan belyse personens sikkerhetsmessige skikkethet fra ulike offentlige og private kilder og videreformidle denne til klareringsmyndighetene som grunnlag for vurdering og avgjørelse av klareringssaken.

Videre skal NSM i henhold til klareringsforskriften § 18 «utarbeide sikkerhetsmessige vurderinger av relevante staters betydning for norske sikkerhetsinteresser i klareringssaker». Ordningen er ment å være til støtte for klareringsmyndighetenes vurdering av hvilken betydning en tilknytning til et annet land kan ha i en klareringssak. NSM skal formidle vurderingene til klareringsmyndigheten, og «klareringsmyndigheten skal legge vekt på vurderingene i saker der personer som inngår i personkontrollen har tilknytning til andre stater». Denne oppgaven fikk NSM i 2006 da regelverket for personellsikkerhet ble endret på flere områder.

NSM skal videre i henhold til klareringsforskriften § 28 «ha et register over alle klareringsavgjørelser». Opplysninger om klareringsstatus kan utleveres til klareringsmyndigheter og autorisasjonsansvarlige.

NSM er etter sikkerhetsloven § 8-17 andre ledd, og som følge av at SKM klarerer NSMs eget personell, nå felles klageinstans for alle klareringssaker i forvaltningen. For domstolene, Stortinget og Stortingets organer er det etablert særskilte ordninger. SKM er her ikke klareringsmyndighet og NSM er ikke klageinstans. NSM gjennomfører personkontroll og stiller veiledningsmateriell til rådighet også for disse.

Sikkerhetsgraderte anskaffelser

Før en leverandør av varer og tjenester til en virksomhet som er omfattet av loven kan få tilgang til informasjon gradert KONFIDENSIELT eller høyere, skal leverandøren ha gyldig leverandørklarering for angitt sikkerhetsgrad. Leverandøren skal også klareres dersom det er nødvendig av andre grunner, jf. sikkerhetslovens § 9-3. Også der en leverandør skal ha elektronisk tilgang til eller råde over objekt/infrastruktur klassifisert KRITISK eller høyere skal det etter forskrift om virksomheters arbeid med forebyggende sikkerhet § 83 foreligge en leverandørklarering. En leverandørklarering skal bare gis dersom det ikke er noen rimelig grunn til å tvile på at leverandøren er sikkerhetsmessig skikket. I vurderingen skal det bare legges vekt på forhold som kan innvirke på leverandørens evne og vilje til å gjøre forebyggende sikkerhetsarbeid etter loven. Kontroll av personer i leverandørens styre og ledelse skal være en del av vurderingsgrunnlaget.

Kongen utpeker i henhold til sikkerhetsloven § 9-3 en klareringsmyndighet for leverandørklarering. Ifølge klareringsforskriften § 32 skal NSM klarere norske leverandører for sikkerhetsgraderte anskaffelser. I henhold til klareringsforskriftens § 36 skal klareringsmyndigheten før klarering gis, kontrollere at leverandøren oppfyller kravene som stilles til sikring av de skjermingsverdige verdier. Slik kontroll skal senere gjennomføres ved behov, og de kan etter avtale gjennomføres av oppdragsgiveren. NSM skal også føre register over leverandørklareringer og sikkerhetsgraderte anskaffelser, jf. klareringsforskriftens § 39.

4.3 Oppgaver som er gitt til NSM utenfor sikkerhetsloven

Flere av NSMs oppgaver er gitt etter andre hjemmelsgrunnlag enn sikkerhetsloven, se figur 4.1. Det gjelder oppgaver som fulgte med fra Forsvarets sikkerhetstjeneste (FO/S) da NSM ble etablert i 2003 og andre oppgaver som er kommet til i ettertid.

4.3.1 Oppgaver som fulgte med fra Forsvarets sikkerhetstjeneste (FO/S) da NSM ble etablert i 2003

NSM fikk ved etableringen i 2003 med seg flere oppgaver fra Forsvarets sikkerhetstjeneste (FO/S) enn de som fulgte av sikkerhetsloven. Nedenfor følger en oversikt over disse oppgavene der blant annet hjemmelsgrunnlag, målgruppe og historikk er beskrevet.

Lov om oppfinnelser av betydning for rikets forsvar

Grunnlag for oppgaven er hovedinstruksen.

Loven skal gi staten det nødvendige handlingsrommet for å bidra til at oppfinnelser med betydning for forsvaret i Norge kommer rikets sikkerhet til gode og gi behandlingsregler for dette. NSMs oppgaver følger av forskrift om behandling av saker etter lov om oppfinnelser av betydning for rikets forsvar. NSMs oppgaver er å motta søknader, avgjøre om en oppfinnelse er av betydning for rikets forsvar, involvere andre i saksbehandlingen, som primært Forsvarets forskningsinstitutt (FFI) og Patentstyret, treffe vedtak om avståelse eller begrensning i råderett, treffe vedtak om eller oppheve hemmelighold, pålegge beskyttelse, foreta ettersyn og rapportere til regelverksforvalter. I loven ivaretas også internasjonale forpliktelser Norge har på dette området knyttet til hemmelighold av patenter.[57]

Målgruppen er oppfinnere, rettighetshavere, FFI, Patentstyret og Forsvarsdepartementet som regelverksforvalter.

Loven ble første gang vedtatt i 1953 og iverksatt 1. januar 1956. Den sentrale oppfølgingen av loven med tilhørende forskrift ble lagt til Forsvarets sikkerhetstjeneste og fulgte med til NSM da direktoratet ble etablert i 2003. Oppgaven ble vurdert å ha nær tilknytning til sikkerhetsloven og omfattet sivile/private målgrupper. Benevnelsen Forsvarets overkommando i forskriften er ikke endret, men oppgavene er fra 2003 ivaretatt av NSM. Forsvarsdepartementet gjennomførte i 2023 en høring av et forslag til lov om beskyttelse av norsk forsvarsteknologi og sikkerhetsgraderte patenter.[58] Den foreslåtte loven er ment å erstatte lov om oppfinnelser av betydning for rikets forsvar. Forslaget innebærer at NSMs oppgaver på dette feltet avgrenses til å gi råd. Myndighetsutøvelsen foreslås lagt til Forsvarsdepartementet med Forsvarsmateriell som saksforberedende organ.

Forskrift om kontroll med informasjon innhentet med luftbårne sensorsystemer

Grunnlag for oppgaven er hovedinstruksen.

Departementene fastsetter forbudsområder hvor det ikke er tillatt å bruke luftbårne sensorsystemer. Personer som skal betjene slike systemer over forbudsområder eller innhente informasjon om et forbudsområde, må ha tillatelse, være sikkerhetsklarert, ha lisens fra NSM og de må være ansatt i et leverandørklarert operatørselskap. NSM kan sette vilkår for å få lisens, kontrollere innholdet i informasjonen som innhentes og føre tilsyn med opptaksplattformer og sensorsystemer mv. Det følger av regelverket at NSM skal publisere oversikt over forbudsområder med angivelse av hvilke forbud som gjelder.

Målgruppen er departementene, brukere av sensorsystemer som flyfotografer og dronebrukere, leverandørklarerte operatørselskaper, Forsvarsdepartementet som regelverksforvalter.

[57] Iht. *NATO Agreement for the Mutual Safeguarding of Secrecy of Inventions relating to Defence and for which Applications for Patents have been made.*

[58] Forsvarsdepartementet, (15/3310) Høringsnotat – forslag til ny lov om beskyttelse av norsk forsvarsteknologi og sikkerhetsgraderte patenter, datert 4. januar 2023. Frist for høringsinnspill var 13. april s.å.

Regler om kontroll med fotografering fra luften av hensyn til Forsvaret kom første gang i 1946. Disse ble fastsatt i forskriftsform i 1970 og hjemlet i lov om forsvarshemmeligheter. Den sentrale oppfølging av regelverket ble lagt til Forsvarets sikkerhetstjeneste. Oppgaven fulgte med over til NSM i 2003 fordi målgruppen omfattet sivile og private. Lov om forsvarshemmeligheter ble opphevet 1. oktober 2015. Lovhjemmel for ordningen ble først videreført i midlertidig lov om beskyttelse av og kontroll med geografisk informasjon av hensyn til rikets sikkerhet, og fra 2017 i lov om informasjon om bestemt angitte områder, skjermingsverdige objekter og bunnforhold. Virkeområdet til den sistnevnte loven ble utvidet slik at forbudsområdene ikke lenger bare skulle være knyttet til Forsvarets anlegg. Forskriften er i dag også hjemlet i sikkerhetsloven og i luftfartsloven.

Frivillig sertifiseringsordning for IT-sikkerhet i produkter og systemer (SERTIT)

Grunnlag for oppgaven er hovedinstruksen.

Ordningen skal bidra til å styrke tilliten og sikkerheten til IT-produkter og systemer i samfunnet. Ordningen er åpen og tilgjengelig for alle som ønsker å søke om sertifisering. SERTIT arbeider i dag etter to internasjonalt anerkjente rammeverk, Common Criteria og SOG-IS. Norge anerkjenner sertifikater som er utstedt under disse ordningene, og norske sertifikater anerkjennes også av andre land. I tillegg til å utstede sertifikater, godkjenner SERTIT i NSM evalueringsfirmaer og fører tilsyn med disse.

Målgruppen er produsenter og brukere av IT-produkter og løsninger, regelverksforvaltere og andre kravstillere, evalueringsfirmaer.

To sertifiseringsordninger ble foreslått av en arbeidsgruppe under Rådet for IT-sikkerhet (RITS) på slutten av 1990-tallet, én for IT-sikkerhet i organisasjoner og en for IT-sikkerhet i produkter og systemer. FO/S hadde kompetanse innen systemsikkerhet og ble i 1999 ansvarlig for den sistnevnte ordningen som fikk navnet SERTIT. NSM arvet SERTIT fra FO/S i 2003 fordi bruken av ordningen var konsentrert om sivil side. Til støtte for å drifte og utvikle ordningen var det tilknyttet en styringskomite, senere benevnt Fagråd. Dette fagrådet er nå nedlagt. Etterspørselen etter sertifisering under ordningen har vært begrenset, men sertifisering som metode antas å øke når den nokså nye cybersikkerhetsforordningen i EU tas inn i norsk rett.[59]

Oppgaver i Nasjonalt beredskapssystem (NBS)

Grunnlag for oppgaven er hovedinstruksen

Nasjonalt beredskapssystem (NBS) omfatter Beredskapssystem for Forsvarssektoren (BFF) og Sivilt beredskapssystem (SBS). Disse er koordinert innbyrdes og med NATO Response System Manual (NRSM). NBS inneholder også tiltak for å forsterke den defensive forebyggende sikkerheten. NSM bidrar til å utvikle disse sikkerhetstiltakene og har i tillegg ansvar for i visse situasjoner å iverksette bestemte forhåndsdefinerte handlinger for å forsterke sikkerheten.

[59] Europaparlaments- og rådsforordning (EU) 2019/881 av 17. april 2019 om ENISA (Den europeiske unions cybersikkerhetsbyrå), om cybersikkerhetssertifisering av informasjons- og kommunikasjonsteknologi og om oppheving av forordning (EU) nr. 526/2013 (cybersikkerhetsforordningen).

Sikkerhetsloven skal virke i fredstid, ved krise og i krig. Virksomheter har et ansvar for å sikre egen aktivitet og egne verdier også under situasjoner med økt trusselnivå. Nasjonalt beredskapssystem (NBS) gir rammer for hvordan forsterket egenbeskyttelse kan oppnås. Vedtak om tiltak kan etter tiltakenes art og omstendighetene for øvrig fattes i virksomheter, på sektornivå og på nasjonalt nivå. NBS inneholder også andre beredskapstiltak for økt sikkerhet.[60]

Målgruppen er departementer og virksomheter som er omfattet av sikkerhetsloven, Justis- og beredskapsdepartementet og Forsvarsdepartementet som eiere av NBS, Forsvaret og Direktoratet for samfunnssikkerhet og beredskap (DSB) som sentrale utøvere innenfor BFF og SBS.

NSM fikk ved etableringen i 2003 med seg oppgaver med å følge opp sikkerhetstiltakene i Nasjonalt beredskapssystem (NBS). Begrunnelsen for dette var knytningen til sikkerhetslovens bestemmelser om virksomhetenes plikt til å utvikle tiltak for økt sikkerhet i krisesituasjoner.

Støtte norsk kryptoindustri

Grunnlag for oppgaven er hovedinstruksen.

NSM og norsk kryptoindustri samarbeider om utvikling av kryptoutstyr og produkter for nasjonale behov. Norsk kryptoindustri selger utstyr og produkter også til andre land og til internasjonale organisasjoner som NATO. NSM understøtter dette på ulike måter, herunder gjennom kontakt med sikkerhetsmyndigheter i andre land, ved å bistå ved avtaleinngåelser og med støtte ved kurertransporter mv.

Målgruppen er kryptoindustrien.

Av beredskapshensyn har det i hele etterkrigstiden vært en målsetting å være uavhengig av andre land på dette området. Derfor er det blitt opprettet en ordning for å støtte norsk kryptoindustri.

4.3.2 Andre oppgaver som har kommet til etter 2003

Allvis NOR – fra 2014

Oppgaven er omtalt i NOU i 2015,[61] i stortingsmelding fra Justis- og beredskapsdepartementet i 2017,[62] og i budsjettproposisjon for Justis- og beredskapsdepartementet for 2018.[63]

Allvis NOR er et automatisert system for å kartlegge sårbarheter ved virksomheters tilknytning til internett. Systemet benytter en såkalt portskanner til å identifisere hvilke tjenester som er eksponert for utnyttelse. Det gjøres automatiserte tester for å avdekke hvilken programvare som er benyttet i tjenestene. Denne testingen

[60] NSM, PST og Politidirektoratet (POD) har sammen utgitt veiledere i å forebygge og motvirke terrorhandlinger for målgrupper som ikke er omfattet av NBS og sikkerhetsloven.

[61] NOU 2015: 13, *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*, side 257.

[62] Meld. St. 38 (2016–2017), *IKT-sikkerhet. Et felles ansvar,* faktaboks 6.5, s. 26.

[63] Prop. 1 S (2017–2018) *For budsjettåret 2018 under Justis- og beredskapsdepartementet*, side 165.

gjøres jevnlig og oppdateres med informasjon om eventuelle nye sårbarheter som NSM gjøres kjent med. Når det avdekkes en sårbarhet ved hjelp av Allvis NOR, sender NSM et varsel til virksomheten.

Allvis NOR er en gratis og samtykkebasert tjeneste som i dag primært tilbys virksomheter underlagt sikkerhetsloven. Allvis NOR er en tjeneste som også inngår i VDI-avtalene. Allvis NOR gir myndighetene innsikt i sikkerhetstilstanden på internett og bidrar til at utviklingen kan følges over tid. Allvis NOR er et supplement til ordinær inntrengingstesting.

Målgruppen er virksomheter underlagt sikkerhetsloven og virksomheter som eier eller forvalter samfunnsviktig infrastruktur eller tjenester.

Tjenesten kom i gang i november 2014 som et resultat av Dagbladets serie fra 2013/2014 «Null_CTRL». Serien handlet om sviktende datasikkerhet i private hjem, på arbeid og i det offentlige rom. Dagbladet benyttet nettjenesten Shodan for å kartlegge hvilke enheter som var koblet til Internett i Norge. Allvis NOR ble videreutviklet slik at det var mulig å avdekke den spesifikke sårbarheten som ble utnyttet av løsepengeviruset omtalt som «WannaCry» i mai 2017. Allvis NOR ble fremhevet som et viktig tiltak i planen til regjeringens strategi for digital sikkerhet fra 2019.[64]

Det nasjonale fagmiljø for digital sikkerhet – fra 2014

Grunnlag for oppgaven er instruks for sjef Nasjonal sikkerhetsmyndighet fra 2014, tatt inn i hovedinstruksen til NSM i 2019.

NSM skal ifølge hovedinstruksen utføre en rekke oppgaver innen digital sikkerhet, herunder «vedlikeholde et særskilt risikobilde for digital sikkerhet som omfatter statssikkerhet, samfunnssikkerhet og individsikkerhet», og «foreslå tiltak, gi anbefalinger og fremme forslag til krav innen digital sikkerhet i samfunnet, samt følge opp med råd og veiledning».[65] Dette favner videre enn sikkerhetslovens virkeområde. NSM har innenfor rammen av dette oppdraget gjennom flere år utgitt en årlig, ugradert rapport om det digitale risikobildet. NSM har også utgitt grunnprinsipper for IKT-sikkerhet[66] og foreslått hvordan operativ hendelseshåndtering skal foregå i virksomheter, i sektorene og på nasjonalt nivå, jf. «Rammeverk for håndtering av IKT-hendelser» fastsatt av Justis- og beredskapsdepartementet.[67]

Innen digital sikkerhet skal NSM etter hovedinstruksen også koordinere og legge til rette for en «hensiktsmessig samhandling» mellom myndigheter som har oppgaver innenfor forebyggende digital sikkerhet. NSM har blant annet etablert en egen koordineringsgruppe mellom myndigheter som driver IKT-tilsyn. NSM har videre tatt initiativ til å etablere en egen «toppledergruppe» mellom NSM og de mest berørte sektormyndighetene. Flere myndigheter er representert som partnere i Nasjonalt cybersikkerhetssenter (NCSC) i NSM (se omtale nedenfor). NSM støtter

[64] Tiltaksoversikt til nasjonal strategi for digital sikkerhet, tiltak 1.3: Allvis NOR, kartlegging og sårbarhetsundersøkelse.

[65] Hovedinstruks for Nasjonal sikkerhetsmyndighet, side 4.

[66] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/grunnprinsipper-for-ikt-sikkerhet/introduksjon/

[67] Rammeverk for håndtering av IKT-hendelser – Nasjonal sikkerhetsmyndighet.

som sekretariat Justis- og beredskapsdepartementet med å drive Forum for digital sikkerhet. Hensikten med forumet er å sikre at strategiske spørsmål innen digital sikkerhet blir diskutert mellom private og offentlige myndigheter.

Målgruppen er allmennheten, departementene, sektormyndigheter, regelverksforvaltere, Justis- og beredskapsdepartementet i deres samordningsrolle for digital sikkerhet på sivil side.

NSMs rolle som det nasjonale fagmiljøet innen digital sikkerhet utover sikkerhetsloven bygger på oppgaven NSM hadde som sertifiseringsmyndighet for IT-sikkerhet i produkter og systemer, samt de operative oppgavene med å følge opp varslingssystemet for digital infrastruktur (VDI) og oppgaven som nasjonal responsfunksjon (NorCERT). NSM var også i en årrekke sekretariat for Koordineringsutvalget for informasjonssikkerhet (KIS) som nå er nedlagt.

Å gi NSM denne oppgaven hadde også sammenheng med at samordningsansvaret for IKT-sikkerhet på sivil side i 2013 ble flyttet fra det daværende Fornyings-, administrasjons- og kirkedepartementet (FAD) til Justis- og beredskapsdepartementet.

Boks 4.4 Ansvar for digital sikkerhet

Individer og virksomheter er selv ansvarlige for egen digital sikkerhet. Dette ansvaret kan håndteres på ulike måter.

Ved innkjøp av IKT-produkter tilbyr som oftest leverandøren også egne programvarer som skal bidra til å beskytte produktene mot digitale angrep el.

Større virksomheter har i tillegg gjerne egne avdelinger som følger opp den digitale sikkerheten. Noen inngår dessuten avtaler med selskaper som tilbyr tjenester innen digital sikkerhet.

Flere sektorovergripende og sektorspesifikke regelverk stiller krav til digital sikkerhet og hvordan den skal håndteres. Myndighetene som forvalter regelverkene, gir informasjon, råd og veiledning innen sine felt. Også forsikringsselskaper kan stille krav til digital sikkerhet i virksomheter.

NSM har også utarbeidet grunnprinsipper for IKT-sikkerhet som bidrar som informasjon og støtte for både individer, virksomheter, sektormyndigheter og regelverksforvaltere. Det er også andre kilder til mer spesialisert veiledning, nasjonalt og internasjonalt. Å finne fram til slik informasjon er trolig enklere for store virksomheter enn individer og små og mellomstore bedrifter. Ved digitale hendelser må individer og små og mellomstore bedrifter stort sett klare seg selv, men NorSIS i NSM er en ordning som rådgir denne målgruppen.

For virksomheter som er underlagt sikkerhetsloven, stilles det som nevnt særlig krav til sikkerheten, også digital sikkerhet. Virksomhetene er ansvarlige for å opprettholde en forsvarlig sikkerhet etter sikkerhetslovens krav. NSM informerer om risiko, veileder om hvordan kravene skal forstås, gir råd om tiltak, yter bistand, godkjenner og fører tilsyn.

NSM har i oppgave å være nasjonal responsfunksjon for alvorlige digitale angrep. Det er også etablert egne responsmiljøer i en rekke av samfunnets sektorer som sammen med kvalitetsgodkjente private sikkerhetsfirmaer kan gi virksomhetene bistand ved alvorlige hendelser. Disse møtes jevnlig i Nasjonalt cybersikkerhetssenter (NCSC) i NSM og oppdaterer hverandre om erfaringer, risiko og tiltak.

Oppgaver innen forebyggende sikkerhet i sin alminnelighet – fra 2014

Grunnlag for oppgaven er instruks for sjef Nasjonal sikkerhetsmyndighet fra 2014, tatt inn i NSMs hovedinstruks i 2019.

NSM skal vedlikeholde et helhetlig risikobilde innen forebyggende sikkerhet og produsere en årlig rapport om sikkerhetstilstanden, blant annet basert på trusselvurderinger fra Etterretningstjenesten og Politiets sikkerhetstjeneste. Den årlige rapporten benevnes «Risiko» med angivelse av årstall. NSM utarbeidet i 2015 og 2023 i tillegg en rapport med en utvidet tidshorisont tilpasset planprosesser for forsvarssektoren og det sivile samfunnssikkerhetsarbeidet. Disse rapportene ble kalt «Sikkerhetsfaglig råd». I disse rapportene foreslo NSM tiltak for å bedre sikkerhetstilstanden.

NSM samarbeider med andre relevante aktører og skal medvirke til at ansvarsforhold er avklart. Arbeid med forebyggende sikkerhet favner vidt og det skal søkes å unngå overlapp i myndighetsutøvelsen.

NSM skal i henhold til instruksen bidra til å styrke samfunnets kunnskap, forståelse, motivasjon og evne til å ivareta forebyggende sikkerhet og bidra til at departementene har et godt beslutningsgrunnlag for politikkutvikling på det forebyggende sikkerhetsområdet.

NSMs generelle informasjonsvirksomhet omfatter blant annet undervisning, foredragsvirksomhet, publisering av ulike graderte og ugraderte rapporter, aktiv bruk av web-siden, publisering av podcaster og kontakt med media. NSM har siden oppstarten i 2003 holdt en årlig sikkerhetskonferanse. Her holder også andre myndigheter, privat næringsliv og samarbeidspartnere i andre land presentasjoner. NSM informerer også ved å gi ut podcast-episoder.

Sjef NSM skal delta i det offentlige ordskiftet om NSM og forebyggende sikkerhet, og gi selvstendige høringsuttalelser i spørsmål om forebyggende sikkerhet generelt.

Målgruppen er Justis- og beredskapsdepartementet og Forsvarsdepartementet, andre myndigheter med sikkerhetsansvar, allmennheten.

Deteksjonssystem for falske basestasjoner – fra 2016

Grunnlag for oppgaven er presiseringer, endringer og tillegg (PET) nr. 23 til iverksettingsbrevet for langtidsperioden 2013-2016.

Deteksjonssystemet skal oppdage falske basestasjoner som kan bli brukt til sikkerhetstruende virksomhet mot skjermingsverdige verdier. Systemet innebærer et samarbeid med viktige teleoperatører. I tillegg samarbeider NSM med PST og Nasjonal kommunikasjonsmyndighet (NKOM). Systemet kan brukes både stasjonært og mobilt.

Målgruppen er teleoperatører, Nkom, politiet.

Oppdraget om å etablere deteksjonssystemet kom i 2016 etter en rekke oppslag i media. NSM fikk økt sin tildeling med om lag 11 millioner kroner for oppgaven. Justis- og beredskapsdepartementet ga i 2021 NSM i oppdrag å utvide dekningen.

Felles cyberkoordineringssenter (FCKS) – fra 2016

Dette er oppdrag fra Justis- og beredskapsdepartementet, omforent med Forsvarsdepartementet, datert 15. september 2016.

FCKS består av faste representanter for Etterretningstjenesten, Politiets sikkerhetstjeneste (PST), Kripos ved Nasjonalt cyberkrimsenter (NC3) og NSM. Senteret er plassert på Fornebu og ledes administrativt av NSM. Arbeidet til FCKS skal bidra til å styrke den samlede nasjonale evnen til å motstå alvorlige digitale angrep gjennom tidsriktig informasjonsdeling mellom partene, operativ koordinering og etablering og vedlikehold av et felles situasjonsbilde og en felles situasjonsforståelse. Deltakerne er alle representert i senteret på eget rettsgrunnlag. Aktiviteten i FCKS er nærmere regulert i Retningslinjer for cybersamarbeid som er fastsatt av sjefene for EOS-tjenestene og Kripos.[68]

Målgruppen er deltakerne og politiske myndigheter er målgruppe for senterets produkter.

NSMs oppgaver med Varslingssystem for digital infrastruktur (VDI) og oppgaven som nasjonal responsfunksjon (VDI) springer ut av et mangeårig samarbeid mellom E-tjenesten, PST og NSM. Da VDI i 2003 ble lagt til NSM, ble samarbeidet mellom EOS-tjenestene videreført innenfor rammen av ulike koordineringsgrupper.[69] Dette samarbeidet har blitt gradvis mer utvidet og formalisert. I 2016 ble Felles cyberkoordineringssenter (FCKS) opprettet som et fast, samlokalisert fagmiljø bestående av representanter fra NSM, E-tjenesten, PST og nå også Kripos. Initiativet kom fra tjenestene selv, og disse har gitt felles retningslinjer for cybersamarbeidet hvor FCKS inngår. Disse ble senest revidert i 2022. Senteret er omtalt i Nasjonal strategi for digital sikkerhet fra 2019.

Nasjonalt cybersikkerhetssenter (NCSC) – fra 2019

Grunnlag for oppgaven er tildelingsbrev til NSM for 2019.

Senteret bidrar til en fast struktur for samarbeid om digital sikkerhet mellom både ulike myndigheter og virksomheter.

Senteret er organisert etter mønster av tilsvarende sentre i andre land, se kapittel 8. Senteret består av medlemmer fra næringsliv, akademia, Forsvaret og sivil offentlig sektor. Det er en arena for nasjonalt og internasjonalt samarbeid om deteksjon, håndtering, analyse og rådgiving innen digital sikkerhet. VDI og den nasjonale responsfunksjonen, begge oppgaver etter sikkerhetsloven § 2-4, er del av NCSC.

I dag deltar 62 eksterne partnere i senteret. Nettverket med partnere er delt inn i målgrupper for å nå bedre ut med informasjon som er tilpasset den enkelte virksomheten.

Målgruppen er virksomheter omfattet av sikkerhetsloven, medlemmer av VDI-samarbeidet, utpekte sektorvise responsmiljøer (SRM), medlemmer av NSMs

[68] Retningslinjer for cybersamarbeid av 2017 med endringer, senest 2. februar 2022.

[69] *Koordineringsgruppen for IKT-trusselbildet*, etterfulgt av *Cyberkoordineringsgruppen.*

kvalitetsordning for hendelseshåndtering, virksomheter av avgjørende betydning for kritisk digital infrastruktur.

NSM opprettet Nasjonalt cybersikkerhetssenter (NCSC) i 2019. Arbeidet med opprettelsen var omtalt i NOU 2018: 14 om IKT-sikkerhet som ble lagt fram 3. desember 2018[70] og i Nasjonal strategi for digital sikkerhet 2019.[71]

Nasjonalt kontaktpunkt for motvirkning av sikkerhetstruende økonomisk virkemiddelbruk – fra 2021

Oppgaven ble kunngjort av Justis- og beredskapsministeren i Stortinget 19. mai 2021. Tildelingsbrev for 2022 omtaler at NSM har denne oppgaven. Det samme gjør Justis- og beredskapsdepartementets retningslinjer fra 2022 for behandling av saker om sikkerhetstruende økonomisk aktivitet.

NSM er nasjonalt kontaktpunkt for meldinger om oppkjøp og investeringer som kan true nasjonale sikkerhetsinteresser. Dette innebærer at NSM skal kunne motta varsler når det er mistanke om eller det oppdages pågående eller planlagt sikkerhetstruende økonomisk virksomhet. NSM vil så informere rett departement som vil vurdere vedtak etter følgende bestemmelser i sikkerhetsloven:

- § 9-4 som kan stanse eller sette vilkår for anskaffelse til skjermingsverdig informasjonssystem, objekt og infrastruktur
- § 10-3 som kan stanse eller sette vilkår for erverv av virksomheter underlagt sikkerhetsloven
- § 2-5 som kan hindre sikkerhetstruende virksomhet eller annen planlagt eller pågående aktivitet som kan innebære en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet

Kontaktpunktet koordinerer informasjonsinnhenting fra andre, aktuelle etater og bidrar til at departementet får tilgang til et beslutningsgrunnlag med et tilstrekkelig kvalitetsnivå.

Kontaktpunktet gir videre råd og veiledning til virksomheter som skal gjennomføre eller har gjennomført en sikkerhetsgradert anskaffelse der det er grunner for å undersøke nærmere hvorvidt det er innslag av utenlandske interesser i verdikjeden.

Som kontaktpunkt skal NSM ivareta behovet for kapasitet, kunnskapsutvikling/forskning og videreutvikling av screeningmekanismen på sikt.

Målgruppen er beslutningstakere (departementer, regjeringen), meldere (virksomheter, enkeltpersoner), bidragsytere (øvrige EOS-tjenester, andre myndigheter).

I Norge har en screeningmekanisme vært under utvikling siden sikkerhetsloven trådte i kraft i 2019. Mekanismen består i dag av et nettverk mellom departementer ledet av Justis- og beredskapsdepartementet og et nettverk mellom etater ledet av NSM. Oppgaven som nasjonalt kontaktpunkt i NSM kom til etter saken om det mulige salget av Bergen Engines AS til et firma med russiske eierinteresser.

[70] NOU 2018: 14 *IKT-sikkerhet i alle ledd – Organisering og regulering av nasjonal IKT-sikkerhet*, kapittel 17, side 81.

[71] Jf. tiltaksoversikt til nasjonal strategi for digital sikkerhet, tiltak 3, side 10.

Deltakelse i Nasjonalt etterretnings- og sikkerhetssenter (NESS) – fra 2022

Oppgaven er omtalt i tildelingsbrev til NSM for 2023.

E-tjenesten, NSM, PST og det øvrige politiet samarbeider i NESS for å forstå sammensatte trusler og sårbarheter. I senteret utarbeides vurderinger og anbefalinger om tiltak. Etableringen av NESS kommer i tillegg til og endrer ikke FCKS sitt mandat.

Målgruppen er departementene.

Det er lang tradisjon for samarbeid mellom EOS-tjenestene. I og med opprettelsen av Felles kontraterrorsenter i 2014 mellom E-tjenesten og PST[72], og opprettelsen av Felles cyberkoordineringssenter (FCKS) i 2017, fikk dette samarbeidet fastere rammer. I FCKS deltar også NSM og Politiet ved Kripos. Regjeringen besluttet i november 2022 å opprette et nasjonalt etterretnings- og sikkerhetssenter (NESS).

Utvikle og drifte nasjonal myndighetsportal og støtteverktøy for digital sikkerhet – fra 2023

Grunnlag for oppgaven er supplerende tildelingsbrev 2 og 4 til NSM for 2022 og tildelingsbrev for 2023, 2024, og 2025.

Myndighetsportalen skal være en felles inngangsport for ulike brukergrupper, men utformet slik at alle får ensartede råd tilpasset sin brukergruppe. NSM skal lede og koordinere arbeidet med utarbeidelsen av innholdet i portalen.

Støtteverktøyet for digital sikkerhet skal tilbys alle norske virksomheter gjennom nasjonal portal for digital sikkerhet. Verktøyet skal bidra til arbeidet med digital sikkerhet hos virksomhetene, herunder gjøre det lettere å evaluere egen sikkerhetstilstand. NSM skal i utviklingen se hen til liknende løsninger som er utarbeidet i markedet eller av andre i offentlig sektor, og det skal vurderes muligheter for samarbeid.

Målgruppen er alle norske virksomheter og ulike brukergrupper.

I Prop. 78 S (2021–2022) om økonomiske tiltak som følge av krigen i Ukraina ble det lagt planer for å utvikle en myndighetsportal og støtteverktøy for digital sikkerhet som skal tilbys alle norske virksomheter.

I NSMs tildelingsbrev for 2023 står det at NSM skal etablere, forvalte og drifte portalen. Ifølge tildelingsbrevet for 2024 ble rammene for dette arbeidet endret sammenliknet med forutsetningene i Prop. 78 S (2021–2022). Det skal hentes ut gevinster ved å redusere antallet statlige nettsider om digital sikkerhet og driften av disse.

[72] Felles kontraterrorsenter heter i dag Felles etterretnings- og kontraterrorsenter (FEKTS).

Nasjonalt senter for anvendt kryptologi – fra 2023

Grunnlag for oppgaven er tildelingsbrev til NSM for 2022 og 2023.

Senteret skal samle fagpersoner fra myndigheter, akademia og industri for å utvikle og ta i bruk sikkerhetsløsninger som ligger i front av teknologiutviklingen på dette området. Senteret skal bidra til at Norge opprettholder og videreutvikler nasjonal kryptokompetanse og til å gjøre Norge bedre rustet til å møte fremtidens utfordringer innen kryptologi og opprettholde vår internasjonale posisjon. NSMs oppgraderte kryptolaboratorium er en viktig del av senteret. Forsvarsdepartementet har gitt en omfattende tildeling for kryptolaboratoriet over 5 år (2020–2024) for oppgradering og utrustning.

Målgruppen er representanter for myndigheter, akademia og industrien som er involvert i kryptoutvikling.

Trekantsamarbeid mellom myndighetene, industri og akademia har eksistert på kryptofeltet i hele etterkrigstiden. Opprettelsen av senteret i NSM styrker og intensiverer samarbeidet. Det nasjonale senteret ble etablert etter initiativ fra NSM.

Nasjonalt koordineringssenter for forskning og innovasjon innen cybersikkerhet (NCC-NO) – fra 2024

Grunnlag for oppgaven er tildelingsbrev til NSM for 2023.

Senteret er etablert av NSM og Norges forskningsråd (NFR) for å drive veiledning om søknader på forsknings- og investeringsmidler fra EU og nasjonalt. Senteret skal også drive delvis fordeling av slike midler. Senteret skal støtte forvaltningen av EU-midler til cybersikkerhet fra Horisont Europa og DIGITAL, samt andre finansieringsprogrammer i perioden frem til og med 2027. Oppgavefordelingen mellom NFR og NSM er regulert i Norges søknad til EU-kommisjonen fra november 2022. Senteret samarbeider med andre miljøer for å styrke arbeidet med forskning, innovasjon og kompetanse innenfor digital sikkerhet. Dette tiltaket følger opp EUs forordning om å opprette et nettverk av nasjonale koordineringssentre for digital sikkerhet i medlems- og EØS-landene. En viktig oppgave for senteret er å fremme og gi veiledning til søkere ved utlysninger av prosjekter i de europeiske investeringsprogrammene DIGITAL og Horisont Europa innenfor cybersikkerhetsrelaterte utlysninger.

Målgruppen er mulige søkere på forsknings- og investeringsmidler fra EU og nasjonalt.

Koordineringssenteret ble etablert i 2024.

Drift av Norsk senter for informasjonssikring (NorSIS) – fra 2024

Grunnlag for oppgaven er supplerende tildelingsbrev nr. 4/2023.

NorSIS-funksjonen i NSM skal utarbeide og formidle råd og veiledning til allmennheten og små- og mellomstore bedrifter (SMB). Formålet er å bidra til økt kunnskap om digital sikkerhet hos målgruppen(e) ved å bevisstgjøre om trusler og sårbarheter, opplyse om tiltak og påvirke til gode holdninger og sikker atferd. Med innbyggere menes både enkeltindivider som privatpersoner og ansatte i virksom-

heter. Produkter, råd og veiledning som produseres av NorSIS, skal være åpne og tilgjengelige for alle gjennom en egen hjemmeside.

Med virksomhetsoverdragelsen følger ansvaret for

- Å gjennomføre nasjonal sikkerhetsmåned, den årlige kampanjen for økt oppmerksomhet om digital sikkerhet. Av dette følger at NSM/NorSIS er Norges ansvarlige partner i ECSM «European Cyber Security Month» i regi av European Union Agency for Cyber security (ENISA). NSM/NorSIS skal tilrettelegge og koordinere aktiviteten mellom norske aktører.
- Å etablere og videreutvikle møteplasser og arenaer for å bygge kompetanse og erfaring, samt synliggjøre viktige tiltak for bedret digital sikkerhet for målgruppen.
- Å videreføre råd- og veiledningstjenesten slettmeg.no med eventuelle relevante samarbeidspartnere.
- Å følge opp de delene av Nasjonal strategi for digital sikkerhet og Nasjonal strategi for digital sikkerhetskompetanse som tillegges NorSIS.

Målgruppen er primært allmennheten, sekundært SMB-markedet.

NorSIS ble opprinnelig opprettet som et prøveprosjekt med Senter for informasjonssikring (SIS) i 2002. SIS var tilknyttet SINTEF og med daværende Uninett og Institutt for telematikk ved NTNU som deltakere. Det ble igangsatt på initiativ fra Nærings- og handelsdepartementet.

I 2006 reetablerte regjeringen senteret fast under navnet NorSIS som det nasjonale kontaktpunktet for informasjonssikkerhet for små og mellomstore bedrifter, offentlig sektor og privatpersoner. Dette var samtidig med at NorCERT ble etablert som en fast ordning i NSM. Etableringen av NorSIS og NorCERT ble av regjeringen presentert som en samlet satsing. NorSIS ble flyttet fra Trondheim til Gjøvik.

Gi råd til kommuner om digital sikkerhet – fra 2024

Grunnlag for oppgaven er oppdragsbrev 1 og tildelingsbrev til NSM for 2024.

NSM skal gi råd til kommuner om digital sikkerhet.

Målgruppen er kommuner og fylkeskommuner.

Justis- og beredskapsdepartementet bestemte 25. januar 2024 at ansatte i Nasjonalt senter for informasjonssikkerhet i kommunene (Kommune-CSIRT) skulle tilbys ansettelse i NSM. Dette ble bestemt i forbindelse med at sektorvist responsmiljø ble opprettet for kommunesektoren ved HelseCERT. Ressursen skulle ha arbeidssted på Gjøvik og konkrete oppgaver for den enkelte stilling ville være del av overdragelsesprosessen.

4.4 Oppgaver «på vei inn til» NSM

4.4.1 Lov om digital sikkerhet

Lov om digital sikkerhet (digitalsikkerhetsloven) ble vedtatt i 2023, men har ikke trådt i kraft i påvente av at forskrift til loven skal bli ferdig. NSM er i forslaget til forskrift gitt flere oppgaver.[73]

Loven skal innarbeide det såkalte NIS-direktivet fra EU i norsk rett. NIS-direktivet regulerer tiltak for å understøtte et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i EU og EØS. Direktivet pålegger medlemsstatene blant annet å lage en strategi for sikkerhetsarbeidet, etablere en IKT-sikkerhetsberedskapsenhet (CSIRT) og pålegge tilbydere av samfunnsviktige tjenester IKT-sikkerhetskrav og varslingsplikt ved alvorlige IKT-sikkerhetshendelser. De oppgaver som er foreslått for NSM, er i stor grad oppgaver som er parallelle til de NSM allerede har etter sikkerhetsloven. NSM skal holde oversikt over tilbydere av samfunnsviktige tjenester, motta varsler om hendelser, inneha rollen som nasjonalt responsmiljø, veilede om risikovurderinger, være nasjonalt kontaktpunkt mot andre land og EU og utføre enkelte oppgaver overfor virksomheter der disse ikke er underlagt noe departement.

NSM deltar internasjonalt i NIS Coordination Group,[74] og i kommisjonsarbeidsgruppen Cybersecurity Comittee.[75] NSM skal også representere Norge i European Cybersecurity Certification Group (ECCG) og European Cybersecurity Certification Committee (ECCC).

4.4.2 Kompetent PRS-myndighet

Galileos offentlige regulerte tjenester (PRS) er tjenester i satellittnavigasjonsprogrammet Galileo for brukere myndighetene har autorisert og som har særlig behov for robust tilgang uten avbrudd.[76]

Med tilgang til PRS vil brukere kunne benytte Galileo til å navigere med og bestemme posisjon og tid under forhold der den åpne tjenesten er degradert eller utilgjengelig på grunn av signalforstyrrelser. PRS skal gi like god nøyaktighet som den åpne tjenesten, men ha vesentlig større motstandsdyktighet mot såkalt jamming og narring. Det har sammenheng med at tjenesten benytter egne frekvenser med krypterte signaler. Norge har forhandlet med EU om tilgang til tjenesten siden 2017.

Et resultat av avtalen vil være at det etableres en «Competent PRS Authority (CPA)» i Norge. CPA skal forvalte og kontrollere bruken av Galileo PRS, samt følge opp og føre kontroll med industri som utvikler eller produserer PRS-mottakere. Når avtalen

[73] Justis- og beredskapsdepartementet, (24/3567) Høringsbrev – forslag til forskrift til digitalsikkerhetsloven (digitalsikkerhetsforskriften), datert 11. september 2024. Frist for høringsinnspill var 11. desember s.å.

[74] Justis- og beredskapsdepartementets tildelingsbrev til NSM for 2024.

[75] Justis- og beredskapsdepartementets tildelingsbrev til NSM for 2025.

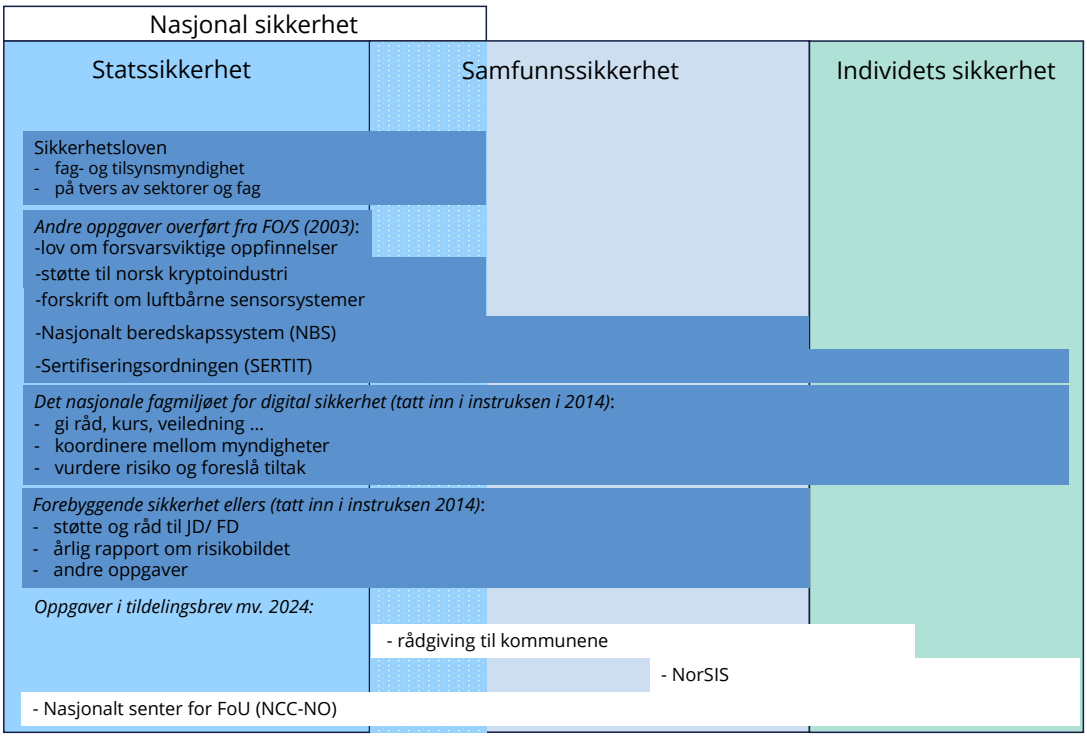
[76] Galileo er et system for satellittnavigasjon som etableres av Den europeiske union og Den europeiske romfartsorganisasjon.

om Galileo PRS er på plass, er NSM tiltenkt oppgaven med å være kompetent PRS-myndighet i Norge (Competent PRS Authority).[77]

4.5 Oppgavene til NSM – en oppsummering

Som omtalt i dette kapittelet, har NSM fått flere oppgaver over tid. I figur 4.2 er oppgavene gruppert omtrent etter samme gruppering som omtalen over. Figuren er inspirert av figur 3.1 og inndelt i områdene statssikkerhet, samfunnssikkerhet, nasjonal sikkerhet og individets sikkerhet.

Figur 4.2 NSMs oppgaver og nasjonal sikkerhet, statssikkerhet, samfunnssikkerhet og individets sikkerhet[1)]



[1)] Ikke alle NSMs oppgaver er tatt med. Plasseringen av de ulike gruppene antyder hvilke områder i arbeidet med sikkerhet de dekker, men den kan ikke bli helt nøyaktig.

Den øverste gruppen med oppgaver i figuren er de som følger av sikkerhetsloven. Sikkerhetsloven er en lov om *nasjonal sikkerhet*. Enkelte oppgaver i loven har likevel et noe bredere nedslagsfelt en nasjonal sikkerhet.

Da NSM ble opprettet, arvet NSM flere oppgaver fra Forsvaret. Disse fremkommer i den andre gruppen oppgaver. Formålet for flere av disse er at de først og fremst skal ivareta statssikkerheten, som er noe smalere enn nasjonal sikkerhet. Enkelte

[77] Meld. St. 10 (2019–2020) *Høytflyvende satellitter – jordnære formål, side 25*.

av oppgavene som NSM arvet, omfatter også samfunnssikkerhetsområdet. Sertifiseringsordningen SERTIT, kan strekke seg ut i området for individets sikkerhet.

I 2014 ble det tatt inn i hovedinstruksen at NSM skal være «*det nasjonale fagmiljøet for digital sikkerhet*». NSM hadde allerede da hatt oppgaver innen digital sikkerhet, også etter sikkerhetsloven. Oppgaven som følger av å være «det nasjonale fagmiljøet for digital sikkerhet» favner vidt. NSMs hovedinstruks sier blant annet at NSM skal vedlikeholde et særskilt risikobilde for digital sikkerhet «som omfatter statssikkerhet, samfunnssikkerhet og individsikkerhet», foreslå tiltak og gi anbefalinger mv.

Den fjerde gruppen omhandler oppgaver med forebyggende sikkerhet som også ble tatt inn i hovedinstruksen i 2014. Blant annet skulle NSM gi støtte og råd til Justis- og beredskapsdepartementet og Forsvarsdepartementet og gi ut en årlig rapport om risikobildet.

Videre fikk NSM flere nye oppgaver innen digital sikkerhet i 2024. Blant disse var å opprette et nasjonalt koordineringssenter for cybersikkerhet sammen med Norges forskningsråd, overta kommuneCSIRTs oppgave med å gi råd til kommunene om digital sikkerhet og å ta over NorSIS på Gjøvik.

5 Styring og finansiering av Nasjonal sikkerhetsmyndighet

Dette kapittelet omhandler hvordan styringslinjer og rapportering mellom Justis- og beredskapsdepartementet, Forsvarsdepartementet og NSM fungerer i dag, formelt og i praksis. I denne sammenhengen har utvalget også sett på hvordan NSM finansieres.

5.1 Styringsdokumenter og styringsdialog

Det administrative ansvaret for oppfølgingen av NSM ble overført fra Forsvarsdepartementet til Justis- og beredskapsdepartementet i 2019, jf. kgl.res. 3. mai 2019. Det innebærer blant annet at Justis- og beredskapsdepartementet fremmer forslag om NSMs budsjett og samordner styringssignalene fra Justis- og beredskapsdepartementet og Forsvarsdepartementet til NSM. Ordningen av 2019 er en «speilvending» av disse departementenes roller fram til 2019.

NSMs «hovedinstruks» er fastsatt av Justis- og beredskapsdepartementet og Forsvarsdepartementet i fellesskap og trådte i kraft 3. mai 2019. Denne erstattet direktoratets første instruks fra 2014. Instruksen av 2019 angir NSMs myndighet, ansvar og oppgaver. Justis- og beredskapsdepartementet har det administrative ansvaret for NSM. Begge departementene har instruksjonsmyndighet i saker innenfor egne ansvarsområder. Når NSM på vegne av Forsvarsdepartementet bidrar i det forebyggende sikkerhetsarbeidet i forsvarssektoren, har dette departementet dermed myndighet til å innvirke på NSMs arbeid og prioriteringer av oppgaver. NSM er slik en virksomhet tilknyttet forsvarssektoren.

Justis- og beredskapsdepartementet utsteder i samarbeid med Forsvarsdepartementet de årlige tildelingsbrevene, supplerende tildelingsbrev, oppdragsbrev og presiseringsbrev til NSM. Etter at regjeringen har lagt fram sitt budsjettforslag i oktober, sender Justis- og beredskapsdepartementet et utkast til tildelingsbrev til NSM for kommende budsjettår. Det er dialog mellom departementene og NSM i arbeidet med utforming av tildelingsbrevet. NSM får anledning til å komme med innspill, og ambisjonsnivået for kommende år drøftes som en del av dialogen. Hovedprioriteringer for NSM i det påfølgende året behandles i regjeringen i november eller desember, blant annet basert på trusselrapporter fra Etterretningstjenesten og Politiets sikkerhetstjeneste (PST) og risikovurderinger fra NSM. Endelig tildelingsbrev sendes ut etter at Stortinget har vedtatt budsjettet i desember.

NSM rapporterer til Justis- og beredskapsdepartementet med kopi til Forsvarsdepartementet i henhold til fastsatt styringskalender for budsjettåret. I tillegg til årsrapporten for det foregående året, rapporterer NSM etter første og andre

tertial i inneværende år. Departementene kan be om rapportering også utenom disse faste tidspunktene. NSM rapporterer om noen oppgaver innen forsvarssektoren til Forsvarsdepartementet med kopi til Justis- og beredskapsdepartementet, og i enkelte saker som omhandler Norges forpliktelser overfor NATO, bare til Forsvarsdepartementet.

Justis- og beredskapsdepartementet sørger for at det avholdes jevnlige etatsstyringsmøter med NSM. Forsvarsdepartementet deltar i disse møtene. I et normalår gjennomføres tre ordinære etatsstyringsmøter mellom departementene og NSM: Ett årsrapportmøte i april om resultater for foregående år og to møter i henholdsvis juni og oktober om tertialrapportene. Møtene følger en fast dagsorden med blant annet gjennomgang av rapporter, budsjettprognose og vurdering av risiko for at NSM ikke innfrir resultatforventninger i tildelingsbrevet. Det kan også avholdes særmøter om spesielle tema som det eventuelt ikke blir tid til å behandle i de ordinære etatsstyringsmøtene. Begge departementene gjennomgår og godkjenner referatene fra møtene.

Departementene la i styringsdialogen med NSM i siste halvdel av 2023 og hele 2024 vekt på å følge opp virksomhetens økonomistyring og internkontroll. Bakgrunnen var at NSM i 2022 og 2023 hadde ambisjoner og planer som ikke var tilpasset virksomhetens gjeldende rammer, se også omtale av finansieringen av NSM nedenfor. Det ble fra juni 2023 og gjennom hele 2024 avholdt månedlige etatsstyringsmøter med NSM av denne grunn. Månedlige møter om økonomistyring og internkontroll videreføres ikke i 2025, men oppfølging av internkontrollen vil ifølge Justis- og beredskapsdepartementet fortsatt være et sentralt tema i styringsdialogen.

Departementene avholder normalt et årlig strategimøte med NSM om utfordringer og videre utvikling av virksomheten i et mer langsiktig perspektiv. På grunn av de økonomiske utfordringene har det ikke vært avholdt strategimøte med NSM siden våren 2023. Ifølge Justis- og beredskapsdepartementet planlegges det et nytt strategimøte i løpet av 2025.

5.2 Finansiering av NSM

NSM er en ordinær bruttobudsjettert, statlig virksomhet som finansieres over statsbudsjettet. NSMs utgifter til drift og investeringer bevilges som en utgift på statsbudsjettet. I tillegg kan NSM ta brukerbetaling for enkelte tjenester som budsjetteres som en inntektsbevilgning i statsbudsjettet.

Da Justis- og beredskapsdepartementet overtok det administrative ansvaret for oppfølgingen av NSM i 2019, ble de daværende driftsutgiftene til NSM i sin helhet overført til og bevilget under Justis- og beredskapsdepartementets budsjett mot en tilsvarende reduksjon under Forsvarsdepartementets budsjett. Tilsvarende ble

gjort for NSMs driftsinntekter.[78] NSM mottar i tillegg drifts- og investeringsmidler fra Forsvarsdepartementet, hovedsakelig til ulike prosjekter. Fra 2024 mottar NSM også budsjettmidler fra Digitaliserings- og forvaltningsdepartementet til finansiering av tiltak for digital sikkerhet i kommunesektoren i forbindelse med at NSM har overtatt oppgaver fra KommuneCSIRT, se omtale i kapittel 4. NSM mottar i 2024 og 2025 også budsjettmidler fra Kunnskapsdepartementet i forbindelse med oppdraget «Kunnskapsgrunnlag for vurdering av sensitive teknologier».

Utvalget som våren 2024 gikk gjennom forholdene rundt NSMs leie av Snarøyveien 36, pekte på at det er forskjellig praksis for budsjettering av underliggende virksomheter i Justis- og beredskapsdepartementet og Forsvarsdepartementet.[79] Utvalget viste til at Forsvarsdepartementet i større grad praktiserer en helhetlig rammestyring og en form for porteføljestyring av investeringer innenfor rammen av forsvarssektorens langtidsplan. Justis- og beredskapsdepartementets etater styres fullt ut med egne, årlige budsjetter for drift og investeringer.

Budsjettsystemet i Norge er orientert rundt ettårsprinsippet der framlegget av statsbudsjettet om høsten avklarer nye bevilgninger. NSM kan årlig sende forslag til Justis- og beredskapsdepartementet om økte bevilgninger som departementene vurderer i prosessen fram mot budsjettet legges fram. NSM har også anledning til å komme med forslag til budsjettjusteringer i det reviderte budsjettet i mai (RNB) og ved nysalderingen av budsjettet i november. I henhold til Finansdepartementets retningslinjer skal slike budsjettforslag gjennom året likevel begrenses til strengt nødvendige tillegg og endringer som kan skyldes ny informasjon og endrede forutsetninger som må håndteres raskt.

[78] Prop. 57S (2018–2019) og Innst. 236S (2018–2019). Som følge av endringene i departementsstrukturen og i ansvarsdelingen mellom departementene våren 2019, vedtok Stortinget den 25. april 2019 å bevilge 316,4 mill. kroner under nytt kap. 457 *Nasjonal Sikkerhetsmyndighet*, post 01 Driftsutgifter under JD, mot tilsvarende reduksjon under Forsvarsdepartementets kap. 1723, post 01.Videre ble det bevilget 11,9 mill. kroner under nytt Kap. 3457, post 01 Driftsinntekter, mot tilsvarende reduksjon under kap. 4723, post 01.

[79] Rapporten *NSMs leie av Snarøyveien 36*, avlagt 1. mars 2024 fra et utvalg oppnevnt av regjeringen 15. desember 2023, side 12.

Tabell 5.1 NSMs disponible midler i perioden 2015–2025 i faste 2025-priser

Dep.	Kap/post*	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
	Utgifter											
FD/JD	1723/01 457/01**	313,8	340,9	402,3	398,8	440,4	465,5	434,5	476,4	512,4	568,0	527,2
JD	457/21									216,4	54,7	
JD	457/45						25,0	43,0	71,1	53,6	35,8	13,2
FD	1700/01										0,5	0,5
FD	1710/47							8,4				
FD	1760/01	10,0	6,7	14,6	10,6	13,2	28,8	47,2	46,0	47,5	38,0	7,3
FD	1760/45	34,2	51,5	30,6	29,1	33,7	48,4	52,0	110,0	71,2	76,7	127,9
KD	0288/21										0,6	
DFD	1541/22										5,8	
Sum		358,0	399,1	447,6	438,5	487,3	567,8	585,1	703,6	901,0	780,1	676,1
	Inntekter**											
JD	**3457/01**	**20**	**25**	**44,1**	**33,2**	**34,4**	**33,8**	**29,7**	**20,6**	**46,3**	**43,9**	**37,5**

* Kilde: Tallene for 2015–2024 er hentet fra NSMs årsrapporter og inkluderer overføringer fra foregående år. Tallene for 2025 er hentet fra tildelingsbrev til NSM for 2025. Det framgår av tildelingsbrevet at NSM i 2025 vil bli gitt belastningsfullmakter fra DFD og KD, men beløpene er ikke oppgitt.

** Driftsutgiftene til NSM ble bevilget under Forsvarsdepartementets kap. 1723, post 01 t.o.m. 2018. Fra 2019 ble midlene overført til Justis- og beredskapsdepartementet og bevilges der under kap. 457, post 01. Inntektene ble tilsvarende bevilget under Forsvarsdepartementets kap. 4723, post 01 t.o.m. 2018 og fra 2019 under Justis- og beredskapsdepartementets kap. 3457/post 01.

5.2.1 Utgifter

Bevilgningen på kap. 457 Nasjonal sikkerhetsmyndighet fremmes av Justis- og beredskapsdepartementet og skal i utgangspunktet dekke ordinære drifts- og investeringsutgifter for NSM. I årene 2022 og 2023 innrettet NSM virksomheten ut fra en forventning om å få økte økonomiske rammer i fremtidige budsjettvedtak.[80] NSM reduserte kostnadene gjennom 2024 for å bringe forbruket mer i samsvar med bevilget budsjett. Tiltakene ga imidlertid ikke store nok innsparinger til å bringe budsjettet i balanse. For at NSM fortsatt skulle kunne ivareta sitt samfunnsoppdrag, og for å unngå uhjemlet merforbruk, bevilget Stortinget ekstra midler til NSM både i nysalderingen av budsjettet for 2023 (20 mill. kroner) og i RNB 2024 (90 mill. kroner).[81] NSM fikk ved nysalderingen av budsjettet for 2023 dessuten en ekstraordinær bevilgning på 200 mill. kroner til sanering av lån som ble tatt opp til finansiering av en ekstra oppgradering av bygg til leie på Fornebu.[82]

[80] NSM økte bemanningen og inngikk ny leieavtale i forbindelse med samlokalisering av direktoratet. Dette utløste forpliktelser til lønn og husleie som langt oversteg bevilgningen for 2024.

[81] Prop. 19 S (2023–2024) og Innst. 143 S (2023–2024), samt Prop. 104 S (2023–2024) og Innst. 447 S (2023–2024).

[82] Prop. 34 S (2023–2024) og Innst. 150 S (2023–2024). Deler av tilbakebetalingen ble forskjøvet til 2024, og ubrukt bevilgning fra 2023 ble overført til 2024. Forpliktelsene er nå innfridd og post 21 er avviklet.

Tildelingen under kap. 457, post 45 er til definerte investeringer. I 2025 skal den dekke videreutvikling av en nasjonal portal for digital sikkerhet og nasjonalt støtteverktøy for digital sikkerhet.

Midlene NSM får stilt til disposisjon fra Forsvarsdepartementet er i stor grad øremerkede midler som skal dekke blant annet utgifter til sikkerhetsgodkjenning av informasjonssystemer i forsvarssektoren og FoU-relaterte prosjekter. NSM har i tillegg adgang til å fakturere Forsvaret for dokumenterte utgifter til sikkerhetsgodkjenning av informasjonssystemer utover midlene som er stilt til disposisjon for dette formålet. Denne adgangen benyttet NSM seg av første gang i 2024. Midlene til FoU og FoU-relaterte prosjekter går til en nokså bred portefølje av prosjekter. Prosjektenes varighet er normalt ett til tre år. De fleste prosjektene er gradert BEGRENSET eller høyere. Prosjektene følges opp med prosjektrådsmøter mellom Forsvarsdepartementet og NSM. Justis- og beredskapsdepartementet deltar også og får slik blant annet innsyn i eventuelle langsiktige lønns- og driftsforpliktelser fra prosjektene som vil kunne belaste bevilgningen under kap. 457. Finansiering av FoU-relaterte prosjekter har ligget stabilt i perioden siden 2019 på rundt 30 mill. kroner årlig.

Det er i årene 2020-2023 dessuten stilt midler til disposisjon over forsvarsbudsjettet for utvikling av varslingssystemet for digital infrastruktur (VDI) og høyteknologisk kryptolaboratorium. Disse prosjektene er i ferd med å bli avsluttet. I 2025 tilføres NSM prosjektmidler med basis i den nye langtidsplanen for forsvarssektoren.

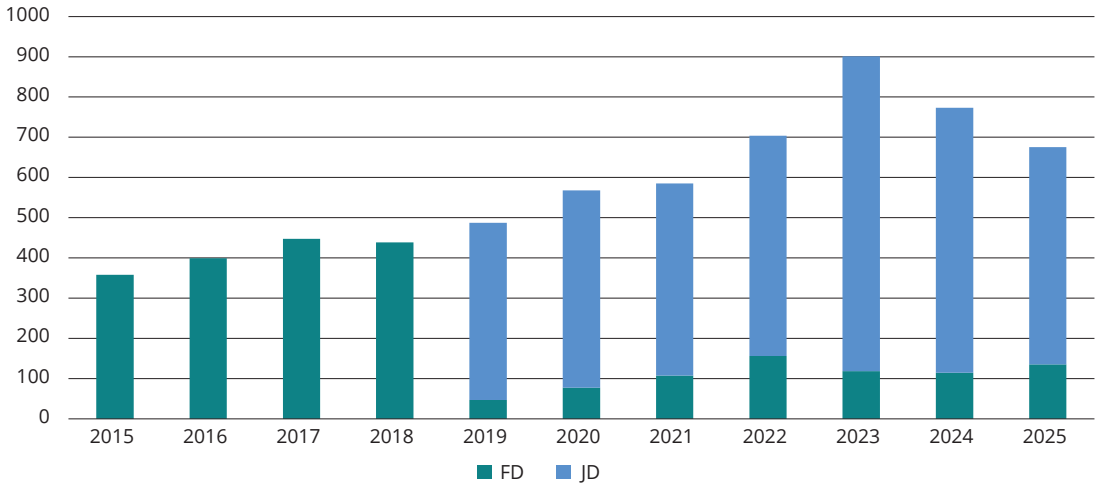
5.2.2 Inntekter

NSM kan i en viss utstrekning ta brukerbetaling for tjenester de utfører. Inntektene fra slike tjenester kommer i hovedsak fra medlemsavgifter fra næringslivet til VDI, avtale med Forsvarsmateriell om militær anvendelse av skytjenester (MAST), kurs- og konferanseavgifter og brukerbetaling ved sikkerhetsgodkjenning av informasjonssystemer. NSM har fullmakt til å overskride bevilgningen under kap. 457, post 01 mot tilsvarende merinntekt under kap. 3457, post 01. NSM har videre en avtale med Forsvaret ved Cyberforsvaret om å videreutvikle VDI. Avtalen er inngått for 20 år fra 2023, og prosjektet finansieres ved at NSM får dekket kostnadene av Cyberforsvaret.

5.2.3 Utvikling i NSMs økonomiske rammer

NSMs driftsutgifter økte kraftig i 2022–2024 som følge av den økte bemanningen og leieavtalen som ble inngått. I 2025 synes driftsutgiftene å være tilbake på normalt nivå. NSMs samlede økonomiske rammer i 2025 er likevel reelt sett økt med nær 90 prosent sammenliknet med 2015. Hvis vi sammenlikner med 2019, da Justis- og beredskapsdepartementet overtok det administrative ansvaret, er den samlede rammen i 2025 økt med nær 40 prosent. Vesentlige deler av dette kan forklares av økte midler til å forbedre digital sikkerhet, både innen forebygging, avdekking og håndtering av hendelser, jf. Prop. 78 S (2021–2022) (Ukrainaproposisjonen) og Innst. 270S (2021–2022).

Figur 5.1 Midler stilt til disposisjon for NSM fordelt på Forsvarsdepartementet og Justis- og beredskapsdepartementet[1)]

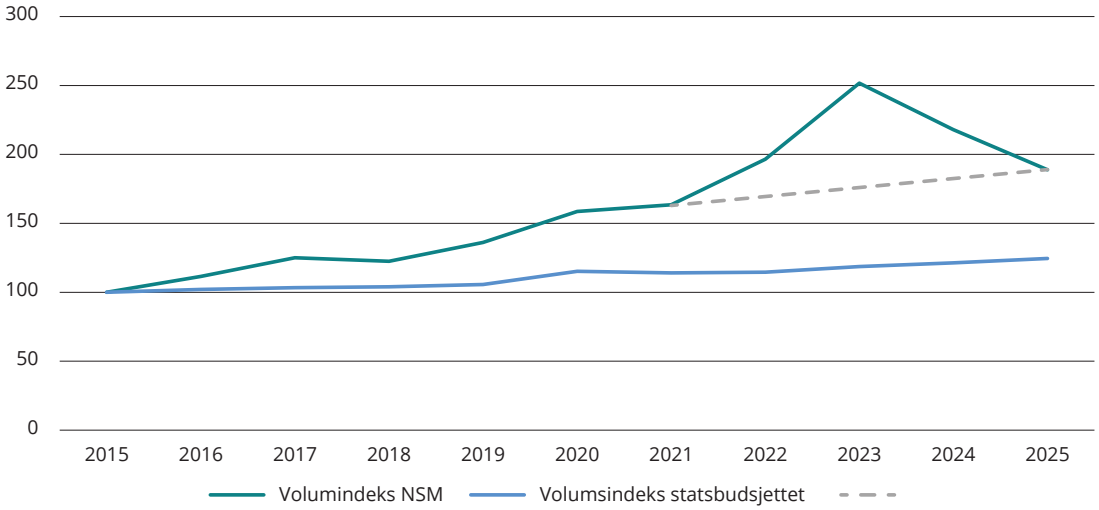


[1)] Omregnet til faste 2025-priser.

Kilde: Se tabell 5.1 ovenfor

I årene 2015–2018 da Forsvarsdepartementet var administrativt ansvarlig departement for NSM, var tildelingene til driften en del av Forsvarsdepartementets budsjett (grønne søyler). Den ordinære driftsbevilgningen ble som nevnt i sin helhet overført til Justis- og beredskapsdepartementets budsjett (blå søyler) da NSM ble overført i 2019. Forsvarsdepartementet tilfører likevel fortsatt midler til noen tiltak og prosjekter.

Figur 5.2 Endring i NSMs disponible midler sammenlignet med statens samlede utgiftsøkning 2015–2025 [1)]



[1)] Volumindekser, 2015 = 100.

Kilde: Se tabell 5.1 ovenfor, Meld. St. 3 (2023–2024) Statsrekneskapen 2023, Meld. St. 1 (2024–2025) Nasjonalbudsjettet 2025.

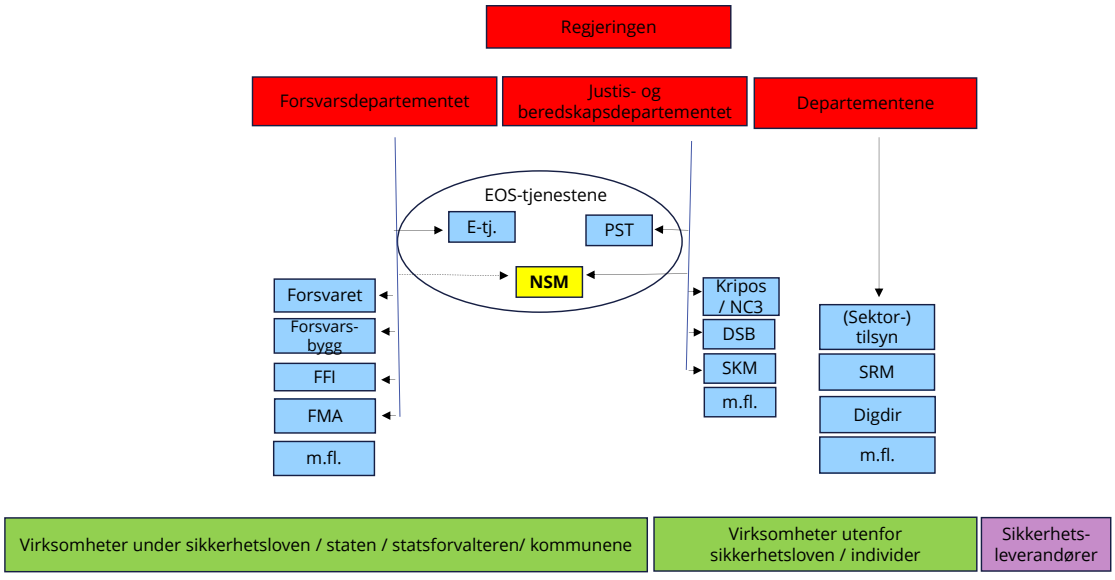
Figur 5.2 viser at NSMs disponible midler har økt mer enn de samlede utgiftene over statsbudsjettet i perioden 2015–2025. Det skyldes særlig en noe sterkere vekst i årene fram til 2021, men også fra 2021 til 2025 har de økonomiske rammene til NSM vokst noe raskere enn statens samlede utgifter.

6 Tilgrensende myndigheter

Mandatet ber utvalget vurdere om grensesnittet mot andre, tilgrensede statlige virksomheter er «tilstrekkelig avklart og effektivt organisert». Dersom noen av dagens oppgaver «dupliseres eller av andre grunner kan utføres av andre på en mer hensiktsmessig og effektiv måte», bør disse vurderes overført. Utvalget skal konsentrere oppmerksomheten sin om «de mest tilgrensede og eventuelt overlappende» oppgavene og virksomhetene. Tilsvarende skal utvalget også vurdere om det er oppgaver som bør overføres til NSM der dette vil bidra til å samle nasjonal innsats på viktige områder, eller om det er oppgaver som kan løses i partnerskap med næringslivet.

Virksomhetene som omtales nedenfor, er ikke uttømmende for hvilke som har grenseflater mot NSM. De vurderes imidlertid å være blant de mest sentrale.

Figur 6.1 NSM har en sentral plass i arbeidet med forebyggende sikkerhet [1)]



[1)] Mange aktører er involvert i arbeidet med forebyggende sikkerhet. Figuren er en forenkling av virkeligheten. Figuren viser sentrale myndigheter og virksomheter som tar del i dette arbeidet, fra regjeringen og ned til enkeltvirksomheter. Den ovale figuren markerer at NSM sammen med E-tjenesten og PST er en av EOS-tjenestene. Det er oppgaver både innenfor og utenfor sikkerhetslovens virkeområde. Forkortelsene i figuren er forklart i Vedlegg 2.

6.1 EOS-tjenestene

Etterretnings-, overvåkings- og sikkerhetstjenestene (EOS-tjenestene) omfatter Etterretningstjenesten (E-tjenesten), Politiets sikkerhetstjeneste (PST) og Nasjonal sikkerhetsmyndighet (NSM). De kalles også de hemmelige tjenester, og skal alle bidra til å verne rikets sikkerhet. Nedenfor omtales E-tjenesten og PST nærmere. De er begge sentrale samarbeidspartnere for NSM.

6.1.1 Etterretningstjenesten (E-tjenesten)

E-tjenesten er Norges utenlandsetterretningstjeneste og har som oppgave å skaffe rettidig, pålitelig og relevant informasjon som beslutningsgrunnlag for militære og sivile myndigheter. Norsk utenlandsetterretning er et sikkerhetspolitisk virkemiddel som skal bidra til å beskytte Norges suverenitet, territorielle integritet, demokratiske styreform og andre nasjonale sikkerhetsinteresser. E-tjenestens hovedoppdrag er å varsle om ytre trusler mot Norge og nasjonale sikkerhetsinteresser, støtte Forsvaret, allierte og partnere, samt understøtte politiske beslutningsprosesser med informasjon av betydning for norsk utenriks-, sikkerhets- og forsvarspolitikk.[83]

E-tjenesten er en del av Forsvaret og underlagt Forsvarsdepartementet. E-tjenestens oppgaver følger av lov om etterretningstjenesten (etterretningstjenesteloven). E-tjenesten sikkerhetsklarerer eget personell.

E-tjenesten bidrar med etterretning og vurderinger av trusler til både NSM og PST. NSM bruker informasjonen i sine risikovurderinger og til å videreutvikle sikkerhetstiltak. Slik informasjon kan også lede til at forhåndsplanlagte beredskapstiltak om økt sikkerhet iverksettes.

E-tjenesten deltar sammen med NSM, PST og Kripos i Felles cyberkoordineringssenter (FCKS) som ble etablert i 2017, se også kapittel 4. FCKS er et samarbeid for å dele informasjon og koordinere håndtering av alvorlige cyberhendelser. Partene deltar i samarbeidet på eget rettsgrunnlag. FCKS ledes administrativt av NSM. Samarbeidet er regulert i avtale mellom partene.[84] Sjefene for de deltakende partene igangsatte våren 2024 et arbeid for å videreutvikle cybersamarbeidet. FCKS er en del av dette.

E-tjenesten deltar også i samarbeidsorganet Nasjonalt etterretnings- og sikkerhetssenter (NESS) sammen med NSM, PST og det øvrige politiet. NESS ble opprettet i 2022 av Justis- og beredskapsdepartementet i samråd med Forsvarsdepartementet med formål å styrke nasjonal evne til å identifisere, bygge forståelse for og gi beslutningsstøtte til sammensatte trusler. Senteret ledes administrativt av PST. Samarbeidet i NESS er regulert i felles retningslinjer vedtatt av sjefene for EOS-tjenestene og politidirektøren.[85] Samarbeidet er i 2024 blitt evaluert og skal videreutvikles.

[83] Prop. 1 S (2024–2025) for budsjettåret 2025 under Forsvarsdepartementet.

[84] Retningslinjer for cybersamarbeid, fastsatt 20. mars 2017 med endringer, senest 2. februar 2022.

[85] Retningslinjer for samarbeidet i Nasjonalt etterretnings- og sikkerhetssenter (NESS), gradert BEGRENSET iht. sikkerhetsloven, fastsatt 26. juni 2023.

6.1.2 Politiets sikkerhetstjeneste (PST)

PSTs primære ansvar er å forebygge, avverge, håndtere, etterforske og iretteføre de mest alvorlige truslene mot rikets sikkerhet og grunnleggende nasjonale interesser. Som ledd i dette, skal tjenesten identifisere, vurdere og håndtere trusler fra fremmede staters virkemiddelbruk i Norge. Det kan dreie seg om etterretningsoperasjoner, sabotasje eller påvirkningsoperasjoner. I tillegg skal tjenesten forebygge og avverge terrorhandlinger i Norge. PSTs ansvar gjelder både i det fysiske og det digitale domenet. Tjenesten utarbeider analyser og trusselvurderinger som underlag for myndighetenes og andre aktørers beslutninger. PST har også ansvaret for livvakttjenesten for myndighetspersoner.[86] PST er både en innenlands etterretningstjeneste, en polititjeneste og en sikkerhetstjeneste.[87]

PST er underlagt Justis- og beredskapsdepartementet. Samfunnsoppdraget følger av politiloven § 17 og utfyllende regler om PSTs virksomhet er fastsatt i Instruks for politiets sikkerhetstjeneste med hjemmel i politiloven.[88] PST består av Den sentrale enhet (DSE) og elleve distriktsenheter, én i hvert politidistrikt. Etterforskning og straffesaksbehandling innenfor PSTs område er underlagt riksadvokatens faglige ledelse.[89]

Mens PST arbeider med å avdekke og forebygge sikkerhetstrusler innenfor landets grenser, har NSM ansvaret for å identifisere risiko og sårbarheter som kan utnyttes av fiendtlige trusselaktører. PST skal forebygge og avverge at en aktør gjennomfører spionasje, sabotasje, terrorhandlinger mv. NSM skal blant annet gjennom krav, informasjon, veiledning mv. legge til rette for at virksomhetene selv sikrer sine objekter, infrastruktur, systemer, informasjon og aktiviteter mot det samme, se nærmere omtale av NSMs oppgaver i kapittel 4.

Begge etatene gir råd om tiltak som myndigheter og virksomheter kan iverksette for å ivareta den nasjonale sikkerheten. NSM veileder innenfor fagområdene fysisk sikkerhet, personellsikkerhet, digital sikkerhet og sikkerhetsstyring, mens PST blant annet gir råd om tiltak for å ivareta virksomheters og myndighetspersoners sikkerhet i særskilte situasjoner, herunder politioperative sikkerhetstiltak.[90] PST skal også gi råd til myndigheter og virksomheter. Her kan det være gråsoner mot NSMs plikt til å veilede og å gi råd, og PST og NSM inngikk i 2020 en avtale om koordinering av virksomhetenes sikkerhetsfaglige rådgiving mot felles målgrupper.[91]

PST og NSM bidrar til hverandres oppgaveløsning. PST er en viktig kilde til opplysninger for NSMs arbeid med å klarere leverandører etter sikkerhetsloven og til NSMs personkontroll som grunnlag for sikkerhetsklareringer. Videre er PSTs vurdering av trusselbildet et viktig underlag for NSMs anbefalinger om tiltak for å oppnå

[86] Medlemmer av Kongehuset, Stortinget, regjeringen og Høyesterett.

[87] Prop. 1 S (2024–2025) for budsjettåret 2025 under Justis- og beredskapsdepartementet.

[88] Instruks for Politiets sikkerhetstjeneste, fastsatt ved kgl.res. 19. august 2005 med hjemmel i lov 4. august 1995 nr. 53 om politiet (politiloven) §29.

[89] Justis- og beredskapsdepartementets hovedinstruks til Politiets sikkerhetstjeneste. Fastsatt av Justis- og beredskapsdepartementet med virkning fra 20. mai 2019.

[90] Forsvarsdepartementet, Justis- og beredskapsdepartementet og NSM: *Evaluering og videreutvikling av Nasjonal sikkerhetsmyndighet. Prosjektrapport (2013).*

[91] NSM S:20/03483-1.

«forsvarlig sikkerhet» i virksomhetene. PST har ansvaret for sikkerhetsklarering av eget personell.

PST har videre ansvar for å forebygge og etterforske brudd på sikkerhetsloven og har dermed en grenseflate mot NSMs ansvar for forebyggende sikkerhet etter sikkerhetsloven.

PST er administrativ leder av NESS og deltar i FCKS, jf. nærmere omtale i avsnitt 6.1.1 om Etterretningstjenesten. Det er også etablert et felles etterretnings- og kontraterrorsenter (FEKTS) for å styrke samarbeidet mellom PST og E-tjenesten. FEKTS er regulert i en egen instruks om samarbeidet mellom E-tjenesten og PST.[92] NSM deltar ikke i FEKTS.

6.2 Politiet

Politiets hovedoppgaver er å opprettholde alminnelig orden, forebygge og forhindre straffbare handlinger, beskytte borgerne og deres lovlydige virksomhet samt etterforske og forfølge straffbare lovbrudd.[93]

Politiet er underlagt Justis- og beredskapsdepartementet og samfunnsoppdraget er definert i politiloven. Politiet er organisert i et direktorat (Politidirektoratet) med tolv underliggende politidistrikter og fem særorgan med nasjonale oppgaver. Etterforskningen av straffesaker ledes av den uavhengige påtalemyndighet under riksadvokatens overordnede ledelse. Ingen kan instruere påtalemyndigheten i enkeltsaker eller omgjøre en påtaleavgjørelse.

Politiets trusselvurderinger bidrar til felles situasjonsforståelse av kriminalitetsutfordringene samfunnet står overfor. Politiets vurderinger kommer i tillegg til de nasjonale trusselvurderingene fra PST og E-tjenesten. I tillegg utgir Kripos en egen trusselvurdering om cyberkriminalitet.[94]

Kripos er politiets nasjonale enhet for bekjempelse av organisert og annen alvorlig kriminalitet. Enheten har oppgaver som både grenser mot NSMs rolle som nasjonalt fagmiljø for digital sikkerhet og mot NSMs rolle som nasjonal responsfunksjon ved alvorlige digitale angrep. I 2019 etablerte Kripos Nasjonalt cyberkrimsenter (NC3) som en egen avdeling. Senteret er et nasjonalt kunnskaps- og kompetansesenter innen teknologirelaterte politioppgaver. Hovedoppgaver er å bekjempe cyberkriminalitet gjennom etterretning, metodeutvikling, forebygging, etterforskning, sikring av digitale spor og patruljering på nett. Senteret skal fremme informasjonsdeling og samvirke mellom private og statlige sikkerhetsaktører nasjonalt og internasjonalt. Målet er å være nasjonalt og internasjonalt ledende i å avdekke og bekjempe trusler og kriminalitet i det digitale rom.[95] NC3s oppdrag har grenseflater

[92] *Instruks om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste*, fastsatt ved kgl.res. 13. oktober 2006 og sist endret 18. juni 2021.

[93] *Hovedinstruks for politiet*. Fastsatt av Justis- og beredskapsdepartementet med virkning fra 21. juli 2022.

[94] *Cyberkriminalitet 2025. Politiets årlige rapport om cyberrettet og cyberstøttet kriminalitet.*

[95] https://www.politiet.no.

mot PSTs ansvar for å etterforske alvorlig kriminalitet som kan true den nasjonale sikkerheten.

NC3 i Kripos og Nasjonalt cybersikkerhetssenter (NCSC) i NSM skal begge bidra til å styrke den nasjonale innsatsen i det digitale domenet. NSM bistår med støtte til å gjenopprette sikker tilstand ved cyberhendelser, samt forhindre ytterligere spredning av skadeomfang, se nærmere omtale i kapittel 4. Kripos har ansvar for å etterforske hendelser.

Det er vanskelig å avgjøre om en cyberhendelse skyldes et uhell, feil i eget system eller en villet handling rett etter at cyberhendelsen har inntruffet. I denne fasen er det behov for utstrakt samarbeid og løpende koordinering mellom NSM, Kripos og PST for å avklare ansvarsforhold. Her er de etablerte koordineringssentrene viktige. Kripos deltar i det løpende operative samarbeidet i både FCKS og i NESS. Dersom det er en villet handling, kan det være vanskelig å vite hvem som står bak: aktivister, en kriminell, kriminelt nettverk, statlige aktører, terrorister eller andre. Politiet og/eller PST har ansvar for videre undersøkelse av cyberangrepet. Om det er politiet eller PST som har ansvaret for videre etterforskning vil være avhengig av hvem man antar står bak handlingen.

6.3 Direktoratet for samfunnssikkerhet og beredskap (DSB)

Direktoratet for samfunnssikkerhet og beredskap (DSB) skal ha oversikt over risiko og sårbarheter i samfunnet og være en pådriver i arbeidet med å forebygge ulykker, kriser og andre uønskede hendelser.[96] DSB skal bidra til god sivil beredskap og effektiv ulykkes- og krisehåndtering. DSB er på vegne av Justis- og beredskapsdepartementet fag-, forvaltnings- og tilsynsorgan på sentrale deler av samfunnssikkerhetsområdet. DSB er nasjonal brannmyndighet, elsikkerhetsmyndighet og fagmyndighet for håndtering av farlige stoffer, eksplosiver og transport av farlig gods. DSB ivaretar også statens eierskap til infrastrukturen i Nødnett, og er tjenesteleverandør for brukerne av nødnett.

Sivilforsvaret, Brann- og redningsskolen og DSBs kurssenter er underlagt DSB. I tillegg styrer direktoratet statsforvalterne på samfunnssikkerhetsområdet på vegne av Justis- og beredskapsdepartementet.

[96] Hovedinstruks til Direktoratet for samfunnssikkerhet og beredskap. Fastsatt av Justis- og beredskapsdepartementet med virkning fra 1. januar 2024.

DSB forvalter følgende lover med tilhørende forskrifter:

– lov om vern mot brann, eksplosjon og ulykker med farlig stoff og om brannvesenets redningsoppgaver (brann- og eksplosjonsvernloven)
– lov om tilsyn med elektriske anlegg og elektrisk utstyr (el-tilsynsloven)
– lov om kontroll med produkter og forbrukertjenester (produktkontrolloven)
– lov om kommunal beredskapsplikt, sivile beskyttelsestiltak og Sivilforsvaret (sivilbeskyttelsesloven)

DSBs brede ansvar har dels sammenheng med at DSB er et resultat av at flere andre direktorater er slått sammen, se boks 6.1.

Boks 6.1 Historie og oppgaver for Direktoratet for samfunnssikkerhet og beredskap (DSB)[97]

Direktoratet for samfunnssikkerhet og beredskap (DSB) ble opprettet i 2003 som et resultat av at Direktoratet for brann- og elsikkerhet (DBE) ble slått sammen med Direktoratet for sivilt beredskap. Før dette er det en lang historie med sammenslåinger av tilsyn og direktorater som har ledet opp til det Direktoratet for samfunnssikkerhet og beredskap vi har i dag:

1898 Elektrisitetstilsynet ble opprettet
1917 Sprengstoffinspeksjonen opprettet
1947 Krigsøkonomikontoret og Sivilforsvarets sentralledelse etablert
1949 Direktoratet for økonomisk forsvarsberedskap (DØF) opprettet
1970 Direktoratet for sivilt beredskap opprettet som et resultat av at man slo sammen blant annet Direktoratet for økonomisk forsvarsberedskap, Krigsøkonomikontoret og Sivilforsvarets sentralledelse.
1972 Statens branninspeksjon opprettet
1984 Sprengstoffinspeksjonen slått sammen med Statens branninspeksjon til Direktoratet for brann- og eksplosjonsvern
1991 El-tilsynet opprettet
1995 Produkt- og elektrisitetstilsynet opprettet
2002 Direktoratet for brann- og eksplosjonsvern slått sammen med Produkt- og elektrisitetstilsynet til Direktoratet for brann- og elsikkerhet (DBE)
2003 DBE ble slått sammen med Direktoratet for sivilt beredskap til Direktoratet for samfunnssikkerhet og beredskap
2017 Direktoratet for nødkommunikasjon (DNK) ble gjort om til en fagavdeling i DSB og avviklet som egen organisasjon

Dette innebærer at DSB har oppgaver innen mange fagområder, som:

- Nasjonal, regional og lokal sikkerhet og beredskap
- Brann- og elsikkerhet
- Industri- og næringslivsikkerhet
- Farlige stoffer og transport av farlig gods
- Nødnett – et nasjonalt, digitalt samband for politi, brann- og helsetjeneste, samt andre aktører med nød- og beredskapsansvar.
- Produkt- og forbrukersikkerhet
- Tilby operativ støtte under kriser innenfor samordning, forsterkning og faglig rådgivning.
- Følge opp norske interesser og forpliktelser i arbeid på samfunnssikkerhetsområdet med internasjonale organisasjoner som EU, FN og NATO
- Etatsledelse av Sivilforsvaret

[97] www.dsb.no.

DSB skal ifølge instruks for departementenes arbeid med samfunnssikkerhet bistå Justis- og beredskapsdepartementet med å koordinere arbeidet med samfunnssikkerhet og beredskap.[98] DSB har dialog med ulike deler av offentlig forvaltning og samfunnskritisk virksomhet.[99] Stadig flere utfordringer er tverrsektorielle. Et særlig viktig verktøy i krisehåndteringen er samordningskonferanser.

DSB skal også bistå i Justis- og beredskapsdepartementets ansvar for samordning innenfor totalforsvaret. DSB leder Sentralt totalforsvarsforum (STF) sammen med Forsvarsstaben. I dette forumet møtes ledere for rundt 30 sivile og militære etater jevnlig for blant annet å etablere en felles forståelse av situasjonen.

I Totalberedskapsmeldingen foreslår regjeringen å gi DSB tydeligere fullmakter i denne samordningsrollen.[100] Fullmaktene skal blant annet sørge for at direktoratet får tilgang til nødvendig informasjon for at etatene på sivil side skal kunne virke sammen ved hendelser i «den øvre delen av krisespekteret». Et revidert mandat skal også bidra til å tydeliggjøre grensesnittet mellom DSBs samordningsrolle og andre aktører i krisehåndteringen.

DSB vurderer utfordringer for samfunnssikkerhet og beredskap på sivil side uavhengig av hva som forårsaker dem. Dette kan føre til overlapp med andre myndigheters ansvar, herunder NSMs arbeid med forebyggende sikkerhet.

DSB skal i henhold til sin hovedinstruks utvikle og vedlikeholde systematisert kunnskap om planlegging, gjennomføring, evaluering og oppfølging av større øvelser og hendelser. DSB skal utvikle et strategisk rammeverk for sivile, nasjonale øvelser. For å følge opp dette vil DSB i 2025 blant annet gjennomføre en nasjonal øvelse for digital sikkerhet som en totalforsvarsøvelse. Øvelsen gjennomføres i nært samarbeid med NSM som har det sikkerhetsfaglige ansvaret. DSB har vært partner i Nasjonalt cybersikkerhetssenter (NCSC) siden oppstarten i 2019. DSB bidrar med analyser innen verstefallsscenarioer for Nasjonalt etterretnings- og sikkerhetssenter (NESS) ved behov.

Begge direktoratene utfører tilsyn med departementene. DSB fører tilsyn med departementenes arbeid med samfunnssikkerhet og beredskap etter samfunnssikkerhetsinstruksen, mens NSM fører tilsyn med departementenes forebyggende sikkerhetsarbeid med hjemmel i sikkerhetsloven. Både DSB og NSM driver omfattende kursvirksomhet, til dels rettet mot de samme målgruppene.

Totalberedskapskommisjonen pekte på at det er ressurskrevende for departementene å forholde seg til to ulike rammeverk som i stor grad overlapper og som det føres tilsyn etter.[101] Kommisjonen anbefalte at rammeverkene for kritiske samfunnsfunksjoner (KIKS, forankret i samfunnssikkerhetsinstruksen) og grunn-

[98] *Instruks for departementenes arbeid med samfunnssikkerhet* (samfunnssikkerhetsinstruksen) fastsatt av Justis- og beredskapsdepartementet 2017 med hjemmel i delegeringsvedtak 10. mars 2017 nr. 312.

[99] *Instruks for Direktoratet for samfunnssikkerhet og beredskaps koordinerende roller*, fastsatt ved kgl.res. 24. juni 2005, jf. St.meld. nr. 17 (2001–2002).

[100] *Meld. St. 9 (2024–2025) Totalberedskapsmeldingen – Forberedt på kriser og krig.*

[101] NOU 2023: 17 *Nå er det alvor – Rustet for en usikker fremtid.*

leggende nasjonale funksjoner (GNF, etter sikkerhetsloven) slås sammen. Se nærmere omtale av disse rammeverkene i boks 6.2 nedenfor.

I Totalberedskapsmeldingen følger regjeringen opp kommisjonens innspill ved å foreslå en ny sektorovergripende lov for grunnsikring av kritiske virksomheter. Arbeidet med loven ses i sammenheng med at EU-direktivene NIS2 og CER tas inn i norsk rett, se kapittel 4 og kapittel 7. Disse direktivene deler samfunnet inn i samfunnsområder som i stor grad overlapper med tilsvarende inndelinger både i rammeverket for kritiske samfunnsfunksjoner og for grunnleggende nasjonale funksjoner, samt NATOs syv grunnleggende forventninger til motstandskraft i kritiske sivile samfunnsfunksjoner. Som en del av arbeidet med den nye loven vil regjeringen ifølge meldingen også gjennomgå samfunnssikkerhetsinstruksen. Grensesnittet mellom den nye loven og sikkerhetsloven og forholdet til relevant sektorregelverk vil bli vurdert.

Boks 6.2 beskriver sentrale sider ved rammeverkene som henholdsvis NSM og DSB har som oppgave å følge opp, de grunnleggende nasjonale funksjonene (GNF-ene) etter sikkerhetsloven og de kritiske samfunnsfunksjonene etter KIKS-rammeverket. Som det fremkommer i boksen, er det betydelig overlapp mellom disse funksjonene. Figur 6.2 under boksen forsøker å illustrere dette grafisk.

I vedlegg 4 er de kritiske samfunnsfunksjonene og de grunnleggende nasjonale funksjonene listet opp. På overskriftsnivå er sammenfallet betydelig. Når overskriftene brytes ned på et lavere nivå, er det imidlertid større forskjeller fordi KIKS og GNF har ulike formål, jf. nærmere omtale i boks 6.2. I vedlegg 5 er også instruksene til NSM og DSB sammenliknet. Tabellen illustrerer at det er overlapp i de to direktoratenes oppgaver.

Boks 6.2 Grunnleggende nasjonale funksjoner (GNF) og kritiske samfunnsfunksjoner (KIKS)

NSM og DSB har ulike utgangspunkt …
NSM skal etter sikkerhetsloven arbeide for å beskytte mot tilsiktede ondsinnede handlinger, mens DSB skal arbeide for å forebygge og redusere konsekvensene av både ondsinnede handlinger og andre utfordringer for samfunnssikkerheten, som uhell, vind og vær, brann mv.

Sikkerhetslovens formål er å ivareta nasjonal sikkerhet. En viktig ramme for sikkerhetslovens virkeområde er de såkalte «grunnleggende nasjonale funksjonene» eller GNF-ene. Disse er i sikkerhetsloven definert som «tjenester, produksjon og andre former for virksomhet som er av en slik betydning at et helt eller delvis bortfall av funksjonen vil få konsekvenser for statens evne til å ivareta nasjonale sikkerhetsinteresser».[102] Departementene har ansvar for å identifisere hva som er GNF-er i egen sektor. Det er ved utgangen av mars 2025 meldt inn 45 GNF-er.

Justis- og beredskapsdepartementet skal etter samfunnssikkerhetsinstruksen utvikle og holde oversikt over hvilke funksjoner som i et tverrsektorielt perspektiv er kritiske for samfunnssikkerheten. DSB har på oppdrag fra departementet ledet arbeidet med å identifisere disse funksjonene (KIKS).

«Kritiske samfunnsfunksjoner» etter det såkalte KIKS-rammeverket er funksjoner som er nødvendige for å ivareta befolkningens og samfunnets grunnleggende behov og samfunnets funksjonalitet.[103] Med grunnleggende behov menes trygghet for den enkelte og elementære fysiske behov som vann, mat, varme, helse og omsorg, redningstjeneste mv., samt ulike infrastrukturbaserte tjenester. Begrepet kritiske samfunnsfunksjoner forbeholdes funksjoner som samfunnet ikke kan klare seg uten i syv døgn eller kortere uten at dette truer befolkningens sikkerhet og/eller trygghet. Det er identifisert 14 ulike kritiske samfunnsfunksjoner.

… men GNF-er og kritiske samfunnsfunksjoner overlapper
Gjennom å identifisere GNF-er kartlegges funksjoner i samfunnet som understøtter en eller flere av de nasjonale sikkerhetsinteressene som sikkerhetsloven definerer. Den detaljerte utformingen av en GNF bidrar igjen til å kartlegge hvilke objekter og infrastrukturer som skal utpekes som skjermingsverdige og beskyttes med sikringstiltak. Dette er skjermingsverdige verdier som har avgjørende betydning for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser. Virksomhetene som eier disse objektene eller

[102] Sikkerhetsloven § 1-5 nr. 2.

[103] Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enhver tid? (DSB 2016). KIKS er en forkortelse for *Kritisk Infrastruktur og Kritiske Samfunnsfunksjoner*.

Boks 6.2 forts.

infrastrukturene, skal underlegges sikkerhetsloven, også om de er private. Virksomhetene må etter loven sørge for en forsvarlig sikkerhet for dem.

Kritiske samfunnsfunksjoner etter KIKS-rammeverket omfatter hele verdikjeder som er nødvendige for å opprettholde funksjonene. Det er imidlertid ikke, som for GNF-ene, et tverrsektorielt regelverk som stiller krav til virksomheter som understøtter KIKS. Sikkerheten for kritiske samfunnsfunksjoner reguleres hovedsakelig i sektorregelverk.

En GNF vil med få unntak også være en del av en kritisk samfunnsfunksjon. Rammes den nasjonale sikkerheten, vil som regel situasjonen bli kritisk for samfunnet og befolkningen. Dette vil likevel ikke alltid gjelde i motsatt retning. Det er lett å tenke seg at det kan være viktige samfunnsfunksjoner rundt om i landet som er kritiske etter KIKS-rammeverket, men som likevel ikke er en GNF. Det kan være lokale og regionale veier eller flyplasser som er svært viktige for lokalbefolkningens trygghet, men som likevel ikke er avgjørende for den nasjonale sikkerheten.

NSM følger opp sikkerhetsloven og arbeidet med GNF-er
NSM har siden GNF-mekanismen ble en del av sikkerhetsloven, informert og gitt råd til departementene i deres arbeid med å identifisere og utforme GNF-er og peke ut virksomheter, objekter og infrastrukturer.

NSM fører tilsyn med departementene for å avklare om departementene har oppfylt sine plikter til å identifisere GNF-er, underlegge virksomheter sikkerhetsloven, om skjermingsverdige verdier er utpekt og om departementene i styringsdialogen med underliggende etater og virksomheter i sektoren følger opp kravene i sikkerhetsloven.

Overfor virksomheter kan NSM vurdere om virksomheten har et styringssystem for sikkerhet, om det foreligger risikovurderinger, og om konkrete skjermingsverdige verdier er tilstrekkelig sikret. Der det er utpekt sektortilsyn, fører i utgangspunktet ikke NSM tilsyn med virksomhetene, men ser til at sektortilsynene fører et tilsyn i tråd med sikkerhetsloven.

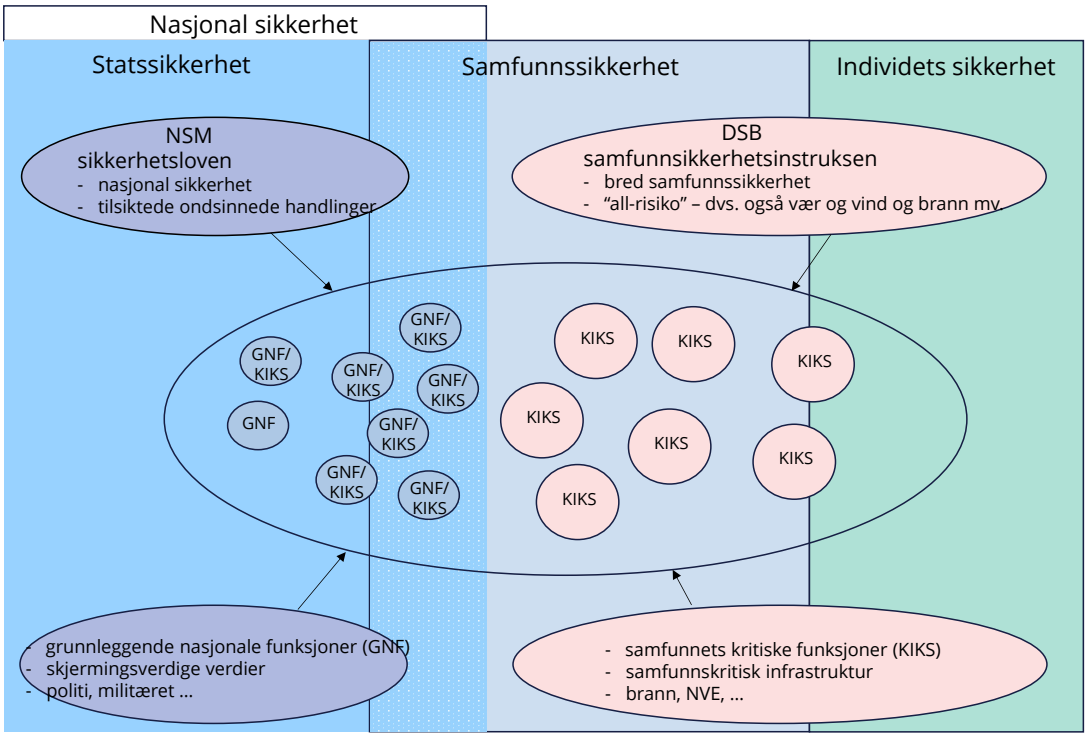
og DSB følger opp de kritiske samfunnsfunksjonene
Samfunnssikkerhetsinstruksen stiller generelle krav til departementenes arbeid med samfunnssikkerhet og særskilte krav til departementer med hovedansvar for kritiske samfunnsfunksjoner. Regjeringen har pekt ut hovedansvarlig departement for hver av de 14 kritiske samfunnsfunksjonene. Departementer med hovedansvar for kritiske samfunnsfunksjoner skal blant annet utarbeide og vedlikeholde risiko- og sårbarhetsanalyser for den kritiske samfunnsfunksjonen, planlegge og gjennomføre felles øvelser, evaluere og følge opp læringspunkter, forelegge forslag til beredskapstiltak for berørte departementer og sørge for erfaringsutveksling og kompetanseheving for

Boks 6.2 forts.

berørte departementer og sørge for erfaringsutveksling og kompetanseheving for berørte aktører. Departementene skal rapportere til Stortinget om status- og tilstandsvurderinger etter en tidsplan som fastsettes av Justis- og beredskapsdepartementet.

DSB fører på vegne av Justis- og beredskapsdepartementet tilsyn med departementenes etterlevelse av samfunnssikkerhetsinstruksen.

Figur 6.2 Sammenheng mellom GNF-er og kritiske samfunnsfunksjoner etter KIKS



Figuren er en prinsippskisse og forenkling. Skillet mellom stats- og samfunnssikkerhet kan være krevende å fastsette.

6.4 Forsvaret og øvrige etater i forsvarssektoren

Forsvarssektoren består av flere etater som har ulike roller og ansvar. De fleste ressursene i sektoren bidrar til å nå mål i etaten Forsvaret. Forsvaret er i tillegg avhengig av sikkerheten i verdikjeder som strekker seg ut i forsvarssektoren, til underliggende leverandører og sivile deler av totalforsvaret samt til andre land og NATO. Forsvarssektoren er en sektor med betydelig sikkerhetsbehov.

6.4.1 Forsvarets sikkerhetsavdeling (FSA)

Forsvarssjefen (FSJ) har som virksomhetens leder ansvaret for sikkerhetsarbeidet i egen etat. Forsvarets sikkerhetsavdeling (FSA) er det sentrale stabsorganet i Forsvaret for sikkerhet mot villede, ondsinnede handlinger, og FSA er forsvarssjefens rådgiver og utøver på dette feltet.

FSA og NSM ble begge opprettet i 2003 som et resultat av nedleggingen av Forsvarets overkommando/Sikkerhetsstaben (FO/S). Mens NSM overtok de sektoroverg ripende oppgavene som hadde ligget til FO/S, blant annet oppgaver som fulgte av sikkerhetsloven, overtok FSA de rene etatsinterne sikkerhetsoppgavene i Forsvaret. Forsvaret forvalter mye sikkerhetsgradert informasjon og andre verdier som er skjermingsverdige av hensyn til nasjonal sikkerhet og har derfor et stort sikkerhetsbehov.

FSA er organisatorisk plassert i Forsvarets fellestjenester (FFT) som er en felles stab og administrasjon for flere av Forsvarets avdelinger. Sjefen for FSA har direkte adgang til forsvarssjefen i sikkerhetssaker.

FSA kontrollerer på forsvarssjefens vegne sikkerhetsarbeidet i etaten. Dette fratar ikke den enkelte militære sjef ansvar for sikkerheten på eget ansvarsområde. FSA er NSMs faglige kontaktpunkt og diskusjonspartner i Forsvaret. På avgrensede områder vil andre i Forsvaret kunne være slikt kontaktpunkt for NSM i stedet for FSA. Et eksempel på dette er innen digital sikkerhet hvor Cyberforsvaret og Forsvarsstaben er viktige samarbeidspartnere for NSM.

FSA klarerer personell i første instans for forsvarssektoren og er dermed den største klareringsmyndigheten i landet. FSA bygger sine avgjørelser på informasjon innhentet gjennom sentral personkontroll utført av NSM og melder resultatet til det sentrale klareringsregisteret i NSM. FSA er også fagmyndighet for vakt- og sikringstjenesten i Forsvaret.

FSA forbereder alle saker om godkjenning av informasjonssystemer i Forsvaret som skal sendes til NSM som godkjenningsmyndighet. FSA rapporterer til NSM om alle sikkerhetstruende hendelser i Forsvaret. NSM koordinerer sine planer for tilsyn i Forsvaret med FSA og presenterer resultater av relevante kontrollmeldinger for FSA før endelig godkjenning.

FSA har i tillegg oppgaver innen militær kontraetterretning, også omtalt som operativ sikkerhet, som skal avdekke og hindre ulovlig etterretningsvirksomhet i og mot Forsvarets verdier, herunder objekter, personell og aktiviteter. FSA samarbeider med Politiets sikkerhetstjeneste (PST) som har et nasjonalt ansvar for

kontraetterretning. FSAs oppgaver innenfor militær kontraetterretning er blant annet å undersøke, sammenstille og analysere informasjon om sikkerhetstruende virksomhet rettet mot Forsvaret og allierte som befinner seg på norsk territorium. Når det vurderes som nødvendig, deles informasjon også med E-tjenesten, NSM og utenlandske samarbeidspartnere. FSA har det utøvende ansvaret for militær kontraetterretning under militære operasjoner i utlandet.

EOS-utvalget fører løpende kontroll med FSA. Det er særlig saker om sikkerhetsklarering og militær kontraetterretning som har vært gjenstand for utvalgets kontroll.

6.4.2 Øvrige etater i forsvarssektoren

Etatene i forsvarssektoren foruten Forsvaret er: Forsvarsmateriell (FMA), Forsvarsbygg (FB), Forsvarets forskningsinstitutt (FFI), Statens graderte Plattformtjenester (SGP) og Forsvarshistorisk museum.[104] NSM er i henhold til Direktoratets instruks av 3. mai 2019 «... en virksomhet tilknyttet forsvarssektoren».

FMA har ansvar for å fremskaffe, forvalte og avhende materiell for Forsvaret. FMA skal også ivareta industrisamarbeid og internasjonalt materiellsamarbeid. FB etablerer, opprettholder og gjenoppretter forsvarssektorens eiendom, bygg og anlegg i fred, krise og krig. Gjennom Nasjonalt kompetansesenter for sikring av bygg (NKSB) leverer FB sikkerhetsfaglig rådgivning til byggeprosjekter i forsvarssektoren og staten for øvrig. FFI er forsvarssektorens egen forskningsinstitusjon. SGP som ble etablert 1. januar 2025, skal levere graderte kommunikasjonsløsninger til offentlige og private virksomheter som er underlagt sikkerhetsloven.

6.5 Sivil klareringsmyndighet (SKM)

Sivil klareringsmyndighet (SKM) er den sentrale klareringsmyndigheten i sivil sektor. Kjerneoppgaven for SKM er å klarere personell for tilgang til sikkerhetsgradert informasjon, skjermingsverdige objekter og skjermingsverdig infrastruktur i den sivile delen av samfunnet. SKM skal verne nasjonale verdier ved å redusere risiko for innsidere, det vil si personer som har eller har hatt legitim tilgang til en virksomhets interne, fortrolige opplysninger og som bevisst eller ubevisst kan tilrettelegge for trusselaktører eller på annen måte skade virksomheten ved å misbruke denne informasjonen.[105]

SKM er underlagt Justis- og beredskapsdepartementet og utøver sitt ansvar i henhold til sikkerhetsloven med forskrifter. I henhold til klareringsforskriften § 1 andre ledd kan klareringsmyndighetene inngå avtale om å klarere for hverandre. Det er inngått avtale om at SKM skal klarere NSMs personell.

NSM er fagmyndighet og tilsynsmyndighet for personellsikkerhet innenfor sikkerhetslovens virkeområde. NSM gjennomfører den sentrale personkontrollen for

[104] Forsvarshistorisk museum som forvalter gjenstandene og dokumentasjonen fra Norges militære historie ble etablert som etat 1. januar 2025.

[105] Prop. 1 S (2024–2025) for budsjettåret 2025 under Justis- og beredskapsdepartementet.

klareringsmyndighetene og fører nasjonalt register over alle personklareringer som gis, se kapittel 4.

SKM skal være pådriver for å utvikle arbeidet med personellsikkerhet og samarbeider med NSM og øvrige klareringsmyndigheter om faglige spørsmål på dette området. SKM skal videre legge til rette for hensiktsmessig samhandling og informasjonsutveksling mellom aktører i saker om personellsikkerhet. SKM skal gjennom faglige analyser og vurderinger bidra til at departementet har et best mulig beslutningsgrunnlag for politikkutvikling innenfor direktoratets ansvarsområde. Denne oppgaven innebærer blant annet å utarbeide nasjonal statistikk for sivil og militær sektor.[106] SKM har overtatt oppgaver knyttet til råd, veiledning og kurs fra 2025.

Det pågår et arbeid for å vurdere å overføre ytterligere oppgaver innen personellsikkerhet i sivil sektor til SKM. Det følger av utvalgets mandat at dette arbeidet vil pågå uavhengig av utvalgets arbeid.

6.6 Digitaliseringsdirektoratet

Digitaliseringsdirektoratet (Digdir) er et direktorat og tilsyn under Digitaliserings- og forvaltningsdepartementet.

Digdirs samfunnsoppdrag er å bidra til en effektiv, brukerrettet og samordnet digitalisering av offentlig sektor. Digitalisering skal bidra til at offentlig sektors tjenester er helhetlige, sammenhengende og av god kvalitet. Offentlig sektor er Digdirs primære målgruppe.

Digdir har fagansvar for offentlig sektors arbeid med informasjonssikkerhet. Direktoratet skal veilede offentlige virksomheter på området og bidra til at offentlige virksomheter har gode rammevilkår for arbeidet med informasjonssikkerhet. Dette innebærer blant annet å arbeide for samordnet og brukerrettet veiledning og hjelp på området.

Digdir har ansvar for nasjonal arkitektur for digital samhandling, felles økosystem for samhandling og tjenesteutvikling på tvers av sektorer, nasjonalt ansvar for informasjonsforvaltning og deling og bruk av data. Digdir har også ansvar for digitale tjenester og fellesløsninger, som ID-porten og Altinn. Videre er Digdir tilsynsmyndighet gjennom ansvaret for Tilsynet for universell utforming av ikt (Uu-tilsynet).

Digdir skal samarbeide med andre virksomheter der det er hensiktsmessig, og særlig der det er tilgrensende eller overlappende ansvarsområder. Det skal støtte opp under at kompetansetiltak, informasjon og veiledning fra det offentlige er samordnet og helhetlig.

[106] Hovedinstruks til Sivil klareringsmyndighet (SKM) fastsatt av Justis- og beredskapsdepartementet med virkning fra 1. januar 2025.

Felles sikkerhet i forvaltningen (FSIF) er et samarbeid som skal bidra til «et nasjonalt løft» for informasjonssikkerhet og personopplysningsvern i offentlige virksomheter, og gjøre dem bedre i stand til å løse oppgavene sine og levere tjenester. Både Digdir og NSM deltar i dette samarbeidet. Samarbeidet er nærmere beskrevet på direktoratets nettside.

Digdir veileder offentlige virksomheters arbeid med informasjonssikkerhet. Digdir legger vekt på styringsaktiviteter som benyttes på tvers av ulike regelverk, som digital sikkerhet, personopplysningsvern og plikter etter sikkerhetsloven. Digdir følger også opp aktiviteter i EU og på nordisk nivå og bidrar med å koordinere og følge opp internasjonale initiativ som Norge deltar i. Digdir bidrar dessuten i arbeidet med å utvikle regelverk innen digitalisering nasjonalt og i EU. Disse oppgavene har grenseflater mot NSMs oppgaver etter hovedinstruksen som «det nasjonale fagmiljøet» for digital sikkerhet. Også NSM gir dermed veiledning til offentlig og privat sektor innen sine fagområder. NSM og Digdir har videre beslektede oppgaver ved at NSM etter instruksen skal koordinere myndigheter som har en rolle i arbeidet med forebyggende digital sikkerhet, blant annet forskning og utvikling, kompetanseutvikling og samarbeid internasjonalt. NSM administrerer dessuten Nasjonalt koordineringssenter for forskning og innovasjon innen cybersikkerhet (NCC-NO) sammen med Forskningsrådet. Digdir er representert i NCC-NOs Advisory Board.

6.7 Myndigheter med tilsynsansvar etter sikkerhetsloven (såkalte sektortilsyn)

Det følger av sikkerhetsloven § 2-2 at «sikkerhetsmyndigheten» har det overordnede ansvaret for at sikkerhetstilstanden i alle sektorer kontrolleres, og skal se til at virksomhetene oppfyller sine plikter etter loven. Sikkerhetsmyndigheten skal videre etter lovens § 3-1 første ledd føre tilsyn med virksomheter som er omfattet av loven. I forarbeidene til loven stadfestes det at det med «sikkerhetsmyndigheten» menes NSM.

Etter sikkerhetsloven kan ansvarlig departement beslutte at myndigheter med sektoransvar som fører tilsyn med beskyttelse av informasjon, informasjonssystemer, objekter og infrastruktur, skal føre tilsyn med virksomheter i egen sektor som er omfattet av loven. Dette omfatter private virksomheter som er omfattet av sikkerhetsloven etter vedtak iht. lovens § 1-3 og statlige og kommunale virksomheter. Dersom sektortilsynet ikke fører tilsyn i samsvar med krav fastsatt i eller i medhold av sikkerhetsloven, kan sikkerhetsmyndigheten gi pålegg om å utføre slikt tilsyn. Sikkerhetsmyndigheten skal gjennomføre tilsyn på sektortilsynets ansvarsområde når dette følger av internasjonale forpliktelser eller når det er tvingende nødvendig.

Det følger videre av sikkerhetsloven at det skal foreligge en avtale om samarbeid mellom sikkerhetsmyndigheten og det utpekte sektortilsynet. Krav til innholdet i avtalen er nærmere regulert i forskrift om virksomheters arbeid med forebyggende sikkerhet § 90, der det står:

– kriterier for tilsyn, jf. Veileder for tilsyn med forebyggende sikkerhetsarbeid
– ansvarsfordeling for opplæring og veiledning, samt gjennomføring av dette
– hvordan felles tilsyn skal forberedes og gjennomføres
– hvordan NSM skal dele relevant informasjon om trusselbildet og risiko med sektormyndigheten
– hvordan sektormyndigheten skal rapportere til NSM om planlagte tilsyn
– hvordan varslinger etter sikkerhetsloven § 4-5 skal behandles
– hvordan godkjennings- og dispensasjonsmyndighet i sektoren skal utøves
– hvordan sektormyndigheten skal dele kunnskap og erfaringer med NSM.

Sektortilsynene skal på forespørsel fra virksomhetene også kunne gi råd om risikovurderinger, jf. sikkerhetslovens § 4-2 fjerde ledd.

I dag er det fem sektortilsyn som er utpekt: Nasjonal kommunikasjonsmyndighet, Norges vassdrags- og energidirektoratet, Havindustritilsynet, Luftfartstilsynet og Jernbanetilsynet. Der det er sektortilsyn, fører ikke NSM tilsyn med virksomheter underlagt sikkerhetsloven, men med at sektortilsynene fører et tilfredsstillende tilsyn med virksomhetene.

Det å bli utpekt som sektortilsyn etter sikkerhetsloven har ifølge de tilsynene utvalget har snakket med, ikke ført til en vesentlig endring i deres arbeid. Det skyldes blant annet at også de respektive sektorregelverkene har bestemmelser om sikkerhet som det allerede er blitt ført tilsyn med over tid. Enkelte av virksomhetene skal også etter sektorregelverket sørge for «forsvarlig sikkerhet», slik de også skal det etter sikkerhetsloven.

Felles for sektortilsynene som er utpekt som tilsynsmyndighet etter sikkerhetsloven, er at de er ansvarlige for å følge opp at private virksomheter som er underlagt sikkerhetsloven, følger opp de kravene som loven stiller. Aktuelle virkemidler er å føre tilsyn, gi råd, informasjon og veiledning. Enkelte av sektortilsynene har også kompetanse til å godkjenne skjermingsverdige informasjonssystemer som er utpekt som, eller har avgjørende betydning for funksjonen til et objekt eller en infrastruktur klassifisert KRITISK eller MEGET KRITISK. Flere av sektortilsynene ivaretar i tillegg funksjonen som sektorvist responsmiljø (SRM) for IKT-sikkerhetshendelser innen egen sektor.

Nkom er omtalt særskilt da denne etaten har oppgaver innenfor digital sikkerhet og kan være en aktuell kandidat til å overta enkelte oppgaver innenfor digital sikkerhet fra NSM, se omtale i kapittel 10.

6.8 Nasjonal kommunikasjonsmyndighet (Nkom)

Nasjonal kommunikasjonsmyndighet (Nkom) er en etat under Digitaliserings- og forvaltningsdepartementet.

Nkom er tilsyns- og kontrollorgan for post, elektronisk kommunikasjon og elektroniske tillitstjenester i Norge. Nkom er også tilsynsmyndighet for datasentre, jf. ny ekomlov som trådte i kraft 1. januar 2025. Nkom forvalter sitt sektoransvar etter lov om elektronisk kommunikasjon, lov om posttjenester og lov om elektroniske tillitstjenester.

Nkom skal bidra til at brukerne i hele landet har gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester med forsvarlig sikkerhet. Nkom skal også legge til rette for at brukerne i hele landet får et landsdekkende tilbud av postsendinger til overkommelig pris og god kvalitet. Etaten har et særskilt ansvar for sikkerhet og beredskap i ekomnett og -tjenester.

Nkom er fagmyndighet i ekomsektoren og fører blant annet tilsyn med at integritet, konfidensialitet og tilgjengelighet i ekomnettene ivaretas.

Digitaliserings- og forvaltningsdepartementet utpekte i 2019 Nkom som sektortilsyn etter sikkerhetsloven. Dette innebærer at Nkom fører tilsyn med at virksomheter underlagt sikkerhetsloven beskytter skjermingsverdige informasjonssystemer, infrastruktur og objekter på en tilfredsstillende måte.

I tillegg er Nkom gitt kompetanse til å godkjenne skjermingsverdige informasjonssystemer som er utpekt som, eller har avgjørende betydning for, funksjonen til et objekt eller en infrastruktur klassifisert KRITISK eller MEGET KRITISK.

7 Internasjonale forpliktelser

Norge har forpliktelser overfor andre land og organisasjoner i arbeidet med forebyggende sikkerhet. I utvalgets mandat understrekes det at *«forpliktelsene en nasjonal sikkerhetsmyndighet har overfor andre land og internasjonale organisasjoner, spesielt Norges forpliktelser til NATO må ivaretas i alle forslag til løsninger».* Utvalget skal også vurdere *«hva som inngår i kontaktpunktfunksjonen til NATO og hvem som er nærmest til å ivareta denne».*

I dette kapittelet redegjøres det for de oppgavene NSM har mot andre land og organisasjoner som fagmyndighet etter sikkerhetsloven. Redegjørelsen er hovedsakelig avgrenset til internasjonalt samarbeid om beskyttelse av sikkerhetsgradert informasjon som Norge har forpliktet seg til.

Det utveksles sikkerhetsgradert informasjon mellom stater og mellom stater og internasjonale organisasjoner. Internasjonale organisasjoner kan også ha et behov for selv å produsere sikkerhetsgradert informasjon. I disse tilfeller vil organisasjonen ha et eget regelverk for hvordan informasjonen skal beskyttes. NATO, den Europeiske romorganisasjon (ESA) og Eurocontrol er internasjonale organisasjoner Norge er medlem av og som alle har slike regelverk.

Den europeiske union (EU) og *Organisasjonen for Felles Forsvarssamarbeid* er organisasjoner med egne sikkerhetsgraderinger og krav til beskyttelse av sikkerhetsgradert informasjon som Norge *ikke* er medlem av, men som vi har sikkerhetsavtaler med.

Til slutt i kapittelet omtales forpliktelser Norge har gjennom EØS-avtalen som følge av visse rettsakter i EU på sikkerhetsområdet og også bilateral utveksling av sikkerhetsgradert informasjon med andre stater.

7.1 Relevante internasjonale organisasjoner som Norge er medlem av

7.1.1 NATO

NATO produserer og utveksler mye sikkerhetsgradert informasjon, både internt og med medlemslandene. NATO har derfor komplekse systemer og et omfattende regelverk for å beskytte sikkerhetsgradert informasjon.

Regelverk:
NATOs regelverk for beskyttelse av sikkerhetsgradert informasjon er omfattende og teller totalt i underkant av 100 ulike dokumenter. De inneholder krav og veiledning. Regelverket omtales som *NATO Security Policy*.

NATO tilvirker egen sikkerhetsgradert informasjon med graderingsnivåene NATO RESTRICTED, NATO CONFIDENTIAL, NATO SECRET og COSMIC TOP SECRET. Plikten til å beskytte denne informasjonen følger av *Avtale mellom partene i Traktat for det nordatlantiske område om beskyttelse av opplysninger* av 06.03.1997. Avtalen pålegger medlemslandene en plikt til å beskytte sikkerhetsgradert informasjon produsert av NATO eller medlemsland til støtte for et NATO prosjekt, program eller kontrakt. Kravene i avtalen er konkretisert i understøttende dokumenter og i en rekke direktiver og veiledningsdokumenter.[107]

Sikkerhetsroller/-funksjoner som medlemslandene må ivareta:
NATOs sikkerhetsbestemmelser forutsetter at medlemslandene etablerer strukturer for å ivareta en rekke sikkerhetsmessige funksjoner.

Den mest sentrale av disse er *National Security Authority (NSA).* Denne funksjonen skal påse at avtalens krav til forebyggende sikkerhetstiltak gjennomføres i medlemslandene. NSA-funksjonen er ansvarlig for:

- at sikkerheten til NATO-sikkerhetsgradert informasjon blir ivaretatt i sivile og militære nasjonale organisasjoner, både i eget hjemland og i utlandet
- at det gjennomføres tilsyn med at NATO-sikkerhetsgradert informasjon beskyttes etter NATOs sikkerhetskrav
- å påse at det utstedes sikkerhetsklarering til alle som kan få tilgang til informasjon sikkerhetsgradert NATO CONFIDENTIAL eller høyere
- å påse at det foreligger beredskapsplaner for å hindre kompromittering av NATO sikkerhetsgradert informasjon i en krise
- å godkjenne opprettelse og nedleggelse av NATO COSMIC TOP SECRET sentralarkiv.

NSA-funksjonen er videre tillagt oppgaver blant annet med å utstede eller bekrefte ulike sikkerhetsmessige godkjenninger. NSA-funksjonen er også tillagt ansvaret for å rapportere brudd på sikkerheten for NATO-sikkerhetsgradert informasjon til NATO Office of Security.

NSA-funksjonen skal videre være medlemslandenes hovedkontaktpunkt for NATO Office of Security (NOS) i spørsmål om sikkerhet. NSA-funksjonen kan også henvise NOS videre til annen kompetent myndighet. NSM er NSA i Norge.

Andre funksjoner som skal etableres etter NATOs sikkerhetsregelverk er:

National CIS Security Authority (NCSA) som skal ivareta sikkerheten for kryptografiske produkter som benyttes for å beskytte NATO-sikkerhetsgradert informasjon. NCSA skal også ivareta sikkerheten for andre produkter som beskytter NATO-sikkerhets-gradert informasjon og som behandles i informasjonssystemer. NSM ivaretar denne funksjonen i Norge.

NCSA er ansvarlig for å utpeke en *National TEMPEST Authority* (NTA) som skal ha ansvar for å ivareta strålingssikkerhet. NSM ivaretar selv denne funksjonen i Norge.

[107] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/natos-sikkerhetsregelverk/.

Hvis denne funksjonen ikke er integrert i NSA-funksjonen, forutsetter regelverket et samarbeid med NSA-funksjonen.

Medlemslandene skal også etablere en *National Distributing Authority* (NDA). NDA er ansvarlig for regnskapsføring og forsvarlig forvaltning av kryptomateriell i landet. Der hvor den ikke er integrert i NSA funksjonen forutsetter regelverket et samarbeid med denne. I Norge ivaretar NSM denne funksjonen.

Hvert medlemsland skal videre etablere en *Security Accreditation Authority* (SAA) med ansvar for å godkjenne nasjonale informasjonssystemer som håndterer NATO-sikkerhetsgradert informasjon og sikkerhetsgraderte NATO-systemer i medlemslandene. Regelverket åpner for at et medlemsland kan etablere flere SAA. NSM ivaretar i dag funksjonen som SAA i Norge.

For NATO-sikkerhetsgraderte informasjonssystemer som er i bruk i flere land, har NATO etablert såkalte *Security Accreditation Boards* (SAB). SAB har det overordnede godkjenningsansvaret for systemet. SAB består ar representanter fra de medlemslandene som har installert systemet og relevante NATO organer. NSM representerer Norge i ulike SABer og gir i denne sammenhengen såkalte samsvarserklæringer (*Statement of Compliance*) for de delene av systemet som er på norsk territorium.

Medlemslandene kan opprette en *Designated Security Authority* (DSA). DSA har ansvar for å følge opp sikkerheten i industrien ved sikkerhetsgraderte anskaffelser. Denne funksjonen kan ivaretas av NSA-funksjonen, slik det er tilfelle i Norge.

NSA-funksjonen kan identifisere såkalte *Competent Security Authority* (CSA). Disse er gitt myndighet til å ivareta spesifikke avgrensede sikkerhetsfunksjoner, for eksempel behandle søknader om sikkerhetsklareringer. I Norge er klareringsmyndighetene å anse som CSA. Sivil klareringsmyndighet (SKM) og Forsvarets sikkerhetsavdeling (FSA) er i denne sammenheng å anse som CSA'er i Norge.

Medlemslandene skal også ha et *Central Registry* som skal være mottaks- og forsendelsespunkt for informasjon sikkerhetsgradert COSMIC TOP SECRET. I Norge er denne oppgaven lagt til Forsvarsdepartementet.

NATO-komitéer med ansvar på sikkerhetsområdet:

NATOs råd har opprettet en sikkerhetskomite, *Security Committee* (SC). Denne komiteen svarer direkte til NATOs råd (*North Atlantic Council* (NAC)) og er ansvarlig for:

- Løpende revidering av NATO Security Policy og regelverk og selv beslutte. endringer i understøttende direktiver og veiledningsdokumenter.
- Vurdere spørsmål om NATO Security Policy.
- Vurdere sikkerhetsmessige saker som er blitt henvist til komiteen fra NATOs råd Militærkomiteen, et medlemsland, Generalsekretæren eller et annet sivilt eller militært NATO organ.

Sikkerhetskomitéen skal bestå av representanter fra medlemslandenes NSAer, og etter behov støttet av andre nasjonale representanter med et sikkerhetsansvar. NATO *Office of Security* leder og ivaretar sekretariatsfunksjonen for gruppen. NATOs

to strategiske kommandoer og andre relevante NATO organer, deltar også i komitéens arbeid. Sikkerhetskomitéen møtes regulært to ganger i året på både sjefsnivå og i fagspesifikke arbeidsgrupper. Møtene omhandler henholdsvis regelverksutvikling og andre spørsmål innenfor informasjonssystemsikkerhet og regelverksutvikling og andre spørsmål innenfor de øvrige sikkerhetsområdene.

Komitéen kan møtes hyppigere ved behov, og den kan også nedsette «*Task Forces*» for utredning og forberedelse av saker for komitéens formelle møter.

NSM er NSA i Norge og representerer også Norge i sikkerhetskomitéen.

SC har grenseflater mot *Digital Policy Committee* (DPC) som har ansvaret for å utvikle tekniske politikk- og kravdokumenter for sikring av informasjons- og kommunikasjonssystemer, herunder krypto. Forsvaret ved Cyberforsvaret (Cyfor) representerer Norge i denne komiteen. Under denne komiteen er det etablert en rekke såkalte «*Capability Panels*», og spørsmål om sikring av informasjons- og kommunikasjonssystemer håndteres i ett av disse; *Information Assurance and Cyber Defence Capability Panel* (CAP4)**.** CAP4 har flere undergrupper, såkalte «*Capability Teams*». NSM deltar i CAP4 og i flere av panelets undergrupper. Også Cyfor deltar i enkelte av undergruppene.

Boks 7.1 **NSA-funksjonen er organisert på ulike måter i ulike NATO-land**

Begrepet «kontaktpunktfunksjonen til NATO» i utvalgets mandat er ikke nødvendigvis et entydig begrep. Innenfor NSMs ansvarsområde er for eksempel den nasjonale responsfunksjonen i NSM (NCSC) **en kontaktpunktfunksjon** mot NATOs responsmiljø (NCIRC). Dette basert på en Cyber Defence MoU inngått mellom Norge og NATO. Det kan også være andre kontaktfunksjoner.

Det legges til grunn at det med «kontaktpunktfunksjon» i mandatet vises til funksjonen som **hovedkontaktpunkt mot NATO og NATO Office of Security** for beskyttelse av sikkerhetsgradert informasjon og NSMs rolle som National Security Authority (NSA).

Denne funksjonen er organisert på ulike måter i NATO-landene:

I **Norge** var NSA-funksjonen fra 1953-1965 lagt til et eget kollegialt organ, Det interdepartementale kontrollutvalg (DIKU), ledet av SMK og med deltakelse fra sjefen for Forsvarets E- og S-tjeneste, Overvåkingssjefen, representanter for FD, JD og UD. Fra 1965 til 2003 var NSA-funksjonen lagt til Forsvarssjefen med støtte av FST/S (FO/S), og fra 2003 har oppgaven vært ivaretatt av NSM. Forkortelsene er forklart i vedlegg 2.

Danmark: *Politiets Efterretningstjeneste (PET) (sivil sektor), Forsvarets Efterretningstjeneste (FE) (militær sektor)*

Sverige*: Utenriksdepartementet*

Finland*: Utenriksdepartementet*

Storbritannia: *Cabinet Office (tilsvarende SMK)*

Frankrike*: Secretariat General de la Defense et de la Securite Nationale (SGDSN) under Statsministerens kontor*

Tyskland*: Innenriksdepartementet*

Nederland*: Innenriksdepartementet (sivil sektor) med støtte av AIVD, Forsvarsdepartementet (militær sektor) med støtte av MIVD*

7.1.2 Den Europeiske romorganisasjon (ESA)

I likhet med NATO produserer også ESA sikkerhetsgradert informasjon (ESA RESTRICTED, ESA CONFIDENTIAL, ESA SECRET og ESA TOP SECRET). Medlemslandene har forpliktet seg til å beskytte denne informasjonen gjennom *Avtale mellom de statene som er part i Konvensjonen om opprettelse av en europeisk romorganisasjon og Den europeiske romorganisasjonen om beskyttelse og utveksling av graderte opplysninger fra* 2002.

Som i NATO er avtalens bestemmelser utdypet og konkretisert i understøttende dokumenter *(ESA Security Regulations*) som er vedtatt av ESAs råd.

Hvert medlemsland skal utpeke en *National Security Authority* (NSA) som er ansvarlig for at ESA-sikkerhetsgradert informasjon beskyttes, at personell som får tilgang til informasjon som er sikkerhetsgradert ESA CONFIDENTIAL eller høyere er sikkerhetsklarert, samt fører tilsyn med beskyttelsen av ESA sikkerhetsgradert informasjon på sitt territorium. I Norge er NSM også NSA i forholdet til ESA.

ESAs råd har nedsatt *ESA Security Committee* (SEC) som skal veilede rådet og Generaldirektøren i alle spørsmål om beskyttelse av sikkerhetsgradert informasjon. Komiteen skal også løpende vedlikeholde *ESA Security Regulations*, utvikle og godkjenne såkalte programsikkerhetsinstrukser (PSI) for ESAs programmer og godkjenne kryptoprodukter som er i bruk i ESA for beskyttelse av sikkerhetsgradert informasjon. De fleste medlemslandene er representert av sine NSA i SEC. Fra Norge møter NSM og Norsk romsenter.

Under sikkerhetskomiteen er det etablert to undergrupper:

Industrial Security Panel som primært har ansvar for å vurdere og utrede spørsmål om sikkerhetsgraderte anskaffelser i ESA, herunder foreslå regelverksutvikling på området og å vedlikeholde ESAs maldokumenter for PSIer.

INFOSEC Panel som har et særskilt ansvar for spørsmål knyttet til informasjonssystemsikkerhet og krypto. Panelet skal rådgi på disse områdene og utvikler også ESAs instruksverk for kommunikasjonssikkerhet (*ESA COMSEC Instructions*)

NSM stiller for Norge i disse panelene.

Komiteen og panelene møtes ordinært to ganger årlig, men hyppigere ved behov. Ledervervet i komiteen og panelene går på rundgang mellom medlemslandene, mens *ESA Security Office* ivaretar sekretariatsfunksjonen.

7.1.3 Eurocontrol

Eurocontrol er en mellomstatlig paneuropeisk organisasjon. Eurocontrol har som primært formål å utvikle og harmonisere et sikkert og effektivt system for lufttrafikkstyring (*Air Traffic Management* (ATM)) i Europa. I denne organisasjonen foreligger det en avtale fra 1969; *Mulitilateral Agreement relating to the Protection of Eurocontrol Classified Material.* Avtalen omhandler sikkerhetsgradering og beskyttelse av sikkerhetsgradert informasjon produsert av Eurocontrol eller frigitt til Eurocontrol fra en medlemsstat. Et vedlegg til avtalen gir detaljerte bestemmelser om hvordan Eurocontrol-sikkerhetsgradert informasjon skal beskyttes, og forplikter medlemslandene til å sikkerhetsklarere egne lands borgere som skal ha tilgang til Eurocontrol-sikkerhetsgradert informasjon med et klareringskrav.

Vedlegget forutsetter også at hvert medlemsland skal utpeke en koordinerende myndighet for beskyttelse av Eurocontrol sikkerhetsgradert informasjon. I Norge er NSM utpekt som koordinerende myndighet.

7.1.4 Multinational Industrial Security Working Group (MISWG)

MISWG har sitt utspring i NATO, men består i dag av 38 land. NATO, EU-kommisjonen, European Defence Agency (EDA), ESA og OCCAR deltar som observatører.

Gruppen skal tilrettelegge for samarbeid og informasjonsdeling ved internasjonale sikkerhetsgraderte anskaffelser, samt søke å standardisere sikkerhetsprosedyrene knyttet til slike anskaffelser.

Gruppen består av representanter fra medlemslandenes NSA og/eller DSA med ansvar for sikkerhetsgraderte anskaffelser. NSM representerer Norge i gruppen. MISWG møtes en gang årlig i plenum. Arbeidet i MISWG koordineres av en *Executive Committee*, som består av valgte representanter blant medlemmene samt foregående og kommende vertsnasjoner for det årlige plenumsmøtet. Vertskapet for dette møtet går på rundgang mellom landene. Norge skal arrangere møtet i 2028 og vil inngå i Executive Committee fra 2026.

Plenumsmøtet kan nedsette *Ad Hoc Working Groups* (AHWG) og *Communities of Practice* (COP). Per i dag er det 5 AHWG og 4 COP i arbeid. Deltakelse i disse gruppene er basert på frivillighet, dog slik at retningslinjene for MISWG oppfordrer til aktiv deltakelse fra medlemmene. Gruppenes møtefrekvens er normalt ett til to årlige møter.

7.2 Internasjonale organisasjoner der Norge ikke er medlem

7.2.1 Den europeiske union (EU)

I EU faller beskyttelse av sikkerhetsgradert informasjon utenfor unionsretten. Medlemslandene forplikter seg til å beskytte EU sikkerhetsgradert informasjon gjennom en mellomstatlig avtale mellom medlemslandene.[108] De ulike EU institusjonene og EU-byråene har alle egne regelverk for beskyttelse av sikkerhetsgradert informasjon. Sikkerhetsbestemmelsene er harmoniserte mellom disse gjennom at Rådets sikkerhetsbestemmelser skal være de normerende.

Utveksling av sikkerhetsgradert informasjon mellom Norge og EU skjer på basis av en sikkerhetsavtale mellom Norge og EU fra 2004.[109] Etter denne avtalen har partene en gjensidig plikt til å beskytte den annen parts sikkerhetsgraderte informasjon som egen informasjon med tilsvarende graderingsnivå. Mer detaljerte sikkerhetsbestemmelser følger av et eget arrangement til avtalen. Etter arrangementet er NSM i rollen som NSA ansvarlig for å gjennomføre og kontrollere etterlevelsen av avtalen i Norge. NSM er også kontaktpunkt mot de tilsvarende sikkerhetsfunksjonene på EU siden.

Partene til avtalen i EU er Rådet, Kommisjonen og *European External Action Service* (EEAS – EU's utenrikstjeneste). Avtalen kommer derfor i utgangspunktet bare til anvendelse for informasjon som Norge utveksler med disse. På denne bakgrunn har Norge ved Forsvarsdepartementet inngått et eget arrangement for utveksling

[108] *Agreement between the Member States of the European Union, meeting within the Council, regarding the protection of classified information exchanged in the interests of the European Union* av 04.05.2011.

[109] Avtale mellom Norge og Den europeiske union om sikkerhetsprosedyrene ved utveksling av gradert informasjon av 22.11.2004.

av sikkerhetsgradert informasjon med *European Defence Agency* (EDA – EU's forsvarsbyrå). Det er videre under forhandling et arrangement for utveksling av sikkerhetsgradert informasjon med *Frontex* som er EU's byrå med ansvar for samordning av EU-landenes kontroll og overvåkning av EUs yttergrenser. NSM har samme funksjon etter disse arrangementene som i det ovennevnte.

I utgangspunktet er arbeid med nasjonal sikkerhet en nasjonal kompetanse for EUs medlemsland.[110] Samarbeidet mellom medlemslandene på dette området har likevel over tid økt over tid og EUs organer har fått stadig flere oppgaver knyttet til forebyggende sikkerhet. Det utarbeides felles regelverk som forplikter medlemslandene, det vedtas felles finansiering og det foregår politiske drøftinger som ikke er forpliktende. Den vanligste formen for reguleringer er at det etableres minstestandarder og eventuelt oppgaver som skal løses innenfor rammen av EU, som deretter gjennomføres nasjonalt og der det er en viss grad av nasjonale variasjoner.

Norge tar del i sikkerhetssamarbeidet i EU der det tar form av rettsakter som enten er EØS-relevante eller Schengenrelevante. Norge har i tillegg sluttet seg til enkelte politiske overenskomster eller bilaterale avtaler. Utviklingen i EU på sikkerhetssiden, og særlig innen digital sikkerhet der antallet rettsakter nå begynner å bli betydelig, vil få stor betydning for Norge.

Nedenfor redegjøres det for sentrale føringer for hvordan EUs medlemsland arbeider med forebyggende sikkerhet. Oversikten er ikke uttømmende.

EU Security Union
EUs sikkerhetsunion er en strategi for å støtte medlemsstatenes oppdrag med å ivareta borgernes sikkerhet og verne om europeiske grunnverdier. Sikkerhetsunionen er et overordnet rammeverk for forebyggende offensiv og defensiv sikkerhet. Den første strategiperioden var årene 2016-2020, mens den nåværende strategien varer ut 2025. Strategien bygger på fire pilarer: Bekjempelse av terrorisme og organisert kriminalitet, beskyttelse av fysisk og digital infrastruktur, og å bygge opp et sterkt sikkerhetsøkosystem. Det siste elementet går ut på å tilrettelegge for utveksling av informasjon mellom nasjonale myndigheter og EU og å imøtegå trusler fra sammensatt virkemiddelbruk og nye teknologier. Europakommisjonen rapporterer om status for alle tiltakene som er iverksatt under strategien.

Nærmere om digital sikkerhet
EU har et eget byrå for cybersikkerhet, *European Union Agency for Cybersecurity* (ENISA). ENISA ble etablert i 2004 og skal styrke EUs medlemslandenes kapasitet og beredskap innen cybersikkerhet. Byrået hjelper til med å beskytte kritisk informasjon, infrastruktur og tjenester mot cybertrusler og -angrep og fremmer samarbeid på tvers av EU-landene innen cybersikkerhet. Norge er assosiert medlem av ENISA,

[110] EU-traktatens paragraf 4.2: *»The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State.»*

men uten stemmerett.[111] Medlemskapet ivaretas av både Justis- og beredskapsdepartementet og Digitaliserings- og forvaltningsdepartementet.

7.2.2 Organisasjonen for Felles Forsvarssamarbeid

Organisasjonen for Felles Forsvarssamarbeid*, Organisation for Joint Armament Cooperation* (OCCAR) er en internasjonal organisasjon bestående av seks land, Tyskland, Frankrike, Belgia, UK, Italia og Spania, som gjennomfører komplekse forsvarsmateriell-prosjekter. Organisasjonen produserer sikkerhetsgradert informasjon, og har et eget regelverk for beskyttelse av denne informasjonen.

For å tilrettelegge for utveksling av sikkerhetsgradert informasjon mellom Norge og OCCAR er det inngått en bilateral sikkerhetsavtale som forplikter partene til gjensidig beskyttelse av gradert informasjon som er utvekslet.[112] Avtalen forutsetter at det skal utpekes en kompetent sikkerhetsmyndighet med ansvar for å påse at avtalens bestemmelser blir gjennomført. På norsk side er dette ansvaret lagt til NSM.

7.3 Rettsakter i EU som skal gjennomføres i norsk lov

EU har vedtatt en lang rekke rettsakter for å ivareta digital sikkerhet, og mange av dem innebærer forpliktelser og oppgaver for nasjonale myndigheter. Rettsaktene kan ha forskjellige formål, fra å beskytte borgere, markeder og land mot angrep til å understøtte konkurransekraft og industrielle vekstvilkår. Relevante eksempler på rettsakter er:

NIS1-direktivet pålegger medlemsstatene å sørge for et visst nivå for landets IKT-sikkerhet ved å lage en strategi for sikkerhetsarbeidet, etablere en IKT-sikkerhetsberedskapsenhet (CSIRT) og pålegge operatører og leverandører av samfunnsviktige tjenester IKT-sikkerhetskrav og varslingsplikt ved alvorlige IKT-sikkerhetshendelser. Direktivet etablerer to internasjonale samarbeidsgrupper, en på strategisk nivå og en på CSIRT-nivå. NIS-direktivet skal iverksettes i norsk rett gjennom digitalsikkerhetsloven. Denne ble vedtatt i desember 2023, men iverksettelse avventer nødvendig forskrift. Utkast til slik forskrift har vært på høring med frist i desember 2024. Regelverksforvalter er Justis- og beredskapsdepartementet. I utkast til forskrift gis NSM flere oppgaver i oppfølgingen av regelverket.

NIS2-direktivet stiller krav til at medlemsstatene skal sørge for et felles minimum cybersikkerhetsnivå og ha en nasjonal cybersikkerhetsmyndighet, samt samarbeide med andre EU-medlemsland om cybersikkerhet. NIS2direktivet er en videreutvikling av NIS-direktivet. Justis- og beredskapsdepartementet er regelverksforvalter. Direktivet planlegges gjennomført i norsk rett i en ny lov om grunnsikring av

[111] Posisjonsnotat av 23/1 2023 om Europaparlaments- og rådsforordning (EU) 2019/881 av 17. april 2019 om ENISA (Den europeiske unions cybersikkerhetsbyrå), om cybersikkerhetssertifisering av informasjons- og kommunikasjonsteknologi og om oppheving av forordning (EU) nr. 526/2013 (cybersikkerhetsforordningen).

[112] Sikkerhetsavtale mellom Kongeriket Norges regjering og Organisasjonen for Felles Forsvarssamarbeid av 28.06.2023.

kritiske virksomheter som også skal ta inn CER-direktivet. NSM og Direktoratet for samfunnssikkerhet og beredskap (DSB) har på oppdrag fra Justis- og beredskapsdepartementet i fellesskap utarbeidet forslag til høringsdokument om loven. NSM vil etter forslaget fortsatt ha en rekke oppgaver i oppfølgingen av regelverket og enkelte oppgaver foreslås ivaretatt av NSM og DSB i fellesskap.

EU har prioritert motstandsdyktighet høyt og har varslet at det vil fortsette. Et sentralt tiltak er *direktiv om motstandsdyktighet i kritiske virksomheter* (*Critical Entities Resilience Directive*). Denne rettsakten omtales som CER-direktivet og stiller krav om minimums beredskapsnivå i virksomheter som leverer samfunnskritiske varer og tjenester i følgende elleve sektorer: energi, transport, bank, finans, helse, drikkevann, avløpsvann, digital infrastruktur, offentlig administrasjon, rommet, og næringsmidler (produksjon, bearbeiding og distribusjon). Direktivet er avstemt med andre EU-initiativer innen klimatilpasning, sivilbeskyttelse, cybersikkerhet og regler om finansielle tjenester, og i særlig grad med NIS2-direktivet. Rettsakten stiller også krav til nasjonale myndigheter om å stille minstekrav og peke ut virksomheter som skal underlegges direktivets virkeområde. Direktivet inneholder retningslinjer for koordinering ved hendelser som treffer flere medlemsland.[113] Direktivet er ansett som EØS-relevant.

Cybersikkerhetsforordningen (Cyber Security Act) etablerer en felles sertifiseringsordning for ulike sider ved cybersikkerhet, som produkter, tjenester, prosesser og sikkerhetsledelse. Ordningen skal bidra til like standarder. Justis- og beredskapsdepartementet er ansvarlig departement. Forordningen vil etablere reviderte sertifiseringsordninger. NSM ved SERTIT forvalter dagens sertifiseringsordning i EU for IT-sikkerhet i produkter og systemer (SOG-IS).

Cybersolidaritetsforordningen (*Cyber Solidarity Act*) forplikter medlemslandene til å samarbeide i håndtering av cyberhendelser. Forordningens vil kunne legge føringer for den nasjonale responsfunksjonen i NSM.

Cybermotstandsdyktighetsforordningen (*Cyber Resilience Act*) stiller felles krav til cybersikkerhet for produkter med digitale elementer. Digitaliserings- og forvaltningsdepartementet er ansvarlig departement. Nasjonal kommunikasjonsmyndighet (NKOM) vil trolig få oppgaver i oppfølgingen av forordningen.

Forordning om håndtering av spredning av terrorrelatert innhold på internett (*Terrorist Content Online Act*) stiller krav om tidlig deteksjon og fjerning av terrorrelatert innhold på nett. Medlemslandene skal peke ut en kompetent myndighet som forvaltningsansvarlig for regelverket.

Forordning om digital operativ motstandsdyktighet (*Digital Operational Resilience Act – DORA*) stiller krav til digital sikkerhetsstyring i finanssektoren, herunder tilsyns- og rapporteringskrav for kompetente myndigheter.

[113] Council Recommendation of 25 June 2024 on a blueprint to coordinate a response at Union level to disruptions of critical infrastructure with significant cross-border relevance. Text with EEA relevance. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202404371

Forordning om kunstig intelligens (*Artificial Intelligence Act*) fastsetter felles regler for hva kunstig intelligens kan brukes til etter en risikobasert tilnærming, hvor risikoen for misbruk som kan føre til urimelig skade er det utslagsgivende for kategoriplassering og hvor strenge begrensninger som legges på systemet. Noen anvendelser av KI forbys helt, og andre klassifiseres som «høyrisiko», hvor de må møte krav knyttet til risikohåndtering, transparens, menneskelig tilsyn, m.m. Forordningen legger direkte føringer på nasjonale myndigheters bruksmuligheter. Digitaliserings- og forvaltningsdepartementeer ansvarlig departement og NKOM får oppgaver i oppfølgingen av forordningen.

Forordning om digitale tjenester (*Digital Services Act*) pålegger digitale tjenestetilbydere forpliktelser til å fjerne ulovlig innhold fra sine plattformer. Medlemslandene må utpeke en kompetent myndighet som skal forvalte rettsakten innenfor sin jurisdiksjon og samarbeid innenfor rammen av EU. Delene av tilsynet som gjelder de største plattformene ligger i kommisjonen. Digitaliserings- og forvaltningsdepartementeer ansvarlig departement, med NKOM som sannsynlig utøver.

De nevnte rettsaktene anses som EØS-relevante og vil sannsynligvis bli norsk lov. Prosessen er ikke endelig fullført for alle rettsaktene.

I tillegg til rettsakter har EU andre samarbeidsflater for digital sikkerhet. Under følger noen eksempler på dette:

Secure Connectivity Programme 2023-27 er et investeringsprogram for å bygge felles satellittbasert infrastruktur for sikker kommunikasjon. Nærings- og fiskeridepartementet er ansvarlig departement.

5G Toolbox er en tiltakspakke for å sikre en koordinert tilnærming til sikkerhet i utrulling av 5G-nettverk innenfor EU. Dette omfatter oppgaver for medlemsstatene og Kommisjonen.

Cyber Diplomacy Toolbox er et rammeverk for koordinert diplomatisk tilsvar til ondsinnede cyberhendelser. Skal legge til rette for at EUs medlemsstater snakker med én stemme.

7.4 Bilateral utveksling av sikkerhetsgradert informasjon med andre stater

Utveksling av sikkerhetsgradert informasjon med andre stater forutsetter at den mottakende stat påtar seg et ansvar for å beskytte informasjonen på en forsvarlig måte. På denne bakgrunn er det internasjonal praksis at utveksling av sikkerhetsgradert informasjon i utgangspunktet bare kan skje der det foreligger en sikkerhetsavtale mellom de berørte landene. Sikkerhetsavtalene gir bestemmelser om hvordan sikkerhetsgradert informasjon skal utveksles på en sikker måte og hvordan informasjonen skal håndteres av den mottakende stat. Normalt gjøres dette i form av en gjensidig anerkjennelse mellom partene av den annen parts regelverk og prosedyrer for beskyttelse av sikkerhetsgradert informasjon. Dette er mulig på bakgrunn av at prinsippene for beskyttelse av sikkerhetsgradert informasjon har blitt internasjonalt anerkjente, med utgangspunkt i NATOs sikkerhetsmessige tilnærming.

Sikkerhetsavtaler kan inngås i noe ulik form. Enkelte av avtalene er inngått på regjeringsnivå i form av traktater, mens andre er inngått som avtaler mellom departementer, i det vesentlige av Forsvarsdepartementet, uten rettsvirkninger som traktat. Disse avtalene vil da ha utveksling av sikkerhetsgradert informasjon innenfor forsvarssektoren som virkeområde, men de kan også ha et snevrere virkeområde, for eksempel avgrenset til materiellsamarbeid eller et konkret program eller prosjekt.

Norge har i dag slike avtaler med 42 land. Sikkerhetsavtaler fremforhandles normalt mellom de respektive sikkerhetsmyndighetene (NSA-funksjonen). I Norge forhandles og reforhandles slike avtaler av NSM i samarbeid med Justis- og beredskapsdepartementet og Forsvarsdepartementet.

Også de bilaterale avtalene forutsetter at det utpekes en kompetent sikkerhetsmyndighet hos hver av avtalepartene. Denne er kontaktpunkt mot den tilsvarende myndigheten i det andre landet og har ansvar for å påse at avtalen gjennomføres i eget land. Den utpekte myndigheten er videre ansvarlig for å bekrefte og iverksette sikkerhets- og leverandørklareringsprosesser på forespørsel fra sikkerhetsmyndigheten i det andre landet, undersøke og rapportere om eventuelle sikkerhetsbrudd knyttet til sikkerhetsgradert informasjon mottatt fra den annen part, og motta tilsvarende rapporter om egen informasjon utlevert den annen part. Det tilligger også de kompetente sikkerhetsmyndighetene å avtale alternative måter å utveksle sikkerhetsgradert informasjon som avviker fra avtalens hovedregel, herunder hvordan sikkerhetsgradert informasjon kan utveksles elektronisk.

I Norden er det etablert multilaterale informasjonssystemer for å utveksle sikkerhetsgradert informasjon mellom de nordiske landene. Krav og forpliktelser er her definert i et teknisk arrangement inngått mellom de nordiske kompetente sikkerhetsmyndigheter. For å følge opp arrangementene og sikkerheten i systemene har de kompetente sikkerhetsmyndighetene etablert et *Nordic System Security Consultation Board* som møtes en til to ganger årlig. NSM representerer Norge i dette forumet.

8 Forebyggende nasjonal sikkerhet i andre land

Utvalget er i mandatet bedt om å «s*e hen til andre sammenlignbare lands organisering av arbeidet med forebyggende nasjonal sikkerhet*». Vi har valgt å se på hvordan arbeidet med forebyggende sikkerhet er organisert i seks andre land.

Danmark, Sverige, Finland og Nederland er valgt fordi de vurderes å være nokså sammenlignbare med Norge, også med hensyn til utfordringer og muligheter i arbeidet med forebyggede sikkerhet. I tillegg beskrives systemene i *USA og Storbritannia* fordi de har stor betydning for Norges sikkerhet generelt og for det forebyggende sikkerhetsarbeidet spesielt.

Informasjonen om systemene i andre land er i hovedsak hentet fra regelverk og forarbeider til regelverk i landene og fra publikasjoner og pressemeldinger fra landenes myndigheter. Hensikten med fremstillingen er å redegjøre for noen hovedtrekk, og ikke å gi et fullstendig bilde av arbeidet med forebyggende sikkerhet i de ulike landene. Dette er gjerne nokså komplekse systemer med mange regelverk og aktører, og detaljer om oppgaveløsning er ikke alltid åpent tilgjengelig. Det tas derfor forbehold om at det kan være elementer som ikke er fanget opp.

Et hovedinntrykk fra gjennomgangen er at organiseringen av arbeidet med forebyggende sikkerhet varierer mye fra land til land. Disse forskjellene må ses i lys av at det er nokså store forskjeller generelt hvordan land organiserer sin egen forvaltning. De ulike systemene har gjerne lange historiske røtter og må passe inn i landenes rettstradisjoner.

Arbeidet med forebyggende sikkerhet i de landene vi har sett på, synes gjennomgående å være mer fragmentert og oppdelt enn i Norge. Her er det selvsagt snakk om grader, også i Norge er det en rekke lover og annet regelverk som omhandler forebyggende sikkerhet og mange aktører som følger dette regelverket opp. Vi har likevel ikke identifisert en tilsvarende myndighet med et sektorovergripende ansvar i de andre landene slik Norge har gjennom NSM. Tilsvarende synes regelverket å være mer oppdelt enn det vi har gjennom sikkerhetsloven. Også skillet mellom sivil og militær sektor er mer markant i enkelte andre land, men ikke alle. I Norge favner sikkerhetsloven og NSM over begge sektorene. Et trekk ved organiseringen i flere andre land er videre at en del etater med ansvar for forebyggende sikkerhet også har ansvar for etterretningsfunksjoner, slik systemet var i Norge fram til 1965. Dette gjelder gjennomgående for de landene som vi har sett på i dette kapittelet.

Det er også likhetstrekk mellom Norge og andre land. Innen digital sikkerhet har flere av landene tilsvarende sentre som NSM har i Nasjonalt cybersikkerhetssenter

(NCSC) hvor man samler funksjoner og tjenester og hvor samarbeidspartnere møtes for å dra nytte av hverandres arbeid.

Danmark har et klarere skille enn Norge mellom sivil og militær sektor i å ivareta av nasjonal forebyggende sikkerhet, selv om skillet er blitt noe mindre tydelig ved opprettelsen av *Ministerium for Samfundssikkerhed og Beredskab* i 2024 og overføringen av oppgaver blant annet fra både det danske Justisdepartementet og Forsvarsdepartementet. I tillegg synes arbeidet med sikkerhet å ha blitt mer samlet med opprettelsen av det nye departementet.

I Sverige er det utbredt samarbeid mellom de ulike myndighetene med ansvar for forebyggende sikkerhet. I likhet med Norge skjer dette samarbeidet innenfor rammen av en samlende sikkerhetslov. Sverige har likevel ikke én virksomhet med det samme brede, tverrsektorielle mandatet som det NSM i Norge har.

Finland har flere forskjellige aktører med ansvar for å ivareta nasjonal sikkerhet. Det er ikke én enhetlig nasjonal sikkerhetslov som regulerer forebyggende sikkerhet i landet. Nederland har en sentral etat som har oppgaver som dekker betydelige deler av NSMs virksomhet, men ingen sentral lov som den norske sikkerhetsloven.

Forebyggende sikkerhet i USA omfatter en rekke mekanismer både på føderalt og delstatsnivå. USA har ikke én samlet sikkerhetslov, men en rekke sikkerhetslover for forebyggende sikkerhet innen ulike samfunnsområder. Systemet er komplekst med mange institusjoner der ingen synes å direkte kunne sammenliknes med NSM. I USA er det videre et tydeligere skille mellom militær og sivil sektor enn i Norge.

Heller ikke i Storbritannia er det en sentral etat med et sektorovergripende ansvar for forebyggende sikkerhet. Ansvaret er mer desentralisert der ulike myndigheter og organisasjoner har spesifikke ansvarsområder. De senere årene har likevel Cabinet Office fått en mer sentral og sektorovergripende myndighet for å ivareta forebyggende sikkerhet, og i arbeidet med cybersikkerhet er det etablert samordningsorganer som har likhetstrekk med Nasjonalt cybersikkerhetssenter i Norge. Storbritannia har videre flere lover for beskyttelse av den nasjonale sikkerheten.

8.1 Danmark

Danmark har ikke noen virksomhet som kan sammenlignes med NSM. Danmark har heller ikke en sektorovergripende lov om forebyggende sikkerhet.[114] Som i Norge, står sektoransvarsprinsippet generelt sterkt i Danmark.

Den danske regjeringen opprettet i august 2024 et nytt *Ministerium for Samfundssikkerhed og Beredskab*. Det nye departementet fikk ansvar for å forebygge, motstå og håndtere hendelser som utfordrer samfunnets grunnleggende funksjoner.[115]

[114] Danmark har heller ikke et særskilt sektorovergripende lovverk om beskyttelse av kritisk infrastruktur. Sikkerhetsgradert informasjon og sikkerhetsklarering av personell er nærmere regulert i *Sikkerhedscirkulæret* av 17. desember 2014.

[115] https://mssb.dk/nyheder/2024/august/regeringen-opretter-nyt-ministerium-for-samfundssikkerhed-og-beredskab/.

Ministerium for Samfundssikkerhed og Beredskab har blant annet fått ansvar for beredskap innen cybersikkerhet og digital informasjonssikkerhet og et koordinerende ansvar for krisehåndtering og forsyningssikkerhet. Flere av oppgavene ble overført fra Forsvarsministeriet, som ansvaret for beredskap og *Beredskapsstyrelsen* (BRS), cybersikkerhet og digital informasjonssikkerhet, deler av *Center for Cybersikkerhed* (CFCS), rollen som nasjonal IT-sikkerhetsmyndighet, akkreditering av IT-systemer til behandling av klassifiserte opplysninger og ansvaret for gjennomføring og tilsyn og koordinering av NIS2-direktivet. Fra Justisdepartementet ble blant annet *Styrelsen for Forsyningssikkerhed* (SFOS) og oppgaven med å koordinere nasjonal krisehåndtering overført.[116] I tillegg ble det nye ministeriet tilført flere oppgaver fra seks andre ministerier, blant annet innen cybersikkerhet.[117]

Med opprettelsen av Ministerium for Samfundssikkerhed og Beredskab er det nå ett departement med ansvar for en rekke av virksomhetene som bidrar i arbeidet med forebyggende sikkerhet i Danmark, men ikke alle. I januar 2025 ble det annonsert at det nye ministeriets fagområder samles i to styrelser (etater).[118] Digital sikkerhet, forsyningssikkerhet og informasjonssikkerhet samt den *Nationale Operative Stab* (NOST) ble samlet i *Styrelsen for Samfundssikkerhed* (SAMSIK). I og med at sikker kommunikasjon og systemer for behandling av graderte opplysninger, fysisk informasjonssikkerhet og internasjonalt samarbeid med blant annet EU, NATO og Norden er blant SAMSIKS hovedoppgaver, vil denne styrelsen trolig bli en viktig samarbeidspartner for NSM.

Den andre styrelsen, *Beredskapsstyrelsen* (BRS), fikk tilført nye oppgaver slik som havmiljøberedskap og kystredningstjeneste. BRS har et bredt ansvar innen forebygging, håndtering og respons på ulike typer kriser i Danmark. BRS skal utvikle samfunnets evne til å forebygge og motstå ulykker, kriser og katastrofer og bistå andre myndigheter ved behov for ekstra personell og utstyr. BRS har mange likhetstrekk med både Direktoratet for samfunnssikkerhet og beredskap (DSB) og Sivilforsvaret i Norge.[119] Viktige oppgaver for BRS er håndtering av den statlige beredskapen, strategisk beredskapsplanlegging og å gjennomføre, føre tilsyn med og koordinere oppfølgingen av CER-direktivet. BRS er også involvert i å trygge Danmarks kritiske infrastruktur mot både naturlige og menneskeskapte trusler.

Andre hovedsamarbeidspartnere for NSM i Danmark er landets to etterretningstjenester, *Politiets Efterretningstjeneste* (PET) og *Forsvarets Efterretningstjeneste* (FE) som sammen ivaretar rollen som nasjonal sikkerhetsmyndighet (NSA) for henholdsvis sivil sektor og forsvarssektoren.

PETs oppgave er å forebygge, undersøke og motvirke trusler mot frihet, demokrati og sikkerhet i Danmark. PET ligger under det danske justisdepartementet og reguleres av lov om Politiets Efterretningstjeneste. Av loven fremgår det at PET skal

[116] De to sistnevnte lå i *Rigspolitiet*.

[117] Fra Finansministeriet, Erhvervsministeriet, Miljøministeriet, Digitaliserings- og Ligestillingsministeriet, Uddannelses- og Forskningsministeriet og Klima-, Energi- og Forsyningsministeriet, jf. kgl-resolution-af-29-august-2024.

[118] https://mssb.dk/aktuelt/2025/januar/ministeriet-for-samfundssikkerhed-og-beredskab-omorganiseres/ Ministeriet for Samfundssikkerhed og Beredskab 29. januar 2025.

[119] Beredskabsstyrelsen har blant annet eget personell hvori det også inngår vernepliktige.

«*være national sikkerhedsmyndighed og rådgive og bistå offentlige myndigheder og private i sikkerhedsspørgsmål, herunder at bistå ved personsikkerhedsundersøgelser*».[120] Som etterretningstjeneste samler, analyserer og formidler PET informasjon om trusler mot Danmark og danske interesser.

Som sikkerhetstjeneste skal PET også motvirke de truslene etterretningsinnsatsen identifiserer.[121] En av seks hovedoppgaver for PET er å gi råd om sikkerhet. Enhver offentlig myndighet i Danmark er klareringsmyndighet for eget personell og for ansatte i private selskaper som arbeider for den offentlige myndigheten. PET gjennomfører personkontroll som grunnlag for myndighetenes sikkerhetsklareringer.

FE er i all hovedsak direkte underlagt Forsvarsministeriet. FE har fire hovedoppgaver: 1) utenriks- og militæretterretningstjeneste 2) militær sikkerhetstjeneste, blant annet militære sikkerhetsklareringer) 3) nettsikkerhetstjenester og 4) defensive og offensive cybereffekter til det danske Forsvaret.[122]

FE har et særskilt ansvar for industrisikkerhet innen både militær og sivil sektor. FE utøver også rollen som *National Communication Security Authority* (NCSA), mens ansvaret for kryptodistribusjon ivaretas av *Forsvarsministeriets Materiel- og Inkøbsstyrelse*.

Som nevnt ble *Center for Cybersikkerhed* (CFCS) overført fra Forsvarsministeriet til *Ministerium for Samfundssikkerhed og Beredskab*, men ikke hele senteret. *Netsikkerhedstjenesten* og øvrige deler av senteret som ivaretar den operative defensive cyberinnsatsen samt oppgaver vedrørende Forsvaret, ble ikke overført.

CFSC kan sammenliknes med Nasjonalt cybersikkerhetssenter (NCSC) i Norge, men har også andre oppgaver. CFCS er regulert av en egen lov.[123] CFCSs hovedoppgave er å bidra til høy sikkerhet for infrastrukturen for informasjon og kommunikasjon som samfunnsviktige funksjoner er avhengige av. CFCF skal oppdage, analysere og bidra til å motvirke avanserte cyberangrep mot myndigheter og virksomheter som er engasjert i samfunnsviktige funksjoner.

Nettsikkerhedtstjenesten ble etablert i 2014 som en sammenslåing av de to varslingstjenestene GovCERT og MILCERT. Nettsikkerhetstjenesten har som oppgave å avdekke, analysere og bidra til å motvirke sikkerhetshendelser i Forsvaret og de virksomhetene og statlige myndighetene som er tilknyttet tjenestens såkalte sensornettverk. Regioner, kommuner og private virksomheter som utfører samfunnsviktige funksjoner, kan på forespørsel kobles til tjenesten. Sensornettverket kan sammenliknes med Varslingssystem for digital infrastruktur (VDI) i Norge som driftes og organiseres av NSM ved NCSC.

I *National strategi for cyber- og informationssikkerhed 2022–2024* som ble lansert av den danske regjeringen i 2021, slås det fast at cyber- og informasjonssikkerhet i

[120] Lov om Politiets Efterretningstjeneste (PET) 19. desember 2014, § 1, nr. 5.

[121] Center for Terroranalyse (CTA) som inngår i PET er et senter med ansatte fra fire danske myndigheter: FE, PET, Udenrigsministeriet og Beredskabsstyrelsen. CTA analyserer og vurderer terrortrusselen mot Danmark og danske interesser i utlandet.

[122] FE er regulert av Lov om Forsvarets Efterretningstjeneste (FE) 4. januar 2016, jf. § 1, nr. 3 stk. 2.

[123] Lov om Center for Cybersikkerhed 25. juni 2014.

Danmark er basert på sektoransvarsprinsippet.[124] Det innebærer at de enhetene som har ansvaret for en oppgave til daglig, også har ansvaret når det oppstår en cyberhendelse. Enhetene skal selv sørge for at den får bistand fra driftsleverandør dersom det er inngått avtale om dette, eller fra «de sentrale cybersikkerhedsenheter» hvis det er behov for det. Berørt enhet er dessuten selv ansvarlig for å aktivere slik støtte, stå for den innledende håndtering og, avhengig av hendelsens omfang, anmelde til politiet samt informere kompetente myndigheter. Det er likeledes den ansvarlige enheten som i utgangspunktet skal informere utad om hendelsen dersom det er behov for det. Ved større cyberhendelser som påvirker flere sektorer, kan *National Operativ Stab* (NOST), som var forankret i Rigspolitiet og nå er del av SAMSIK underlagt det nye Ministerium for Samfundssikkerhed og Beredskab, aktiveres.

Medio januar 2025 ble det annonsert en ny politisk avtale om beredskapsområdet mellom den danske regjeringen og seks partier i Folketinget. Et element i avtalen er at det skal utarbeides en ny nasjonal strategi for cyber- og informasjonssikkerhet i 2025.[125]

8.2 Sverige

Arbeidet med å ivareta nasjonal forebyggende sikkerhet i Sverige er delt mellom ulike statlige aktører. Sverige har i likhet med Norge en egen lov om beskyttelse av nasjonal sikkerhet; *Säkerhetsskyddslagen*. Säkerhetsskyddslagen ble revidert i 2018 (SFS 2018:585) da både cybersikkerhet og beskyttelse av informasjon og infrastruktur mot moderne trusler ble tillagt mer vekt enn tidligere.[126] Revisjonen sammenfalt i tid med revisjonen av den norske sikkerhetsloven.

Säkerhetsskyddslagen ble betydelig revidert igjen i 2021 (SFS 2021:952) da virkeområdet ble ytterligere utvidet, kravene til private aktører som arbeider med kritisk infrastruktur eller som har tilgang til sensitiv informasjon ble strammet til, og det ble strengere krav til tilsyn og oppfølging fra myndighetene. Det er etter loven opp til virksomhetene selv å vurdere om virksomheten er av betydning for Sveriges nasjonale sikkerhet. Virksomhetene har i så fall en plikt til å melde fra om dette til relevant tilsynsmyndighet. Brudd på meldeplikten kan medføre sanksjoner.

Säkerhetsskyddsförordning fra 2021 (SFS 2021:955) presiserer enkelte bestemmelser i Säkerhetsskyddslagen, blant annet kravene til hvordan virksomheter skal håndtere informasjonssikkerhet, fysisk sikkerhet, personellsikkerhet og organisatorisk sikkerhet. Det angis også hvem som er tilsynsmyndighet for ulike myndigheter og virksomheter.[127] Både Forsvarsmakten og Säkerhetspolisen er sentrale tilsyns-

[124] National strategi for cyber- og informationssikkerhed 2022-2024. Sektoransvars-prinsippet er i strategien blant annet utlagt til å innebære at den myndighet, som har ansvaret for en oppgave til daglig, bevarer ansvaret under en hendelse. Det gjelder både i daglig beredskap, under hendelser og ved gjenoppretting etter hendelser.

[125] https://mssb.dk/aktuelt/2025/januar/ny-beredskabsaftale/Ministeriet for Samfundssikkerhed og Beredskab 15. januar 2025.

[126] Den reviderte loven utvidet virkeområde gjennom at flere private aktører som håndterer sensitiv informasjon eller arbeider med kritisk infrastruktur ble inkludert.

[127] Säkerhetsskyddsförordning (2021:955) | Sveriges riksdag.

myndigheter i tillegg til andre myndigheter med ansvar for egne sektorer, som Finansinspektionen og Försvarets materielverk. Länsstyrelsene i fire av Sveriges 21 län (tilnærmet norske fylker) fører tilsyn med kommuner, regioner, statlige myndigheter og andre virksomheter.

Samtidig som Sverige har én lov som overbygg, fremstår utøvelsen av forebyggende sikkerhet mer delt opp i Sverige enn i Norge. Ulike statlige myndigheter har spesifikke ansvarsområder som dekker ulike sider av nasjonal sikkerhet. En sektorovergripende funksjon ligger dog i Utenriksdepartementet, som er National Security Authority (NSA) i forhold til NATO og andre land.

Det svenske forsvaret, Försvarsmakten, har viktige oppgaver i arbeidet med nasjonal sikkerhet. Militära underrättelse- och säkerhetstjänsten (MUST) følger den sikkerhetspolitiske og militære utviklingen i Sveriges nærområde og andre deler av verden som er av betydning for svensk utenriks-, sikkerhets- og forsvarspolitikk. Arbeidet består i å innhente, bearbeide, analysere og dele informasjon og vurderinger om ulike aktørers intensjoner og evner. MUST er sikkerhetsmyndighet i Försvarsmakten og ivaretar hovedsakelig forebyggende sikkerhet i egen sektor gjennom rådgivning og kontroll. MUST har også ansvaret for klarering av personell. MUST skal også beskytte hele det svenske totalforsvarets kommunikasjons- og it-system fra inntrengning ved hjelp av både signalbeskyttelse og kryptografiske metoder.

Försvarets radioanstalt (FRA) arbeider med signaletterretning og utgjør en del av Sveriges etterretningstjeneste. FRA er en sivil myndighet under Forsvarsdepartementet. FRA skal også ivareta cyber- og informasjonssikkerhet og har lenge bidratt i beskyttelsen mot avanserte cyberangrep. Fra og med 1. november 2024 tok FRA over ansvaret for Sveriges nasjonale cybersikkerhetssenter, Nationellt cybersäkerhetscenter (NCSC).

NCSC ble opprettet i 2020 som del av Myndigheten för samhällsskydd och beredskap (MSB). Med overtakelsen av NCSC fikk FRA ansvaret for å utvikle et støtteapparat til både offentlige og private virksomheters cybersikkerhet. Arbeidet i NCSC gjennomføres og finansieres i samarbeid med Försvarsmakten, MSB, Säkerhetspolisen, Försvarets materielverk (FMV), Polismyndigheten og Post- och telestyrelsen (PTS).[128]

Försvarets materielverk (FMV) er ansvarlig for å anskaffe, utvikle og vedlikeholde materiell og utstyr for Sveriges forsvar og har også oppgaver innen forbyggende sikkerhet blant annet med å se til at kritisk infrastruktur, som kommunikasjonssystemer og forsvarsteknologi, er beskyttet mot cybertrusler og angrep. Sentralt i dette arbeidet er Sveriges Certifieringsorgan för IT-säkerhet (CSEC) som er en uavhengig del av FMV. CSEC er Sveriges nasjonale sertifiseringsorgan for it-sikkerhet i produkter og systemer. FMV er også nasjonal industrisikkerhetsmyndighet og har i denne rollen ansvar for å behandle søknader om leverandørklareringer.

[128] Tilknyttet den organisatoriske endringen annonserte den svenske regjeringen at den ville tilføre FRA 50 millioner kroner for å bygge opp en effektiv og velfungerende virksomhet innen NCSC. Hensikten var å skape et mer formålstjenlig og utadrettet cybersikkerhetssenter som gagner hele samfunnet.

I justissektoren har særlig *Säkerhetspolisen* (SÄPO), Myndigheten för samhällsskydd och beredskap (MSB) og Myndigheten för psykologiskt försvar (MPF) sentrale roller i det svenske apparatet for ivaretagelse av forebyggende sikkerhet.

SÄPO arbeider med å forbygge og avsløre forbrytelser mot Sveriges sikkerhet, bekjempe terrorisme og beskytte den sentrale statsledelsen. SÄPO er videre en sentral aktør i arbeidet med å identifisere, vurdere og forebygge ulike typer trusler som kan påvirke Sveriges nasjonale sikkerhet. SÄPO samarbeider med FRA med å overvåke og analysere trusler fra både innenlandske og utenlandske aktører. SÄPO har et primært ansvar for sikkerheten innenlands mot blant annet terrorisme, mens FRA har ansvar for signaletterretning og cybersikkerhet. SÄPO utøver også rådgiving og kontroll av sivile etater og private foretak som er underlagt sikkerhetslovgivningen, inkludert informasjonssikkerhet, personkontroll for sikkerhetsklarering og sikkerhetsopplæring.

Myndigheten för samhällsskydd och beredskap (MSB) skal styrke samfunnets evne til å forebygge og håndtere ulykker, kriser og konsekvenser av krig. MSB samarbeider med en rekke andre aktører, koordinerer nasjonale beredskapsplaner og arbeider med å forebygge og håndtere kriser, inkludert de som kan oppstå som følge av cybertrusler. CERT-SE, som er Sveriges nasjonale Computer Security Incident Response Team (CSIRT) med oppgave å støtte samfunnet i arbeide med å håndtere og forebygge it-hendelser, er en del av MSB, men det vurderes om CERT-Se skal overføres til NCSC underlagt Försvarets radioanstalt (FRA).[129.] MSB gir støtte og råd til både offentlige og private aktører for å bidra til at sikkerhetstiltakene er på plass for å beskytte kritisk infrastruktur. MSB har også et ansvar for å koordinere innsatsen mellom ulike myndigheters samfunnsvern og beredskap.

En nokså ny institusjon i det svenske arbeid med forebyggede sikkerhet er Myndigheten för psykologiskt försvar (MPF). MPF ble opprettet i 2022 og er en sivil forsvarsmyndighet underlagt det svenske justisdepartementet.[130] MPF arbeider med å styrke samfunnets felles evne med å identifisere og stå imot utilbørlig informasjonspåvirkning fra fremmede makter. For å løse sitt oppdrag informerer og støtter MPF befolkning og myndigheter, kommuner, regioner, næringsliv, sivilsamfunnet og andre organisasjoner. MPF skal blant annet identifisere, analysere og møte utilbørlig informasjonspåvirkning og annen villedende informasjon som rettes mot Sverige eller svenske interesser og støtte medieforetak med å identifisere, analysere og møte utilbørlig informasjonspåvirkning i den utstrekning slik støtte etterspørres.

8.3 Finland

Flere forskjellige aktører har ansvar for å ivareta nasjonal sikkerhet i Finland. Det er ikke én enhetlig nasjonal sikkerhetslov som regulerer forebyggende sikkerhet i landet, men flere lover som regulerer ulike områder.

[129] https://www.ncsc.se/sv/om-centret/.

[130] En tilsvarende myndighet, *Styrelsen för psykolgiskt försvar*, fantes i Sverige frem til 2009 da den ble nedlagt og oppgavene overtatt av MSB.

Utenriksministeriet er Finlands nasjonale sikkerhetsmyndighet (*National Security Authority, NSA*). NSA-funksjonen er organisert som en frittstående enhet i departementet. NSA skal etter lov om internasjonal informasjonssikkerhet[131] veilede og føre tilsyn med hvordan sikkerhetsgradert informasjon håndteres, representere Finland i internasjonale møter, forhandle om internasjonale avtaler om utveksling og beskyttelse av sikkerhetsgradert informasjon og utstede sikkerhetsklareringer ved internasjonalt samarbeid. Forsvarsdepartementet, Forsvarets Huvudstab, sikkerhetspolitiet og Transport- og kommunikasjonsverket er utpekt som sikkerhetsmyndigheter på avgrensede områder. Utenriksministeriet koordinerer departementene og de utpekte sikkerhetsmyndighetenes arbeid for å legge til rette for en helhetlig sikkerhetsstyring på tvers av ulike sektorer.

Forsvarsministeriet leder arbeidet med sikkerhetsstyring innenfor eget forvaltningsområde. Forsvarsministeriet forvalter og kontrollerer også forsvarsforvaltningens tekniske sikkerhet. *Huvudstaben* leder arbeidet i Forsvaret. Huvudstaben har en avdeling for militær etterretning som også tar seg av stabens oppgaver som avgrenset sikkerhetsmyndighet, herunder personellklarering og leverandørklareringer inn mot Forsvaret.

Også det finske *Inrikesministeriet* er sentral i arbeidet med nasjonal sikkerhet.[132] Det finske sikkerhetspolitiet, *Skyddspolisen* (Skypo), er underlagt dette departementet. Skypo skal forebygge og bekjempe de mest alvorlige truslene mot nasjonal sikkerhet og drive etterretning for statens øverste ledelse og andre sikkerhetsmyndigheter. I tillegg leverer Skypo tjenester til andre myndigheter, virksomheter, organisasjoner og offentligheten. Sikkerhetsklarering av finske borgere utføres av Skypo, med unntak av klareringer for forsvarsmakten, som gjøres av Forsvarets Huvudstab. Skypo bidrar til NSAs internasjonale klareringer.

Transport- och kommunikationsverket (Traficom) er utpekt som sikkerhetsmyndighet for teknisk informasjonssikkerhet og kommunikasjonssikkerhet (*National Communications Security Authority (*NCSA)).[133] Traficom er underlagt det finske *Kommunikasjonsministeriet*. I Traficom ligger også det finske cybersikkerhetssentret (NCSC-FI). Det nasjonale cybersikkerhetssenteret skal utvikle tilliten og sikkerheten til kommunikasjonsnettverk og tjenester og hjelpe til med å undersøke brudd på informasjonssikkerheten. Cybersäkerhetscentret CERT (*Computer Emergency Response Team*) har som oppgave å forbygge sikkerhetsbrudd og informere om spørsmål som gjelder informasjonssikkerhet. Beredskap og håndtering av cyberhendelser gjennomføres i et samarbeid mellom flere aktører for å utveksle informasjon og koordinere felles tiltak. Det finnes flere nasjonale nettverk for informasjonsutveks-

[131] Lag om internationella förpliktelser som gäller informationssäkerhet 588/2004. Loven gjelder også for selskaper som er parter i klassifiserte kontrakter. Den pålegger samarbeid og informasjonsdeling mellom sikkerhetsmyndighetene og inneholder bestemmelser om profesjonell taushetsplikt og sikkerhetskrav. Loven inkluderer også personkontroll og utstedelse av personellsikkerhetsklareringer og leverandørklareringer på nivået KONFIDENSIELT og høyere.

[132] 8. mars 2024 ble det under ledelse av innenriksministeriet og sekretariatet for den finske sikkerhetskomiteen innledet et arbeid med utarbeidelse av strategi for den nasjonale sikkerheten. Det er lagt opp til at strategien skal publiseres i juni 2025, jf. Statsrådet utarbetar en strategi för den nationella säkerheten – Inrikesministeriet.

[133] NCSA-FI er blant annet nasjonal godkjenningsmyndighet for kryptoprodukter og myndighet for distribution av kryptografiskt materiale. Det er også den nasjonale TEMPEST-myndigheten.

ling på frivillig basis. Traficom ivaretar også oppgaven som sertifiseringsmyndighet for IT-løsninger. Sektormyndigheter fører tilsyn i egen sektor i Finland.

Den finske regjeringen la i oktober 2024 frem en oppdatert strategi for cybersikkerhet for perioden 2024–2035.[134] En ny cybersikkerhetslov som blant annet gjennomfører NIS2-direktivet i finsk lov, ble sluttbehandlet i riksdagen 11. mars 2025.[135]

8.4 Nederland

Det forebyggende sikkerhetsarbeidet i Nederland er fordelt mellom flere institusjoner på ulike nivåer, og det er flere lover som regulerer de ulike områdene i arbeidet med nasjonal sikkerhet.

Funksjonen som *National Security Authority* (NSA) i forholdet til NATO ivaretas i Nederland av Innenriksdepartementet og Forsvarsdepartementet med støtte fra henholdsvis den sivile etterretningstjenesten (AIVD) og den militære etterretningstjenesten (MIVD).

Det er likevel én virksomhet som er en særlig sentral nasjonal koordinator for terrorbekjempelse og sikkerhet, *Nationaal Coördinator Terrorismebestrijding* (NCTV). NCTV er ansvarlig for å bekjempe terror, cybersikkerhet, nasjonal sikkerhet, krisehåndtering og statlige trusler. NCTV ligger under det nederlandske justis- og sikkerhetsdepartementet, *Ministerie van Justitie en Veiligheid*. Nederland har en nasjonal sikkerhetsstrategi fra 2023.[136]

NCTV arbeider sammen med andre myndigheter i sikkerhetssektoren, forskningsmiljøer og med privat sektor for å forhindre og minimere samfunnsforstyrrelser. Sentrale oppgaver for NCTV er å analysere og redusere trusler som er identifisert, tilby overvåking og beskytte personer, eiendom, tjenester og arrangementer. For viktige sektorer skal NCTV utvide og styrke cybersikkerheten og bidra til å gjøre eiendom, personer, infrastruktur og nettverk mer motstandsdyktig mot trusler. NCTV skal også bidra til effektiv krisehåndtering og krisekommunikasjon.

Departementene er ansvarlige for å vurdere motstandskraften til kritisk infrastruktur i egen sektor og fastsette rammeverk for sikkerhetsarbeidet. Justis- og sikkerhetsdepartementet skal koordinere departementene og regelmessig vurdere metodikken og om det er behov for nye tiltak. NCTV skal bidra til å klarlegge betydningen av ulike tiltak.[137]

Det nasjonale cybersikkerhetssenteret, *The National Cyber Security Centre* (NCSC), er ansvarlig for digital sikkerhet i Nederland. NCSC faller inn under myndigheten til NCTV og er det sentrale informasjonsknutepunktet for digital sikkerhet. NCSC overvåker internettet. Når senteret identifiserer en trussel, varsles offentlige myndig-

[134] Strategi för cybersäkerheten i Finland 2024–2035.

[135] Regeringens proposition till riksdagen med förslag till lagstiftning om genomförande av cybersäkerhetsdirektivet (NIS 2-direktivet). RP 57/2024 rd.

[136] https://www.government.nl/documents/publications/2023/04/03/security-strategy-for-the-kingdom-of-the-netherlands

[137] https://english.nctv.nl/documents/publications/2018/02/01/factsheet-critical-infrastructure.

heter og virksomheter. NCSC gir også råd om hvordan de kan beskytte seg mot trusler på nettet, følger utviklingen innen digital teknologi og oppdaterer sikkerhetssystemene. NCSC gir råd til offentligheten og virksomheter om hvordan nettkriminalitet kan motvirkes og har informasjonskampanjer for å belyse risikoene.

Lov om sikkerhet for nettverks- og informasjonssystemer (*Wet beveiliging netwerken informatiesystemen* (Wbni)) fra 2018 har som formål å styrke den digitale motstandsdyktigheten, begrense konsekvensene av cyberhendelser for samfunnet. Loven pålegger tilbydere av essensielle tjenester og digitale tjenesteytere å iverksette tiltak for å sikre sine IKT-systemer mot hendelser. For alvorlige hendelser er det meldeplikt.

I desember 2022 fikk NCSC hjemmel til å dele informasjon med andre organisasjoner, for eksempel informasjon om sårbarheter eller angrep. Såkalte organisasjoner for kritiske sektorer og oppgaver (*Organisaties voor Kritieke Takken en Taken* (OKTT-er)) kan dele trusselinformasjon fra NCSC med bedrifter eller organisasjoner i eget nettverk. Det nederlandske økonomidepartementet, *Ministerie van Economische Zaken*, etablerte i 2018 også et digitalt senter, *Digital Trust Center*, som advarer også bedrifter som ikke vurderes som kritiske om alvorlige trusler.

Algemene Inlichtingen- en Veiligheidsdienst (AIVD) er Nederlands sivile etterretningstjeneste og ligger under innenriksdepartementet, *Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*. AIVD undersøker organisasjoner og personer ved alvorlig mistanke om at de utgjør en fare for den demokratiske rettsordenen, statens sikkerhet eller andre viktige statlige interesser. AVID er videre ansvarlig for sikkerhets- og adgangsklarering av personell i sivil sektor. AVID skal også fremme sikkerhetstiltak, inkludert tiltak for å beskytte de delene av offentlig sektor og næringslivet som er av avgjørende betydning for opprettholdelsen av samfunnslivet. AVID utarbeider trussel- og risikoanalyser.

Det nasjonale byrået for beskyttelse av kommunikasjon, *Nationaal Bureau Verbindingsbeveiliging* (NBV), er en del av enheten for motstandsdyktighet i AVID. NBV veileder myndigheter om beskyttelse av kritisk informasjon. NBV utfører også oppgaver blant annet innen informasjonssystemsikkerhet og registrering og distribusjon av kryptografisk utstyr. Sertifiseringsordningen tilsvarende SERTIT i Norge, er i Nederland ivaretatt av det kommersielle sertifiseringsorganet TrustCB B.V.

Den militære motparten til AVID er *Militaire Inlichtingen- en Veiligheidsdienst* (MIVD) som er Nederlands militære etterretnings- og sikkerhetstjeneste. MIVD er en egen organisasjon under forsvarsdepartementet, *Ministerie van Defensie*. MIVD har blant annet ansvar for sikkerhets- og adgangsklarering av personell i forsvaret og leverandører til forsvaret. MVID har også som oppgave å iverksette tiltak for å beskytte forsvarets sikkerhet og beredskap, herunder sikkerheten til gradert militær informasjon. MIVD utarbeider trusselsanalyser av personer, saker og steder av militær betydning.

AIVD og MIVD arbeider tett sammen og har også slått seg sammen i en felles signaletterretning og Cyber-enhet (*Joint Sigint Cyber Unit* (JSCU)). JSCU avlytter kommunikasjon og støtter etterforskning av trusler mot Nederland og de væpnede

styrkene. I rammeverket til den nasjonale cybersikkerhetsstrategien skal JSCU-spesialister også beskytte internett.[138]

Oppgavene og fullmaktene til MIVD og AIVD er nedfelt i en felles lov om etterretning og sikkerhetstjenester, *Wet op de inlichtingen- en veiligheidsdiensten 2017* (Wiv 2017) og i lov om sikkerhetsundersøkelser, *Wet veiligheidsonderzoeken 2002*. I juli 2024 trådte en midlertidig lov om cyberoperasjoner i kraft. Bakgrunnen for den midlertidige loven var at Wiv 2017 ikke var tilstrekkelig i lys av den raske utviklingen i cyberverdenen og utfordringene med å spore trusler[139].

8.5 USA

Forebyggende sikkerhet i USA omfatter en rekke mekanismer som er utformet for å hindre trusler før de oppstår, beskytte nasjonens sikkerhet og stabilitet og sikre kritisk infrastruktur, offentlige tjenester og økonomien. USA har ikke én samlet sikkerhetslov, men en rekke nasjonale sikkerhetslover for forebyggende sikkerhet innen ulike samfunnsområder. Det er heller ikke én institusjon med et tilsvarende ansvar som vårt NSM.

National Security Council (NSC) spiller en sentral rolle i koordineringen av blant annet forebyggende sikkerhet i USA. NSC er en rådgivende enhet for presidenten og har som hovedmål å legge til rette for at USA er forberedt på å håndtere og forebygge nasjonale sikkerhetstrusler, både interne og eksterne. NSC skal koordinere sikkerhetsarbeidet mellom føderale etater og byråer.

Det amerikanske sikkerhetsdepartementet, *Department of Homeland Security* (DHS), er ansvarlig for nasjonal sikkerhet og samfunnssikkerhet. DHS ble opprettet i 2002 etter terrorangrepet 11. september 2001. Departementets oppdrag omfatter blant annet kontraterror og håndtering av trusler mot nasjonal sikkerhet, grensesikkerhet, cybersikkerhet og kritisk infrastruktur, økonomisk sikkerhet og beredskap og motstandsdyktighet i samfunnet. DHS gir retningslinjer og støtte til private selskaper for å forbedre deres sikkerhetstiltak og hindre angrep som kan ramme nasjonens kritiske infrastruktur. *Cybersecurity and Infrastructure Security Agency* (CISA) ligger under DHS og ble etablert i 2018 for å lede arbeidet med føderal cybersikkerhet og koordinerer det nasjonale arbeidet med sikkerhet rundt kritisk infrastruktur.

Det amerikanske justisdepartementet, *Department of Justice* (DoJ) er også sentralt for ivaretagelse av nasjonal sikkerhet. Under DOJ er bl.a. det føderale etterretningsbyrået *Federal Bureau of Investigation* (FBI). FBI har blant annet ansvaret for å beskytte USA fra terrorangrep, utenlandsk etterretning, spionasje og cyberoperasjoner og cyberkriminalitet. FBI har en rekke rettslige hjemler for å kunne etterforske føderale forbrytelser og trusler mot nasjonal sikkerhet. FBI kan også innhente etterretning og assistanse fra andre virksomheter.

[138] https://english.nctv.nl/topics/netherlands-cybersecurity-strategy-2022-2028.

[139] https://www.aivd.nl/onderwerpen/wet-op-de-inlichtingen-en-veiligheidsdiensten/tijdelijke-wet-onderzoeken-aivd-en-mivd-naar-landen-met-een-offensief-cyberprogramma.

Det amerikanske forsvarsdepartementet, *Department of Defense* (DoD) ivaretar oppgaven som *National Security Authority* (NSA) i forhold til NATO. Under DoD har *National Security Agency* (NSA) blant annet ansvar for signaletterretning og cybersikkerhet. Under betegnelsen *Central Security Service* (CSS) har NSA en utvidet rolle knyttet til kryptologi. NSA samarbeider med andre byråer som CISA og FBI for å forhindre cyberangrep og fiendtlige aktører i å infiltrere amerikanske systemer, og har et sentralt ansvar for hendelseshåndtering i forsvarssektoren. Ansvaret for personsikkerhet og bakgrunnssjekk i saker om klarering av personell er lagt til etaten *Defense Counterintelligence and Security Agency* (DCSA). DCSA sjekker bakgrunnen til personell for mer enn hundre byråer på føderalt nivå og i forsvaret. DCSA har også en viktig oppgave knyttet til sikkerhetsgraderte anskaffelser i forsvarssektoren. Videre er *Department of Defense Cyber Crime Center* (DC3) et føderalt cybersenter som blant annet har ansvar for å støtte cybersikkerheten til forsvarsindustrien. *United States Cyber Command* (USCYBERCOM) under DoD er blant annet ansvarlig for å forsvare militære nettverk og hindre cyberangrep mot USA. Sjef NSA har rollen som *Cyber Commander*.

Office of the Director of National Intelligence (ODNI) ble opprettet i 2004[140] og er et uavhengig kontor direkte underlagt presidenten. Hovedoppdraget til ODNI er å lede det amerikanske etterretningsfellesskapet (*Intelligence Community* (IC)) som inkluderer byråer som NSA, CIA, FBI med mål om å levere best mulig etterretning. *Central Intelligence Agency* (CIA), et uavhengig føderalt byrå, rapporterer direkte til presidenten gjennom ODNI. CIA samarbeider med andre etterretningsbyråer for å avdekke terrorplaner, spionasjeoperasjoner og andre trusler mot nasjonal sikkerhet.

ODNI har opprettet nasjonale sentre som koordinerer aktivitetene til hele IC og i noen tilfeller den amerikanske regjeringen innenfor IC's hovedoppdragsområder. Ett av disse sentrene er *National Counterterrorism Center* (NCTC) som leder den nasjonale innsatsen for å beskytte USA mot terrorisme, og *National Counterintelligence and Security Center* (NCSC) som støtter USAs regjering med kontraetterretning. NCSCs ansvar omfatter blant annet cybersikkerhet, fysisk sikkerhet og personellsikkerhet. Et annet senter er *Cyber Threat Intelligence Integration Center* (CTIIC) som skal styrke samarbeidet mellom relevante institusjoner for å beskytte USA mot cybertrusler. USAs nasjonale cybersikkerhetsstrategi *(National Cybersecurity Strategy)* ble oppdatert i mars 2023. Et tredje senter under ODNI som kan nevnes her er *The Foreign Malign Influence Center* (FMIC) som er USAs primære organisasjon for å integrere etterretning for bekjempelse av utenlandsk påvirkning. I tillegg huser FMIC *Election Threat Executive* (ETE) som skal bidra til valgsikkerhet.[141]

Information Security Oversight Office (ISOO) er underlagt USAs riksarkiv og ble etablert ved presidentordre i 1978. Kontoret skal påse at føderale myndigheter beskytter gradert informasjon og gir tilgang til informasjon når det legale grunn-

[140] ODNI ble etablert som et resultat av *9/11 Commission Report* (National Commission on Terrorist Attacks Upon the United States), som pekte på behovet for en mer koordinert tilnærming til nasjonal etterretning i USA etter terrorangrepene den 11. september 2001. Dette ledet til *Intelligence Reform and Terrorism Prevention Act of 2004* og opprettelsen av ODNI.

[141] *National Counterproliferation and Biosecurity Center* (NCBC) er et femte av ODNIs nasjonale sentre.

laget er til stede. Kontorets fokus er på å standardisere og vurdere prosessene knyttet til håndtering av gradert og «controlled unclassified information» gjennom tilsyn, utvikling av policy, veiledning, kompetanseheving og rapportering.

Ovenstående er ikke en uttømmende oversikt over de mange ulike samarbeids- og koordineringsmekanismene i arbeidet med forebyggende sikkerhet i USA.

8.6 Storbritannia

Ansvars- og oppgavefordelingen mellom statlige myndigheter for å ivareta forebyggende sikkerhet i Storbritannia er kompleks og involverer flere organer på tvers av ulike sektorer.

Den britiske regjeringen har det øverste politiske ansvaret for nasjonal sikkerhet. Som i Norge har de ulike departementene ansvaret for forebyggende sikkerhet innenfor sin sektor. Storbritannia har ingen sektorovergripende fagetat med et ansvar som vi har ved NSM. Tre av departementene har et særlig ansvar for forebyggende sikkerhet: Statsministerens kontor (*Cabinet Office)*, innenriksdepartementet (*Home Office)* og utenriksdepartementet (*Foreign, Commonwealth and Development Office)*. Men også andre, som forsvarsdepartementet (*Ministry of Defence*), ivaretar viktige funksjoner.

Cabinet Office koordinerer arbeidet med nasjonal sikkerhet, beredskap og krisehåndtering på tvers av ulike departementer og myndigheter, spesielt i krisetider. Cabinet Office ivaretar rollen som *National Security Authority* (NSA) i forhold til NATO. Cabinet Office har langt flere ansatte enn Statsministerens kontor i Norge og om lag 30 virksomheter og offentlige organer under seg.

National Security Council (NSC) ligger under Cabinet Office og har som hovedoppgave å koordinere den britiske regjeringens respons på nasjonale og internasjonale sikkerhetstrusler. Det inkluderer både å legge langsiktige planer og å lede arbeidet med å håndtere krisesituasjoner. NSC ledes av den nasjonale sikkerhetsrådgiveren *National Security Advisor (NSA)* og består ellers av sentrale medlemmer av regjeringen.

National Security Advisor (NSA) gir råd til statsministeren og andre ministre om nasjonal sikkerhet. NSA koordinerer arbeidet mellom de ulike departementene og etatene som er involvert i nasjonal sikkerhet. NSA bidrar også til at de britiske etterretningstjenestene og politimyndighetene deler informasjon og oppdaterte trusselvurderinger effektivt. Andre enheter som bidrar med å koordinere og rådgi regjeringen i etterretningsarbeidet, er *Joint Intelligence Committee* (JIC) og *Joint Intelligence Organisation* (JOC).

Government Security Group er underlagt Cabinet Office og utarbeider retningslinjer for forebyggende sikkerhet for offentlig forvaltning, det vil si departementene, etatene og partnere som håndterer myndighetsinformasjon. Arbeidet understøttes av informasjon fra *National Cyber Security Centre* (NCSC) og *National Protective Security Authority* (NPSA), som er underlagt henholdsvis etterretningsetatene Government Communications Headquarters og MI5.

Cabinet Office ivaretar også cybersikkerhet i offentlig sektor gjennom *Government Cyber Coordination Centre* (GCCC (GC3)). GC3 samordner og koordinerer cybersikkerhet på tvers av departementer og etater og er et fellesforetak mellom ovennevnte *Government Security Group* og NCSC samt *Central Digital and Data Office.*[142] GC3 bidrar til å koordinere responsen på cyberhendelser som kan påvirke både offentlig sektor og private aktører. I 2023 overtok Cabinet Office også ansvaret for å følge opp *The National Security and Investment Act 2021* (NSI Act)[143] fra departementet for næringsliv og handel (*Department for Business and Trade*).

Ytterligere et sentralt organ som bidrar til å ivareta forebyggende sikkerhet under Cabinet Office er *United Kingdom Security Vetting* (UKSV). UKVS sjekker bakgrunn og klarerer personer som skal ha tilgang til sensitiv informasjon eller som arbeider i sikkerhetsrelaterte stillinger på oppdrag fra den britiske regjeringen, herunder private kontraktører. Tidligere ble sikkerhetsvurderingene utført av forskjellige departementer og organisasjoner, men UKSV ble opprettet for å konsolidere denne prosessen på tvers av offentlig og privat sektor. UKSV ble etablert i 2017 og lå opprinnelig under MoD, men har siden 2020 vært i Cabinet Office hvor det er del av Government Security Group.

Cabinet Office har dermed ansvar for alle deler av prosessen med å klarere personell. Som EOS-tjenesten i Norge, foretar de britiske etterretningstjenestene sikkerhetsklarering og kontroll av eget personell, men i nær kontakt med UKSV.

Det britiske innenriksdepartementet *Home Office* er ansvarlig for politiet, immigrasjon og grensekontroll, kontraterrorisme og rikets sikkerhet. Den britiske sikkerhetstjenesten *Security Service*, kjent som *MI5*, er Storbritannias innenlandske etterretningstjeneste og underlagt Home Office. MI5 skal beskytte Storbritannia mot trusler som kan skade nasjonal sikkerhet, som terrorisme, spionasje og andre former for intern og ekstern destabilisering. I denne sammenhengen er forebyggende sikkerhet en viktig del av MI5s arbeid, spesielt å hindre at trusler materialiserer seg i alvorlige hendelser. *National Protective Security Authority* (NPSA) er del av MI5 og er Storbritannias nasjonale tekniske myndighet for fysisk sikkerhet og personellsikkerhet. NIPSA skal gjøre Storbritannia mindre sårbart og mer motstandsdyktig mot nasjonale sikkerhetstrusler. NPSA utvikler veiledninger innen forebyggende sikkerhet for britiske myndigheter og industri og skal gi råd til private og offentlige organisasjoner og virksomheter, som teknologiske oppstartsbedrifter, arrangementer og universiteter.

Flere viktige organer for forebyggende sikkerhet er dessuten underlagt *Foreign, Commonwealth & Development Office* (FCDO), det britiske utenriksdepartementet. MI6, eller *Secret Intelligence Service* (SIS), er Storbritannias utenlandsetterretningstjeneste og skal beskytte nasjonale interesser gjennom etterretning og operasjoner i utlandet.

[142] *Central Digital and Data Office* (CDDO) er del av *Department for Science, Innovation and Technology* som ble etablert i februar 2023.

[143] https://www.gov.uk/government/collections/national-security-and-investment-act

Government Communication Headquarters (GCHQ) er også underlagt FCDO og er Storbritannias etat for signaletterretning. GCHQ har også utviklingsoppgaver innen digital sikkerhet, herunder kryptoutvikling og distribusjon. *National Cyber Security Centre* (NCSC) er en underliggende avdeling i GCHQ. NCSC bistår som nevnt ovenfor med å beskytte kritiske tjenester mot cyberangrep, håndtere store hendelser og forbedre generell internettsikkerhet. NCSC gir blant annet råd til borgere og organisasjoner. NCSC er også sertifiseringsmyndighet med et ansvar tilsvarende SERTIT i NSM i Norge. Her ligger også den nasjonale responsfunksjonen. NCSC ble etablert i 2016 og anses som en av de første organisasjonene i verden som hadde et slikt spesialisert mandat for å beskytte et lands cybersikkerhet på et nasjonalt nivå og i et integrert samvirke med andre aktører. NCSC samarbeider som nevnt med Government Security Group med å koordinere cybersikkerhet via Government Cyber Coordination Centre (GC3). *National Authority for Counter Eavesdropping* (UK NACE), den britiske tjenesten for bekjempelse av avlytting, skal forhindre at fiendtlige aktører skal få tilgang til eller manipulere sensitiv informasjon og teknologi. Dette skjer bl.a. gjennom tekniske sikkerhetsundersøkelser.

Storbritannias forsvarsdepartement, *Ministry of Defence* (MOD), arbeider med forebyggende sikkerhet først og fremst rettet mot spesifikke områder i forsvarssektoren og for beskyttelse av nasjonens interesser. MOD er involvert i beskyttelse av kritisk infrastruktur, som inkluderer militære baser, forsvarsanlegg, kommunikasjonssystemer og andre vitale nasjonale sikkerhetselementer. MOD samarbeider med andre myndigheter og bidrar til å vurdere trusler og risikoer for landets sikkerhet i bredt. MOD bidrar blant annet til å lære opp sikkerhetspersonell og i Storbritannias nasjonale cyberforsvar. MOD har en sentral rolle innen sikkerhetsgraderte anskaffelser, og representerer dette fagfeltet i internasjonal sammenheng. Gjennom *Defence Cyber Operations* (DCO) bidrar MOD til å beskytte både militære og nasjonale cyberinfrastrukturer mot angrep og samarbeider i dette arbeidet med blant annet *National Cyber Security Centre* (NCSC).

The National Security Act 2023 er en av de nyeste lovene for å styrke nasjonal sikkerhet i Storbritannia og gi myndighetene flere verktøy for å håndtere nye trusler i en mer kompleks geopolitisk og teknologisk verden.

9 Trusselbildet[144]

9.1 Nasjonal sikkerhet: Nåsituasjon og fremtidig utvikling

Norge står overfor et komplekst trusselbilde som påvirker nasjonal sikkerhet, motstandsdyktighet i kritisk infrastruktur og samfunnets grunnleggende sikkerhet. Trussel- og risikovurderingene for 2025 fra EOS-tjenestene (Fokus 25, NTV 25 og Risiko 25), Langtidsplan for forsvarssektoren (Prop. 87 S (2023–2024), jf. Forsvarskommisjonens rapport (NOU 2023: 14)) og Totalberedskapsmeldingen (Meld. St. 9 (2024–2025), jf. Totalberedskapskommisjonens rapport (NOU 2023: 17)) er sentrale dokumenter som gir omfattende innsikt i både nåværende og fremtidige sikkerhetsutfordringer som vi står ovenfor. Den senere tids turbulente utvikling påvirker trusselbildet ytterligere. Disse vurderingene viser viktigheten av et robust forsvar, et effektivt beredskapssystem og robuste forebyggende sikkerhetstiltak som er tilpasset de ulike truslene mot nasjonens sikkerhet. Tjenestene trekker særlig frem i rapportene for 2025 økte utfordringer med sammensatte trusler og den teknologiske utviklingen som del av strategisk konkurranse mellom stormaktene.

9.2 Russlands destabiliserende kampanje

Russland er den viktigste og mest direkte trusselen mot norsk sikkerhet. Russland anser seg selv i direkte konflikt med Vesten. Dette vil vedvare uavhengig av utfallet av krigen i Ukraina, og bidrar til høy spenning i forholdet til Vesten også i og utover 2025.

Russlands brede virkemiddelbruk, som blant annet omfatter desinformasjon, cyberangrep, sabotasje og økonomiske pressmidler, utgjør en strategisk trussel mot statssikkerheten og norske interesser. Russland bruker også store ressurser på påvirkningsoperasjoner. I Norge inkluderer dette å fremme narrativer som undergraver tillit til institusjoner. Ifølge Etterretningstjenesten søker Russland å destabilisere vestlige demokratiske samfunn gjennom slike operasjoner. Sammensatte trusler benyttes som en strategi for å ramme nasjonale sikkerhetsinteresser gjennom å svekke allianse-samhold, internasjonal rett, norske institusjoner og undergrave tilliten til myndighetene, i tillegg til å svekke forsvarsvilje og operativ evne. Dette krever styrket beredskap og koordinerte mottiltak fra både forsvarssektoren og sivile institusjoner. Russlands fullskala-invasjon av Ukraina i 2022 viser evne og vilje til å bruke militær makt for å nå sine strategiske mål. Det må antas en

[144] Dette kapittelet er vurderinger som utvalget etter anmodning har fått fra Justis- og beredskapsdepartementet og Forsvarsdepartementet. Utvalget legger disse vurderingene av trusselbildet til grunn.

tilsvarende høy vilje til å benytte virkemiddel som ligger under terskelen for væpnet angrep. Etterretningstjenesten peker på at russiske trusselaktører i 2025 vil gjennomføre nettverksbaserte innhentingsoperasjoner mot norske beslutningsorganer, utenriksstasjoner, Forsvaret, kritisk infrastruktur, akademia og teknologibedrifter. Innhenting mot kritisk infrastruktur kan også ha som formål å klargjøre for fremtidig digital sabotasje. Videre vil utvisningen av russisk etterretningspersonell fra europeiske land medføre at Russland i økende grad utfører fordekte operasjoner i Europa via stedfortredere, såkalte proxyer. Slike stedfortredere utfører påvirkningsoperasjoner, politisk undergraving, sabotasje og informasjonsinnhenting på vegne av russiske statlige aktører. NSM påpeker også at Russlands aktiviteter inkluderer forsøk på å infiltrere norske virksomheter som har betydning for nasjonale sikkerhetsutfordringer, der enkelte særskilte sektorer som utenriks, forsvar, energi og ekom er særlig utsatt.

I følge Etterretningstjenesten er Russland blant landene som benytter en rekke metoder for å anskaffe og utnytte sivil, vestlig teknologi til militære formål. Kompliserte anskaffelsesnettverk tilslører sluttbrukeren for både leverandøren og statlige eksportkontrollmekanismer. Norskprodusert maritim teknologi og kommunikasjons- og navigasjonsteknologi, samt norsk forskning og utvikling innen halvleder- og sensorteknologi, materialteknologi, kryptologi, IKT-sikkerhet, bioteknologi og kunstig intelligens, er attraktive objekter for fordekte anskaffelser fra aktører underlagt sanksjoner og eksportkontrollregimer. Dette krever forbedret forebyggende sikkerhet i offentlige og private virksomheter på tvers av sektorer og forvaltningsnivå.

For å håndtere de omfattende utfordringene fra Russland, understreker langtidsplanen for forsvarssektoren viktigheten av å investere i moderne forsvarsteknologi, inkludert oppgraderte våpensystemer og styrket evne til militær mobilisering. Dette krever både nasjonale tiltak og tett samarbeid med NATO-allierte for å sikre en samlet og effektiv respons på den russiske trusselen. Det krever en robust sikkerhetstjeneste i forsvarssektoren og forebyggende sikkerhetstiltak i hele levetidsløpet til systemene.

9.3 Kinas økonomiske og teknologiske påvirkning

Kina representerer en økende sikkerhetsutfordring for Norge, særlig som etterretningstrussel, men også gjennom sin strategiske bruk av økonomisk makt og teknologisk innflytelse. Dette inkluderer investeringer i teknologi som kan brukes til overvåkning og kontroll, noe som øker risikoen for økonomisk og politisk avhengighet. Nasjonal sikkerhetsmyndighet påpeker at Kina investerer i kritisk infrastruktur og teknologi for å oppnå global innflytelse. NSM understreker at slike investeringer kan føre til strategisk avhengighet som kan påvirke Norges suverenitet og svekke nasjonal sikkerhet.

Kinas interesser i Arktis er særlig bekymringsfulle, ettersom regionen har stor geopolitisk og økonomisk betydning for både Norge og andre stormakter. Forsvarskommisjonen påpeker at Kinas samarbeid med Russland i Arktis kan utfordre vestlige interesser i regionen og skape økt spenning. Kina benytter også tekno-

logiske virkemidler for å samle inn etterretningsinformasjon og påvirke norske beslutningstagere, noe som ytterligere svekker Norges strategiske posisjon.

Etterretningstjenesten viser til at kinesiske etterretnings- og sikkerhetstjenester (KEST) driver fysiske og digitale operasjoner mot et bredt spekter av mål i Europa, herunder politiske beslutningstakere, sivilsamfunnsaktører, næringslivet og forsknings- og utviklingsinstitusjoner. Formålet med operasjonene er både tradisjonell etterretningsinnhenting av sensitiv informasjon, politisk påvirkning og industrispionasje. I tillegg til sitt eget etterretningspersonell, har KEST lovhjemmel og ressursgrunnlag til å utnytte alle kinesiske virksomheter og enkeltpersoner til etterretning, påvirkning og andre statlige formål.

I tillegg til økonomiske og teknologiske investeringer benytter Kina også kulturelle og akademiske forbindelser som virkemidler for å utøve påvirkning. Dette kan inkludere samarbeid mellom universiteter, forskningsinstitusjoner og kulturelle utvekslingsprogrammer som har som mål å fremme kinesiske interesser og samle inn informasjon. NSM understreker at slike initiativer kan svekke Norges akademiske uavhengighet og kompromittere forskningssikkerheten.

Kina har en langsiktig strategi for å sikre tilgang til kritiske mineralressurser, og dette skaper utfordringer for Norge når det gjelder å bevare sin suverenitet og kontroll over nasjonale ressurser.

9.4 Cybertrusler fra statlige aktører

Cybertrusler utgjør en vedvarende og betydelig risiko for Norge. Statlige aktører som Russland, Kina, Iran og Nord-Korea har gjennomført flere avanserte cyberoperasjoner rettet mot norske virksomheter og samfunnskritisk infrastruktur. Disse cyberangrepene har som mål å stjele informasjon, sabotere kritiske systemer og svekke Norges evne til å respondere på kriser. Nasjonal sikkerhetsmyndighet fremhever at slike angrep særlig retter seg mot viktige sektorer som energiforsyning, finans og offentlig administrasjon.

NSM understreker at Norge må styrke sitt cyberforsvar gjennom omfattende forebyggende sikkerhetstiltak. Dette inkluderer investeringer i teknologiske forsvarssystemer, forbedret overvåkning, og en økt evne til å oppdage og respondere på cyberangrep. Økt samarbeid mellom offentlige og private aktører er også nødvendig for å sikre en helhetlig tilnærming til cybersikkerhet. Det er også viktig at forebyggende cybersikkerhet inngår fra starten av ved utvikling av nye IT-systemer.

NSM påpeker også at Norge må forbedre sin evne til å håndtere cyberangrep gjennom styrking av det nasjonale cybersikkerhetssenteret og samarbeid med internasjonale partnere. Dette inkluderer bedre informasjonsutveksling og felles tiltak for å beskytte kritisk infrastruktur.

For å møte den økende trusselen fra cyberangrep må det også legges vekt på å utdanne og trene spesialister innen cybersikkerhet. NSM peker på at mangel på kompetanse innen dette feltet er en betydelig utfordring for Norge. Ved å investere

i opplæring og rekruttering kan Norge styrke sin kapasitet til å møte de fremtidige utfordringene i cyberspace.

Totalberedskapskommisjonen understreker også viktigheten av å øke bevisstheten om cybersikkerhet blant befolkningen. Det er nødvendig å iverksette informasjonskampanjer for å styrke befolkningens forståelse av digitale trusler og hvordan de kan beskytte seg selv og sine data. Økt samarbeid mellom offentlige myndigheter, privat sektor og akademia vil være avgjørende for å skape et robust cyberforsvar.

I en tid med økende cybertrusler er det viktig at ikke bare kommunikasjonsløsningene er robuste mot angrep, men også at vi evner å beskytte sensitiv og gradert informasjon som sendes mellom ulike lokasjoner. Sikker krypto sikrer at denne informasjonen ikke kan avlyttes eller manipuleres av uautoriserte parter, og det er avgjørende at vi evner å ivareta behovet for sikker krypto i fremtiden.

9.5 Sammensatte trusler og den teknologiske utviklingen

Tjenestene viser en økende bekymring for sammensatte trusler. Sammensatte trusler utfordrer nasjonal sikkerhet mer enn tidligere av flere grunner: *Kompleksitet*: Sammensatte trusler kombinerer ulike metoder som cyberangrep, desinformasjon og tradisjonell spionasje, og det er utfordrende å se dem i sammenheng, og få en helhetlig situasjonsforståelse over intensjonen til trusselaktøren og den overordnede strategiske trusselen. *Fordekt natur*: Disse truslene er ofte fordekte og kan operere under radaren til tradisjonelle sikkerhetstiltak, og vil kun oppdages dersom motstanderen gjør en feil. For eksempel kan desinformasjon spres gjennom sosiale medier uten å bli umiddelbart oppdaget. *Sivile mål:* Sammensatte trusler retter seg ofte mot sivile mål og kritisk infrastruktur, noe som kan skape kaos og undergrave tilliten til myndighetene. *Uklarhet:* sammensatte trusler rettes bevisst mot områder som er preget av gråsoner i roller, ansvar, myndighet, jus etc. nettopp for å skape utfordringer for situasjonsforståelse og forsinke beslutningsprosesser. *Rask utvikling*: Teknologisk utvikling gjør det enklere for trusselaktører å tilpasse og forbedre sine metoder, noe som krever kontinuerlig oppdatering av forsvarsmekanismer. Dette medfører at forsvareren alltid ligger et skritt bak.

Den teknologiske utviklingen utfordrer nasjonal sikkerhet av flere grunner. Utviklingen av avansert teknologi som kunstig intelligens, droner og kvantedatamaskiner kan brukes både til sivile og militære formål. Dette skaper nye muligheter, men også nye sårbarheter. I tillegg medfører økt digitalisering av samfunn og infrastruktur at flere viktige funksjoner blir avhengige av teknologi, noe som øker risikoen for cyberangrep. Moderne teknologi som 5G-nettverk og IoT-enheter kan ha sikkerhetshull som kan utnyttes av trusselaktører. Økt avhengighet av teknologi gjør derfor samfunnet mer sårbart for teknologiske feil og angrep, noe som kan føre til store forstyrrelser i og cyberangrep kan lamme kritisk infrastruktur som strømnett, vannforsyning og kommunikasjonssystemer. Dette kan ha alvorlige konsekvenser for nasjonal sikkerhet.

9.6 Desinformasjon og påvirkningsoperasjoner

Fremmede staters bruk av desinformasjon for å påvirke norsk offentlig debatt og svekke tilliten til myndighetene er en vedvarende trussel. Politiets sikkerhetstjeneste understreker at Russland og Kina aktivt driver desinformasjonskampanjer som tar sikte på å undergrave demokratiet og skape splittelse i det norske samfunnet, og samarbeidet mellom de to landene øker, også på dette området. NSM påpeker at desinformasjon ofte rettes mot politiske prosesser og valg, for å påvirke offentlige beslutninger. Den teknologiske utviklingen gjør det enklere å spre desinformasjon og påvirke opinionen, noe som kan destabilisere samfunn og undergrave tilliten til institusjoner.

Desinformasjon benyttes også til å skape mistillit mellom allierte land og forstyrre Norges utenrikspolitiske mål. Totalberedskapskommisjonen påpeker at det er viktig å utvikle en helhetlig nasjonal strategi som inkluderer både forebygging og respons på desinformasjon, slik at Norge bedre kan forsvare seg mot fremmede staters påvirkningsforsøk. Regjeringens kommende strategi for motstandskraft mot desinformasjon skal møte noen av disse utfordringene. Dette inkluderer å sikre tilgang til pålitelig informasjon for innbyggerne, samt styrking av samarbeidet mellom offentlige myndigheter og medieaktører for å motvirke spredning av falsk informasjon.

9.7 Kritisk infrastruktur som mål

Norges kritiske infrastruktur er sårbar for angrep fra fremmede stater. Ifølge NSM har både Russland og Kina vist stor interesse for å utnytte norske infrastrukturer, enten gjennom økonomisk kontroll eller direkte sabotasje. NSM understreker at beskyttelse av kritisk infrastruktur krever økt oppmerksomhet på både fysisk og digital sikring, inkludert styrket sikkerhet for nøkkelpersonell og forbedret overvåkning av strategiske anlegg.

Totalberedskapskommisjonen understreker at Norges rolle som stor energileverandør til Europa gjør denne infrastrukturen ekstra utsatt. Det er viktig å styrke redundans i kritisk infrastruktur, slik at samfunnets funksjoner kan opprettholdes selv ved angrep eller alvorlige hendelser. Dette innebærer blant annet utvikling av alternative forsyningslinjer og forbedret robusthet i energisystemer og transportnettverk.

Forsvarskommisjonen påpeker viktigheten av å sikre norsk infrastruktur mot trusler. Dette krever økt overvåkning og beskyttelse av samfunnskritiske funksjoner, samt en mer omfattende beredskap for å håndtere mulige sabotasjeangrep. I langtidsplanen for forsvarssektoren fremheves behovet for samarbeid mellom militære og sivile aktører for å sikre at infrastrukturen er godt beskyttet og at beredskapen kan tilpasses de skiftende truslene.

Totalberedskapskommisjonen fremhever også betydningen av å bygge opp beredskapslager og sikre redundante forsyningslinjer som en måte å redusere sårbarheten på. For å oppnå dette må Norge utvikle omfattende strategier som omfatter alle aspekter av kritisk infrastruktur, inkludert energiforsyning, transport og digitale nettverk. Beredskapstiltak bør inkludere kontinuerlig testing og evaluering for å sikre at alle systemer fungerer under press.

9.8 Innsiderisikoen og personellsikkerhet

Innsidere har ofte tilgang til sensitiv informasjon og systemer som er kritiske for nasjonal sikkerhet. Dette kan være tilgang til både sikkerhetsgradert og annen sensitiv informasjon, eller fysiske tilganger til objekt, infrastruktur eller informasjonssystemer. Trusselaktører kan utnytte menneskelige sårbarheter som økonomiske problemer, personlige konflikter eller ideologiske overbevisninger for å rekruttere innsidere. Dette gjør det mulig for dem å få tilgang til informasjon og ressurser som ellers ville vært utilgjengelige. Innsidere kjenner til interne systemer og rutiner, noe som gjør det lettere for dem å omgå både digitale og fysiske sikkerhetsbarrierer. Dette kan føre til alvorlige sikkerhetsbrudd. Innsidere kan være en nøkkelkomponent i cyberoperasjoner mot en virksomhet, spesielt når teknologiske sikkerhetstiltak blir mer avanserte. Økt geopolitisk spenning og økonomisk usikkerhet kan øke risikoen for innsidevirksomhet, da flere aktører kan være villige til å utnytte innsiderisiko for å oppnå sine mål. For å motvirke innsiderisiko er det viktig med hensiktsmessige sikkerhetstiltak, som sikkerhetsklarering, autorisasjon, og kontinuerlig sikkerhetsoppfølging av ansatte.

9.9 Oppsummering

Norge befinner seg i en farligere og mer uforutsigbar verden. Den alvorlige sikkerhetspolitiske situasjonen i Europa som følge av Russlands angrepskrig mot Ukraina, krigen i Midtøsten, og en tilspisset global konkurranse og rivalisering mellom stormakter som USA og Kina om militær, politisk, økonomisk og teknologisk makt, preger vår tid. Digitaliseringen av samfunnet, bruk av sosiale medier, og utviklingen av ny teknologi, som kunstig intelligens og droner, utfordrer sikkerhet og beredskap på måter vi ennå ikke fullt ut overskuer. Klimaendringene både øker risikoen for naturfare her hjemme, og kan forsterke migrasjon og konflikter globalt. I møte med denne samfunnsutviklingen må Norge styrke sin samlede forsvarsevne. I det forebyggende sikkerhetsarbeidet er det viktig at vi sikrer motstandsdyktige militære og sivile systemer og at det sivile samfunnet er forberedt på krise og krig, at evnen til å understøtte militær innsats videreutvikles og at samfunnet evner å motstå sammensatte trusler.

Norge står overfor en rekke komplekse og dynamiske trusler som utfordrer nasjonal sikkerhet og stabilitet. Det omfattende trusselbildet, beskrevet i vurderingene fra EOS-tjenestene, Forsvarskommisjonen og Totalberedskapskommisjonen, viser nødvendigheten av en helhetlig og koordinert innsats.

Sabotasje, desinformasjon, påvirkningsoperasjoner, instrumentalisert migrasjon fordekte investeringer i strategisk næringsvirksomhet, forstyrrelser i forsyningskjeder, innsidere i kommersielle eller offentlige virksomheter, samt hyppigere digitale angrep, er eksempler på virkemidler som trusselaktørene benytter seg av.

Det er avgjørende at Norge kontinuerlig tilpasser sin forsvars- og sikkerhetspolitikk for å kunne møte både dagens og morgendagens trusler.

10 Utvalgets vurderinger

I en usikker verden er behovet for å ha et godt og helhetlig rammeverk for forebyggende sikkerhetsarbeid blitt enda tydeligere. Norge står overfor komplekse trusler som utfordrer nasjonal sikkerhet. Det tradisjonelle skillet mellom statssikkerhet og samfunnssikkerhet er blitt mindre tydelig, se nærmere omtale i kapitlene 3 og 9. En koordinert innsats fra en rekke aktører er derfor nødvendig for å ivareta sikkerheten.

Flere offentlige utvalg har utredet ulike sider ved sikkerhet og beredskap de senere årene. Totalberedskapskommisjonen og Forsvarskommisjonen la fram rapporter så sent som i 2023. Stortinget vedtok i juni 2024 ny langtidsplan for forsvarssektoren for perioden 2025–2036. Den legger opp til en betydelig styrking av det norske forsvaret. Regjeringen la fram Totalberedskapsmeldingen tidligere i år.

Nasjonal sikkerhetsmyndighet (NSM) arbeider med forebyggende sikkerhet i Norge. Utvalget har som mandat å vurdere NSMs oppgaveportefølje og samspillet med andre myndigheter og virksomheter. For å få et best mulig grunnlag for våre vurderinger har vi hatt møter med en rekke aktører som arbeider med og har innsikt i arbeidet med forebyggende sikkerhet, se en oversikt i kapittel 2 og i vedlegg 3.

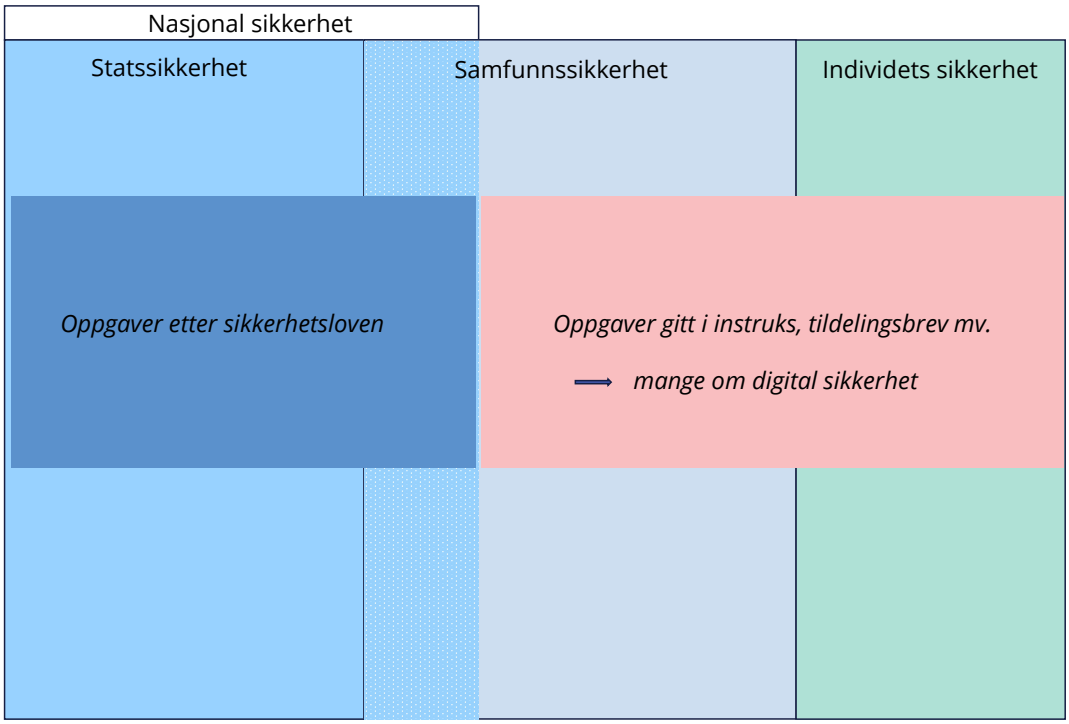
Et hovedinntrykk er at NSM fyller viktige funksjoner. Det er en organisasjon med dyktige medarbeidere innen flere ulike fagfelt. Men organisasjonen har også fått svekket ry etter svikt i den interne økonomiske styringen, kamp om utvidet revir, interne siloer med ulike budskap og lange saksbehandlingstider. Viktige oppgaver etter sikkerhetsloven er forsømt, samtidig som direktoratet er blitt pålagt stadig nye oppgaver utenfor loven. Det ryddes nå opp i styringen av økonomien, organisasjonen utvikles og det samarbeides bedre internt og eksternt.

Oppgaveporteføljen til NSM er uklart definert og har over tid blitt for bred. Særlig har oppgavene innen digital sikkerhet økt i omfang. En for bred portefølje av oppgaver kan svekke kvaliteten i det som blir gjort. Det er påvist svikt på flere områder i oppfølgingen av sikkerhetsloven. Omfanget av oppgaver bør derfor reduseres. NSM bør konsentrere seg om det som bør være direktoratets kjerneoppgave og være i stand til å løse den med høy kvalitet. Hva som er NSMs kjerneoppgave, er derfor viktig å avklare.

Utvalget mener her det må gjøres et veivalg mellom to alternativer. Direktoratet kan gå tilbake til sitt utgangspunkt, det vil si i det vesentlige å fylle funksjonen som sikkerhetsmyndighet etter sikkerhetsloven. Da bør en rekke oppgaver innen digital sikkerhet utenfor sikkerhetsloven, tas bort. Alternativet er å definere digital sikkerhet som NSMs kjerne, og la direktoratet få konsentrere seg om disse. Et tredje alternativ kunne være å øke ressursene til NSM i stedet for å redusere omfanget av oppgaver. Det ville imidlertid ikke løse problemet med at viktige oppgaver da

lett ville komme i oppmerksomhetsskyggen. Utvalget har ikke vurdert dette som et alternativ å gå videre med.

Figur 10.1 NSMs oppgaver og nasjonal sikkerhet, statssikkerhet og samfunnssikkerhet



Utvalget mener NSMs kjerne bør være konsentrert om nasjonal sikkerhet etter sikkerhetsloven. Trusselbildet Norge står overfor, underbygger denne vurderingen. Dette er også i tråd med utvalgets mandat om at den sikkerhetspolitiske utviklingen og utviklingen i risikobildet for nasjonal sikkerhet skal være førende for vurderingene. Nasjonal sikkerhet er en av grunnmurene for sikkerhetsarbeidet ellers i samfunnet.

Ettersom det ble opprettet et eget digitaliseringsdepartement i 2024, er det riktig at oppgaver for digital sikkerhet som tas ut av NSM, legges under dette departementet. Vi utdyper vårt syn i de følgende avsnittene.

Hva NSMs ansvar etter sikkerhetsloven er, bør gjøres klarere. For flere av oppgavene bør det dessuten vurderes nærmere hvor dypt NSM skal gå i utførelsen av dem. Det er rom for at flere oppgaver enn i dag kan settes ut til markedsaktører og til andre etater. Samarbeid og grensedragning mot andre myndigheter begynner å få en bedre form, men det er likevel behov for klarere retningslinjer enn i dag for samarbeidet mellom NSM og Direktoratet for samfunnssikkerhet og beredskap (DSB). NSM og politiet ved Kripos må ha et godt og hensiktsmessig samarbeid ved angrep på samfunnskritisk digital infrastruktur.

Utvalget viser også til at departementenes styring av NSM bør bedres. Hvor godt NSM utfører sine oppgaver, er avhengig av en god styring fra departementene.

10.1 Å ha én nasjonal sikkerhets-myndighet har verdi

Det kan skilles mellom *funksjonen* nasjonal sikkerhetsmyndighet og *direktoratet* Nasjonal sikkerhetsmyndighet, se omtale i kapittel 3. Funksjonen nasjonal sikkerhetsmyndighet følger blant annet av NATOs krav overfor medlemslandene om å ha en National Security Authority (NSA) som skal ivareta sikkerheten for NATO-gradert informasjon, se kapittel 3 og 7. Da Nasjonal sikkerhetsmyndighet (NSM) ble opprettet 1. januar 2003, ble oppgaven med å ivareta denne funksjonen lagt til det nye direktoratet. Også sikkerhetslovens forarbeider og forskrifter legger til grunn at rollen som sikkerhetsmyndighet skal legges til NSM.

Sikkerhetsmyndighetens oppgaver etter sikkerhetsloven kapittel 2 og 3 er særlig sentrale. Sikkerhetsmyndigheten skal legge til rette for og påse at skjermingsverdige verdier har forsvarlig sikkerhet. Oppgavene omfatter både fysisk og digital sikkerhet, personellsikkerhet og sikkerhetsstyring i både militær og sivil sektor, se kapittel 4. Det har verdi og er riktig å legge disse oppgavene til én myndighet slik det er gjort i Norge, framfor å splitte dem opp på flere. Én sikkerhetsmyndighet kan lettere se helheten i hva som kreves i arbeidet med forebyggende sikkerhet, særlig i en situasjon preget av sammensatte trusler, se nærmere omtale i kapittel 9.

Ved å være fag- og tilsynsmyndighet for alle sektorene får NSM oversikt og innsikt som bidrar til læring og utvikling på tvers av sektorene. Som fagmyndighet skal direktoratet utarbeide retningslinjer og standarder, veilede og gi råd. Som tilsynsmyndighet kan NSM formidle innsikt fra én sektor til andre sektorer.

Sikkerhetsarbeidet er mer fragmentert i andre land enn i Norge, jf. nærmere omtale i kapittel 8. Å ha én sikkerhetslov og én sikkerhetsmyndighet synes Norge å være alene om. Det er viktig å lære av andre land, men utvalget har ikke identifisert én organisering ute som kan sies å være en «beste-praksis». Modellen med én sikkerhetslov og én sikkerhetsmyndighet er en styrke og bør videreføres.

10.2 Nasjonal sikkerhetsmyndighets oppgaver etter sikkerhetsloven

Sikkerhetsloven § 2-2 «Sikkerhetsmyndighetens ansvar for forebyggende sikkerhetsarbeid» er en særlig sentral bestemmelse for NSMs oppgaver. § 2-2 første og andre ledd lyder:

«Sikkerhetsmyndigheten har det sektorovergripende ansvaret for at forebyggende sikkerhetsarbeid i virksomhetene utføres i samsvar med loven.

Sikkerhetsmyndigheten har det overordnede ansvaret for at sikkerhetstilstanden i alle sektorer kontrolleres, og skal se til at virksomhetene oppfyller sine plikter etter loven.»

Bestemmelsen gir NSM som sikkerhetsmyndighet et stort ansvar. Men bestemmelsen inneholder begreper som kan gi grunnlag for ulike tolkninger, det være seg både hva som ligger i et sektorovergripende ansvar og i et overordnet ansvar. Forarbeidene til loven klargjør, som vist til i kapittel 4, at sikkerhetsmyndighetens

ansvar etter sikkerhetsloven ikke griper inn i det enkelte departements ansvar. Men dette hjelper bare et stykke på vei. Hovedinstruksen for Nasjonal sikkerhetsmyndighet 3. mai 2019 bidrar heller ikke til klargjøring av lovens bestemmelser i § 2-2. Instruksen har en lang rekke skal-bestemmelser, men disse knyttes ikke til sektorovergripende ansvar eller hvordan det skal påses at det forebyggende ansvar i virksomheter som er underlagt sikkerhetsloven, utføres i samsvar med loven.

Det er ulike oppfatninger hos sentrale aktører utvalget har møtt, om det nærmere innholdet i nevnte bestemmelse. Særlig gjelder dette hvilket ansvar NSM har og hva som kan iverksettes med utgangspunkt i det sektorovergripende ansvaret og likeledes etter det overordnede ansvar.

Det er neppe behov for lovendringer for å bøte på at det i dag er en viss usikkerhet om innholdet i sentrale bestemmelser i sikkerhetsloven. Justis- og beredskapsdepartementet og Forsvarsdepartementet kan tydeliggjøre hvilket ansvar og hvilke oppgaver som følger av sikkerhetsloven § 2-2, og det må være tilstrekkelig.

Den grad av dobbeltbehandling og sammenfall av instrukser som utvalget peker på hos enkelte offentlige aktører, kan ha sammenheng med den uklarhet som er nevnt her, se omtale av tilgrensende myndigheter i kapittel 6.

Begreper som brukes, bør gi en presis beskrivelse av NSMs oppdrag. Ord som «overordnet», «sektorovergripende ansvar» og «nasjonal responsfunksjon» er omtrentlige og lite presise. Ordet «overordnet» kan gi assosiasjoner i retning av «sjef» og «å lede», men også i retning av «ikke å gå i dybden» av en sak. I stedet for et «sektorovergripende ansvar» er det etter vårt syn en bedre beskrivelse å si at NSM har *oppgaver* som omfatter flere sektorer. Det gjenspeiler at nasjonal sikkerhet avhenger av flere aktører. Hva oppgavene skal gå ut på, må beskrives nærmere. Som omtalt i kapittel 4 ligger *ansvaret* for sikkerheten hos de enkelte departementene og virksomhetene som er underlagt sikkerhetsloven, og NSM skal ikke «gripe inn» direkte i virksomheten. Direktoratet skal bistå de ansvarlige blant annet ved å gi råd, veilede, og føre tilsyn. På enkelte områder beslutter NSM om krav i henhold til loven er oppfylt.

10.3 Personellsikkerhet

I utvalgets mandat vises det til at «det pågår en prosess for overføring av ansvar for klareringssaker i sivil sektor herunder fagmyndighetsoppgaver, fra NSM til Sivil klareringsmyndighet. Denne prosessen skal fortsette uavhengig av dette arbeidet.» Utvalget har derfor ikke gått dypt inn i alle sider av disse problemstillingene.

Når NSM er fag- og tilsynsmyndighet på alle fagområder under sikkerhetsloven, omfattes som nevnt også personellsikkerhet, jf. avsnitt 10.1. En bør unngå å splitte opp utøvelsen av funksjonen som nasjonal sikkerhetsmyndighet på flere myndigheter. NSM bør derfor fortsatt være fagmyndighet for personellsikkerhet.

Som fagmyndighet gir NSM veiledning om regelverket og informasjon om risiko blant annet til klareringsmyndighetene, se omtale i kapittel 4. Det kan bidra til at klareringene følger de samme kriteriene på tvers av sektorer og virksomheter.

NSM bidrar også til å opplyse for å redusere innsiderisiko og motvirke at personell som er sikkerhetsklarert påvirkes av desinformasjon, jf. kapittel 9.6 og 9.8. Slik bør systemet være også fremover. Innenfor disse rammene bør myndighetene som klarerer i første instans, kunne fastsette retningslinjer for hvordan arbeidet skal skje og de enkelte sakene vurderes. Det er disse myndighetene som er nærmest til å legge til rette for en effektiv saksbehandling.

NSM er også klageinstans i klareringssaker. Utvalget ser fordeler ved at denne ordningen videreføres. NSM kan som fagmyndighet lære av å behandle klagesaker. Utfallet av saker vil i seg selv kunne skape presedens for senere klareringssaker og slik ha betydning for NSMs senere veiledning som fagmyndighet.

Behandling av klagesaker har tatt for lang tid i NSM. Det er uheldig og må unngås. Både klarering i første instans og klagesaker bør utføres uten unødig tidsbruk. NSM må her arbeide mer effektivt og gi oppgaven tilstrekkelig prioritet. En større grad av automatisering i arbeidet med innhenting og formidling av personkontrollinformasjon bør prioriteres. Behandlingstiden til NSM er etter det utvalget forstår, nå nede på kravet fra Justis- og beredskapsdepartementet om at minst 85 prosent av sakene skal behandles innen 90–120 dager. Også det er for lenge å vente for de som berøres, og målet bør skjerpes. EOS-utvalgets årsmelding for 2024 ble avgitt til Stortinget 26. mars 2025. Kontrollutvalget har her foreslått at den vedvarende lange saksbehandlingstiden i klareringssaker bør være en sak som behandles av Stortinget, jf. EOS-kontrolloven § 17 fjerde ledd nr. 7.

10.4 Eierskapskontroll

Investeringskontrollutvalget anbefalte i NOU 2023: 28 å legge saker om eierskapskontroll til Direktoratet for eksportkontroll og sanksjoner (DEKSA) som ble etablert 1. januar 2025. Investeringskontrollutvalget skrev blant annet:

> «Utvalget mener det er flere hensyn som taler for at en ny ordning for investeringskontroll legges til en egen, ny myndighet, og at det er relevant å vurdere om denne bør organiseres sammen med den nye etaten for eksportkontroll og sanksjoner.»[145]

Investeringskontrollutvalget anbefalte også at reglene om eierskapskontroll i sikkerhetsloven tilpasses og innarbeides i ny lov om investeringskontroll. Det vil ifølge utvalget bidra til at alle meldinger om investeringskontroll behandles etter det samme regelverket.

Sikkerhetsloven har i dag bestemmelser som regulerer eierskapskontroll av virksomheter underlagt loven. NSMs oppgaver på dette området følger dels av sikkerhetsloven og dels av oppdrag fra Justis- og beredskapsdepartementet.

Sikkerhetsloven §§ 10-1 – 10-3 omhandler eierskapskontroll i virksomheter som er underlagt denne loven. Departementene eller sikkerhetsmyndigheten skal varsles om erverv av en kvalifisert eierandel av slike virksomheter og kan godkjenne

[145] NOU 2023: 28 Investeringskontroll, side 134.

erverv. Dersom et erverv kan medføre en ikke ubetydelig risiko for at nasjonale sikkerhetsinteresser blir truet, kan Kongen i statsråd fatte vedtak om at ervervet ikke kan gjennomføres eller at det stilles vilkår for gjennomføringen. Sikkerhetsloven § 2-5 åpner for at Kongen i statsråd på samme måte kan stanse erverv av virksomheter som ikke er underlagt sikkerhetsloven. Dette er en sikkerhetsventil som kun skal benyttes der det ikke finnes annet grunnlag for å gripe inn.

Stortinget har vedtatt endringer i sikkerhetsloven kapittel 10 som ennå ikke er trådt i kraft. Endringene medfører at også avhender av en virksomhet pålegges en meldeplikt på lik linje med erverver.[146] Dette vil bidra til en enklere og mer effektiv håndhevelse av lovens bestemmelser om eierskapskontroll. I tillegg senkes terskelen for når det skal sendes melding, og flere vil omfattes av bestemmelsene. Det vil være leverandører med leverandørklarering og virksomheter som har vesentlig betydning for grunnleggende nasjonale funksjoner eller nasjonale sikkerhetsinteresser. Disse endringene vil også svare på Investeringskontrollutvalget merknad om at gjeldende § 10-1 i sikkerhetsloven ikke fanger opp alle eierskapssaker fordi bestemmelsen bare pålegger meldeplikt på erverver og ikke på avhender.[147]

NSM ble i 2021 utpekt som nasjonalt kontaktpunkt for varsler «om sikkerhetstruende økonomisk virksomhet». Dette ble gitt som oppdrag i eget brev fra Justis- og beredskapsdepartementet. Som kontaktpunkt bistår NSM departementene med risikovurderinger og innhenter råd fra andre, relevante etater. NSM gir også råd og veiledning til virksomheter som skal gjennomføre eller har gjennomført en sikkerhetsgradert anskaffelse der det er grunner for å undersøke nærmere hvorvidt det er innslag av sikkerhetstruende utenlandske interesser i verdikjeden.

Investeringskontrollutvalgets anbefalinger er under behandling i Nærings- og fiskeridepartementet. Investeringskontrollutvalget peker på hensyn som det er grunn til å vurdere. Det er blant annet gode grunner for at DEKSA som skal utøve eksportkontroll, også vil tilegne seg innsikt som er relevant for saker om eierskapskontroll. Generelt er det også en fordel å samle regelverk som henger nært sammen i samme lov, slik Investeringskontrollutvalget foreslår.

Saker om eierskapskontroll er likevel et fagområde som ikke er løsrevet fra andre fagområder i sikkerhetsloven. Loven understreker at erverv og andre uønskede aktiviteter skal vurderes opp mot betydningen dette vil ha for nasjonale sikkerhetsinteresser. Loven styrkes nå for lettere å fange opp saker som bør kontrolleres. Utvalget har ovenfor pekt på at det er en fordel å ha én sikkerhetslov og én sikkerhetsmyndighet. Det tilsier at lovens bestemmelser om kontroll av eierskap som gjelder virksomheter underlagt sikkerhetsloven, bør videreføres.

I behandlingen av slike saker hvor etater under flere departement medvirker og næringer og bedrifter blir berørt, er det viktig at det er bevissthet om hvilke statsråder som har parlamentarisk ansvar.

[146] Lovvedtak 116 (2022–2023): https://www.stortinget.no/no/Saker-og-publikasjoner/Vedtak/Beslutninger/Lovvedtak/2022-2023/vedtak-202223-116/?all=true

[147] NOU 2023: 28 *Investeringskontroll,* side 92.

10.5 Digital sikkerhet

10.5.1 Oppgaver for digital sikkerhet med utgangspunkt i sikkerhetsloven

Digital sikkerhet eller IKT-sikkerhet er ikke nevnt som begreper i sikkerhetsloven. NSM har likevel flere oppgaver innen digital sikkerhet og IKT-sikkerhet som kan avledes fra sikkerhetsloven. I den videre omtalen benyttes digital sikkerhet og IKT-sikkerhet som synonymer, se også boks 3.2.

NSM har siden kort etter at direktoratet ble opprettet, hatt oppgavene med å drifte og utvikle «Varslingssystem for digital infrastruktur (VDI)» og å være «nasjonal responsfunksjon» for digital sikkerhet, se nærmere omtale i kapittel 4. I 2017 ble den nasjonale responsfunksjonen og VDI tatt inn i sikkerhetsloven som en oppgave for sikkerhetsmyndigheten. I henhold til § 2-4 i loven skal Kongen utpeke en myndighet som skal utføre disse oppgavene. NSM er pekt ut i forskrift.[148]

Etter sikkerhetsloven § 2-3 skal NSM bidra til at det informeres om trusselvurderinger og andre opplysninger som er av betydning for det forebyggende sikkerhetsarbeidet i virksomheten og at det etableres nødvendige fora for informasjons- og erfaringsutveksling. NSM har her bygget opp et nokså omfattende apparat.

NSM bidrar med møteplasser der myndigheter og virksomheter kan utveksle informasjon og kunnskap i arbeidet med digital sikkerhet. I 2019 ble Nasjonalt cybersikkerhetssenter (NCSC) opprettet som et partnerskap mellom NSM og en rekke offentlige myndigheter og private virksomheter. Aktører som utvalget har snakket med, framhever NCSC som en nyttig arena for samhandling og informasjonsutveksling. NCSC drifter og utvikler VDI og den nasjonale responsfunksjonen. NCSC har deltakere og drøfter temaer som strekker seg ut over sikkerhetslovens rammer. Det er likevel viktig at senteret ikke går for langt ut over sikkerhetslovens virkeområde, se også avsnitt 10.5.2 nedenfor.

NSM mottar varsler og kan varsle på tvers av sektorer og virksomheter. Dette er en viktig funksjon som NSM ivaretar. Direktoratet informerer regjeringen og allmenheten. Ugradert informasjon er enklere å spre raskt enn gradert informasjon. Det er viktig at det sørges for en godt utbygget infrastruktur også for å kunne spre gradert informasjon.

Det er viktig at virksomheter har et realistisk bilde av hvordan de kan ivareta sikkerheten og håndtere hendelser som kan oppstå og også av hvilken assistanse NSM kan gi. Det er også viktig at NSM har et realistisk syn på egen evne til å gjenopprette systemer etter angrep og påser at virksomhetene har tilstrekkelig egen kapasitet eller avtale med spesialiserte selskaper. Virksomheter som rammes av digitale angrep, er som regel i det vesentlige avhengige av egne ressurser og hjelp fra private tjenesteleverandører for å gjenopprette ordinær drift. NSMs rolle i dag er beskrevet i «Rammeverk for håndtering av IKT-sikkerhetshendelser» fastsatt av Justis- og beredskapsdepartementet, se boks 4.1. I boks 4.2 er håndteringen av et alvorlig digitalt angrep mot Departementenes sikkerhets- og serviceorganisasjon (DSS) i 2023 beskrevet. NSM samarbeidet da med både DSS og det private selskapet mnemonic.

[148] Forskrift om virksomheters arbeid med forebyggende sikkerhet § 63.

Det er også etablert andre arenaer, som Felles cyberkoordineringssenter (FCKS), for å håndtere alvorlige digitale hendelser, se avsnitt 10.9. Utvalget har ikke merknader til dette.

Oppgaven med å godkjenne skjermingsverdige informasjonssystemer og å gjennomføre tekniske sikkerhetsundersøkelser (TSU) er også oppgaver etter sikkerhetsloven som faller inn under blant annet faget digital sikkerhet, se nærmere omtale i avsnitt 10.6.

10.5.2 Oppgaver for digital sikkerhet utenfor sikkerhetsloven

NSM er over tid også blitt pålagt mange oppgaver innen digital sikkerhet ut over de som følger av sikkerhetsloven. Det kan ses på som naturlig i lys av den økte digitaliseringen av samfunnet og nye sårbarheter som har vokst fram. Skillet mellom statssikkerhet og samfunnssikkerhet er blitt mindre tydelig, jf. nærmere omtale i kapittel 3. Dette gjelder kanskje særlig for digital sikkerhet og avhengigheter mellom virksomheter som er innenfor og utenfor sikkerhetsloven. Utviklingen på området skjer raskt. Det er likevel ikke slik at all aktivitet på dette området har betydning for nasjonal sikkerhet og at det ikke kan trekkes noen grenser. Dersom utviklingen tilsier at mer i samfunnet har betydning for den nasjonale sikkerheten, kan lovens anvendelse utvides blant annet ved at det utpekes nye grunnleggende nasjonale funksjoner (GNF), skjermingsverdige verdier og virksomheter som skal underlegges sikkerhetsloven, se omtale i kapittel 4.

Justis- og beredskapsdepartementet og Forsvarsdepartementet har i hovedinstruksen beskrevet NSM som «det nasjonale fagmiljøet for digital sikkerhet». NSM skal i denne funksjonen støtte og bidra til Justis- og beredskapsdepartementets og Forsvarsdepartementets ansvar innenfor digital sikkerhet, koordinere og legge til rette for samhandling mellom ulike myndigheter, foreslå tiltak, gi anbefalinger og fremme forslag til krav. Direktoratet skal følge opp med råd og veiledning. Justis- og beredskapsdepartementet har siden 2013 hatt ansvaret for å samordne arbeidet med samfunnssikkerhet og arbeidet med digital sikkerhet i sivil sektor.

NSMs rolle bør her klargjøres slik at forventningene til hva de gjør og ikke gjør, er realistiske. Å betegne NSM som «det nasjonale fagmiljøet» i hovedinstruksen bidrar til å overvurdere hvilken rolle direktoratet kan spille. Det er mange fagmiljøer med betydelig kompetanse innen dette området i landet, både i akademia, i forskningsinstitusjoner, offentlige etater og i private virksomheter. NSM støtter seg på disse og bidrar som ett av dem. Det bør komme klarere fram i instruksen. Instruksen slik den er formulert i dag, kan også bidra til at det er for lett å legge nye oppgaver på dette området til NSM og motvirke at det blir utviklet mer egnede alternativer.

NSMs oppgaveportefølje innen digital sikkerhet fremstår alt i alt som for omfattende. Det er en risiko for at en stadig økende oppgaveportefølje kan gå ut over NSMs kapasitet til å følge opp de oppgavene som er i eller nær kjernen, og som er særlig viktige for den nasjonale sikkerheten. Utvalget tilrår på denne bakgrunn at oppgaver som ikke har betydning for nasjonal sikkerhet, bør overføres til andre enn NSM. Utvalget understreker at dette er viktige oppgaver for sikkerheten i samfunnet, for virksomheter og for individer og som derfor må løses, men av andre enn NSM.

NSM skal i henhold til hovedinstruksen «... *vedlikeholde et særskilt risikobilde for digital sikkerhet som omfatter statssikkerhet, samfunnssikkerhet og individsikkerhet* ...» Denne oppgaven angir eksplisitt at NSM skal vurdere og følge opp risiko helt ned til digital sikkerhet for enkeltindivider. Denne oppgaven går for langt. NSM bør vurdere og rapportere om risikobildet for digital sikkerhet, men i hovedsak avgrenset til forhold av betydning for den nasjonale sikkerheten. Å «vedlikeholde et risikobilde» kan for øvrig språklig gi feil assosiasjoner. NSM skal ikke nødvendigvis holde ved like et risikobilde som allerede foreligger, men vurdere om det er endringer i risikobildet fremover.

Instruksen sier videre at NSM «... *skal foreslå tiltak, gi anbefalinger og fremme forslag til krav innen digital sikkerhet i samfunnet, samt følge opp med råd og veiledning*». Direktoratet er pålagt en rekke oppgaver om å gi informasjon, råd og veiledning til statlig og kommunal sektor, private virksomheter og enkeltpersoner. Dette er oppgaver utenfor sikkerhetslovens virkeområde som bør overføres til andre. NSM bør fortsatt bidra, men ikke lede dette arbeidet. Det gjelder blant annet:

– Drift av Norsk senter for informasjonssikring (NorSIS).
– Rådgiving til kommunesektoren som NSM overtok fra det tidligere KommuneCERT. Resten av oppgavene i KommuneCERT ble overført til sektorresponsmiljøet Kommune- og HelseCERT.
– NSMs oppgave med å vedlikeholde grunnprinsipper for IKT-sikkerhet og følge opp med råd og veiledning om disse. NSM bør fortsatt gi råd og veilede om krav som følger av sikkerhetsloven.
– Utvikle og drifte myndighetsportal og støtteverktøy.

Som vist til i avsnitt 10.5.1 ovenfor, bidrar NSM til å koordinere arbeidet med forebyggende sikkerhet i ulike fora for å opprettholde en forsvarlig sikkerhet innenfor sikkerhetslovens rammer, som blant annet Nasjonalt cybersikkerhetssenter (NCSC) og Felles cyberkoordineringssenter (FCKS). Begge disse er nært knyttet til oppgaven å drive en nasjonal responsfunksjon etter sikkerhetsloven. Disse bør NSM beholde. NSM bør også beholde oppgaven med å drifte Nasjonalt senter for anvendt kryptologi da dette er nært knyttet til oppgavene etter sikkerhetsloven.

NSM bør derimot ikke ha et hovedansvar for å koordinere aktiviteter som faller utenfor sikkerhetsloven slik det følger av dagens instruks. Det gjelder også for enkelte aktiviteter innen rammen av NCSC, som å utvikle informasjonsprodukter, gi råd og drive partnernettverk. Direktoratet kan også her bidra og trekkes inn som partner, men ikke ha et hovedansvar.

NSM leder i dag det såkalte SIG (Special Interest Group) IKT-tilsyn. NSM kan delta i kraft av å være tilsynsmyndighet for sikkerhetsloven, men ikke lede gruppen. Heller ikke oppgaven å drive Nasjonalt koordineringssenter for forskning og innovasjon innen cybersikkerhet (NCC-NO) i samarbeid med Norges forskningsråd er en riktig oppgave for NSM.

Utvalget forstår det slik at NSM er tiltenkt ytterligere oppgaver innenfor digital sikkerhet når digitalsikkerhetsloven og lov om grunnsikring i samfunnet innføres, se nærmere omtale i kapittel 4. NSM skal etter høringsforslaget til digitalsikkerhetssforskriften være «nasjonalt kontaktpunkt for sikkerhet i nettverk og informa-

sjonssystemer» og «tilsynsmyndighet i sektorer uten egen tilsynsmyndighet». Dette er ikke nødvendigvis oppgaver som faller innenfor nasjonal sikkerhet, og de bør derfor vurderes gitt til andre. Oppgaven med å drifte en nasjonal responsfunksjon etter digitalsikkerhetsloven sammenfaller derimot i stor grad med tilsvarende oppgave etter sikkerhetsloven og bør derfor samordnes med denne og ligge i NSM.

På tilsvarende måte, når hovedinstruksen sier at «NSM skal bidra til å styrke samfunnets kunnskap, forståelse, motivasjon og evne til å ivareta forebyggende sikkerhet, herunder digital sikkerhet på en best mulig måte» bør rollen avgrenses til det som omhandler nasjonal sikkerhet etter sikkerhetsloven.

Ifølge hovedinstruksen skal NSM «... utøve sertifiseringsmyndighet for IT-sikkerhet i produkter og systemer (SERTIT).» Dette er en frivillig ordning for sertifisering av IT-sikkerhet i produkter og systemer (SERTIT) som andre enn NSM bør ha som oppgave.

Tilsvarende foreslås det at oppgaven med å drifte deteksjonssystemet for falske basestasjoner tas ut av NSMs oppgaveportefølje og overføres til andre.

10.5.3 Plassering av oppgaver som bør tas ut av Nasjonal sikkerhetsmyndighet

Justis- og beredskapsdepartementet tildelte NSM rollen som det nasjonale fagmiljøet for digital sikkerhet etter at departementet i 2013 fikk ansvaret for å samordne IKT-sikkerhet på sivil side, jf. kgl.res. 22. mars 2013.[149] Direktoratet fikk samtidig tildelt økte midler til dette oppdraget. Både Justis- og beredskapsdepartementet og NSM fikk dermed et ansvar for digital sikkerhet som gikk utenfor sikkerhetsloven. Bakgrunnen for at Justis- og beredskapsdepartementet fikk dette samordningsansvaret var et ønske om å se IKT-sikkerhet i sammenheng med arbeidet med samfunnssikkerhet. Men flyttingen innebar samtidig at ansvaret for IKT-politikk og IKT-sikkerhet ble splittet mellom ulike departement.

I den kongelige resolusjonen som ga Justis- og beredskapsdepartementet ansvaret for å samordne IKT-sikkerhet på sivil side, ble det vist til at den raske teknologiutviklingen og den stadig større betydningen av IKT-sikkerhet i samfunnet «tilsier at ansvarsforholdene bør gjennomgås jevnlig for å vurdere behov for justeringer eller presiseringer». Den teknologiske utviklingen har vært formidabel siden 2013, og digital sikkerhet er blitt enda viktigere. Utvalget mener på denne bakgrunn at tiden nå er inne for å vurdere ansvarsdelingen som vist til i den kongelige resolusjonen.

Behovet for å gå gjennom ansvarsdelingen for digital sikkerhet nå støttes av at det nylig er blitt opprettet et eget digitaliseringsdepartement. Digitaliserings- og forvaltningsdepartementet ble opprettet 1. januar 2024.[150] Det nye departementet fikk blant annet ansvar for å «bidra til å styrke statens og samfunnets evne til å utnytte potensialet og håndtere utfordringene som digital teknologi skaper. Departe-

[149] Kgl.res. 22. mars 2013 om overføring av samordningsansvaret for forebyggende IKT-sikkerhet fra Fornyings-, administrasjons og kirkedepartementet til Justis- og beredskapsdepartementet.

[150] Kgl.res. 16. oktober 2023 og kgl.res. 20. desember 2023 om endringer i departementsstrukturen og ansvarsdelingen mellom departementene.

mentet vil ha både et pådriveransvar og en samordningsrolle i dette arbeidet.» Departementet fikk ansvaret for regjeringens digitaliseringspolitikk, elektronisk kommunikasjon og personvernpolitikken. Departementet har også ansvar for å gjennomføre EUs forordning om kunstig intelligens og å samordne regjeringens politikk innen kunstig intelligens.[151] Digitaliserings- og forvaltningsministeren representerte den norske regjeringen på møtet *AI Action Summit* i februar 2025 i Paris mellom statsledere, organisasjoner og næringsliv om hvordan verden kan ta i bruk kunstig intelligens på en forsvarlig og sikker måte. Videre samordner departementet offentlig sektors arbeid med informasjonssikkerhet og regjeringens digitaliseringspolitikk overfor EU.

Digitaliserings- og forvaltningsdepartementet har dermed oppgaver som i vesentlig grad griper inn i området for digital sikkerhet. Det vil etter utvalgets mening være riktig at departementet i forlengelsen av opprettelsen også får et ansvar for å samordne arbeidet med digital sikkerhet utenfor sikkerhetsloven. Oppgaver innen digital sikkerhet utenfor sikkerhetsloven som foreslås tatt ut av NSMs oppgaveportefølje, bør da legges til en eller flere etater under Digitaliserings- og forvaltningsdepartementet.

Flere aktører utvalget har snakket med, peker på at det er knapphet på kompetanse innenfor det digitale sikkerhetsarbeidet i Norge. Det er også økende konkurranse om ressursene. Det er derfor viktig å se på hvordan myndighetene organiserer arbeidet med digital sikkerhet for å nytte de samlede ressursene best mulig. Også Riksrevisjonen har pekt på at myndighetenes samordning av arbeidet med digital sikkerhet er svak.[152] Råd og veiledning innenfor digital sikkerhet framstår som fragmentert, noe som gjør det forebyggende sikkerhetsarbeidet krevende for mange virksomheter.

Utvalgets forslag innebærer at arbeid med digital sikkerhet innenfor og utenfor sikkerhetsloven deles opp. Utvalgets forslag innebærer imidlertid ikke at NSM ikke skal bidra i arbeidet med digital sikkerhet utenfor sikkerhetsloven. Direktoratets kunnskap bør fortsatt nyttes bredt i samfunnet. Utvalgets poeng er at NSM ikke bør ha en ledende rolle for å løse oppgavene som er nevnt i avsnitt 10.5.2.

[151] Europaparlamentets- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelsen av et harmonisert regelverk om kunstig intelligens.

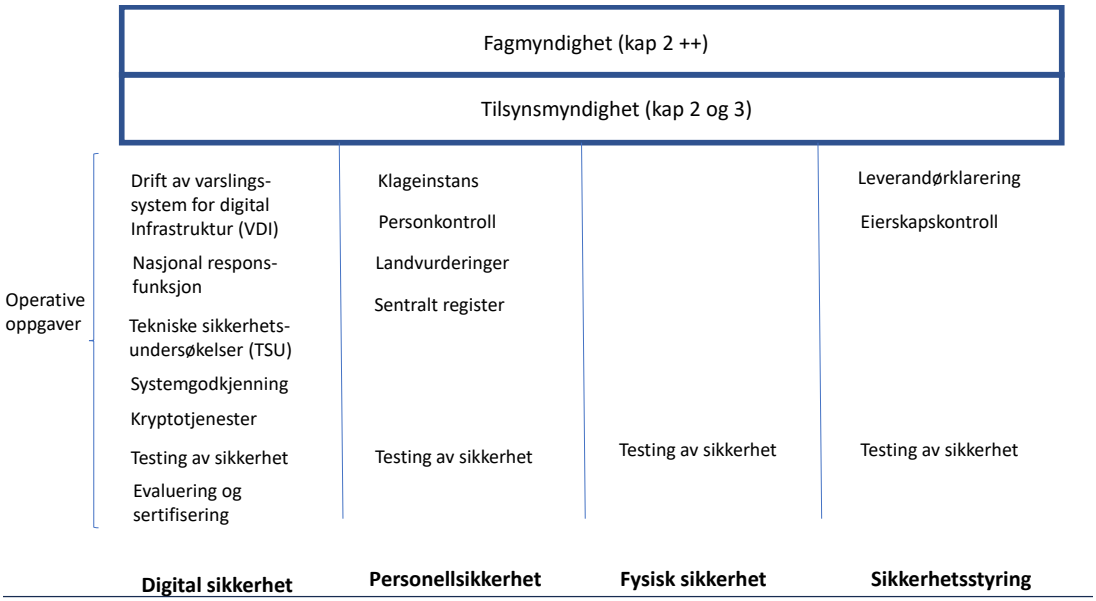
[152] Dokument 3:7 (2022–2023) *Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor*.

10.6 Oppgaver som andre enn Nasjonal sikkerhetsmyndighet kan utføre

I tillegg til å vurdere bredden i NSMs oppgaver er det viktig å se nærmere på hvordan oppgavene best kan løses. Direktoratet arbeider i dag både bredt og dypt. I tillegg til å være fagmyndighet og tilsynsmyndighet utfører NSM selv flere av oppgavene og for egen regning. Det er ressurskrevende.

Utvalget har gått gjennom oppgavene og vurdert om disse kan løses på en mer hensiktsmessig måte enn i dag. Sikkerhetsloven og tilhørende forskrifter åpner for at flere av oppgavene som NSM selv utfører, kan delegeres eller settes ut til andre. Denne muligheten brukes i for liten grad i dag.

Figur 10.2 NSM har en rekke operative oppgaver etter sikkerhetsloven [1)]



[1)] NSM er fag- og tilsynsmyndighet på tvers av sektorer og fag. I figuren har de ulike fagene hver sin kolonne der flere sentrale oppgaver av operativ karakter er listet opp nedover. Enkelte av disse kan utføres av andre.

10.6.1 Tekniske sikkerhetsundersøkelser

NSM bør i større grad enn i dag vurdere mulighetene for å sette ut oppgaven med å gjennomføre tekniske sikkerhetsundersøkelser (TSU). Utvalget er blitt fortalt at behovet for TSU er omfattende, særlig i offentlig sektor som Forsvaret og Utenriksdepartementet, men også i næringslivet. Kapasiteten til slike sikkerhetsundersøkelser i NSM er begrenset og kan derfor ta tid å få utført. Innenfor sine budsjetter har ikke NSM i tilstrekkelig grad valgt å prioritere dette.

Etter forskrift om virksomheters arbeid med forebyggende sikkerhet kan NSM la andre virksomheter utføre slike sikkerhetsundersøkelser.[153] Slik tillatelse er gitt i noen få tilfeller til andre offentlige virksomheter. TSU er en tjeneste som er spesialisert og krever tilgang til sensitivt utstyr og informasjon. Det bør likevel vurderes nærmere om denne muligheten kan nyttes mer enn den er nyttet hittil. Virksomheter som skal utføre sikkerhetsundersøkelser, kan da godkjennes av NSM på forhånd, og direktoratet bør få tilgang til resultatene. NSM tar stilling til om det skal gjennomføres TSU med utgangspunkt i en risikovurdering. Det er derfor viktig at NSM nøye vurderer om det er behov for å gjennomføre TSU. Det bør i tillegg vurderes om det kan legges til rette for at andre kan gi råd til aktuelle virksomheter om sikkerhetstiltak mot avlytting slik at behovet for TSU kan reduseres til det helt nødvendige.

Hvis det ikke er sikkerhetsmessig forsvarlig å sette ut oppgaven i større grad, bør kapasiteten i NSM økes. Direktoratet bør her kunne ta betaling for full kostnad for slike sikkerhetsundersøkelser. Det gir også insentiv hos brukerne til nøye å vurdere behovet. Økt bevissthet hos brukere kan bidra til å styrke sikkerheten. Egenbetaling vil kreve hjemmelsgrunnlag.

10.6.2 Godkjenning av skjermingsverdige systemer

Skjermingsverdige informasjonssystemer skal etter sikkerhetsloven § 6-3 godkjennes av en myndighet som pekes ut av Kongen. Dette er systemer som blant annet skal kunne behandle gradert informasjon, herunder med NATO-gradering. NSM er her pekt ut for de mest komplekse og høyt graderte systemene.[154] Enklere systemer godkjennes av virksomheten selv. NSM eller departementene kan la andre utføre slik godkjenning, men det er i liten grad blitt gjort.

NSM skal som fagmyndighet gi veiledning og råd ved anskaffelser av skjermingsverdige informasjonssystemer. I tillegg skal direktoratet godkjenne systemene før de tas i bruk. Utvalget er blitt fortalt at det har vært aktører som har fulgt rådene, men likevel ikke fått systemene godkjent etter at de er blitt utviklet. Det har vitnet om dårlig kommunikasjon mellom avdelinger og personer i NSM. I tillegg til å gi råd og veiledning og å godkjenne fører NSM tilsyn med systemene.

Godkjenning av informasjonssystemer er en aktivitet som kan kreve virksomhets- eller systemspesifikk kompetanse som kan være krevende for NSM å ha på alle områder, særlig når den teknologiske utviklingen går raskt. Det kan derfor være mer hensiktsmessig at NSM i større grad gir virksomheter adgang til å godkjenne systemet selv. NSM må da vurdere om virksomheten har gode systemer for internrevisjon og internkontroll, at det er nødvendig kompetanse i organisasjonen og at virksomheten er skikket til å ha et slikt eget ansvar for informasjonssystemet. Justis- og beredskapsdepartementet og Forsvarsdepartementet kan sette opp hvilke kriterier virksomhetene skal vurderes ut fra. NATO-krav må ivaretas. Det innebærer blant annet at det må være nødvendig avstand mellom de som drifter og utvikler systemet og de som godkjenner. En slik adgang vil derfor først og fremst kunne

[153] Forskrift om virksomheters arbeid med forebyggende sikkerhet § 48.

[154] Forskrift om virksomheters arbeid med forebyggende sikkerhet § 51.

være aktuelt for store virksomheter. Det må også være regler for de tilfellene der virksomheter ikke blir godkjent til å ha et slikt ansvar.

NSM skal føre tilsyn med at informasjonssystemene som benyttes, er i tråd med sikkerhetslovens krav.

10.6.3 Andre oppgaver som kan utføres av andre

Sikkerhetsloven og forskrifter åpner for at NSM kan delegere eller sette ut oppgaver også på flere andre områder.

NSM kan i henhold til sikkerhetsloven § 5-6 annet ledd godkjenne andre leverandører av tjenester om kryptosikkerhet. Noen få offentlige og private virksomheter er blitt godkjent for dette.

NSM kan videre i henhold til sikkerhetsloven § 6-5 første ledd på anmodning fra virksomheter forsøke å trenge inn i virksomhetens skjermingsverdige informasjonssystemer for å kontrollere om sikkerhetstiltakene er tilstrekkelige. NSM kan i henhold til forskrift om virksomheters arbeid med forebyggende sikkerhet § 62 la andre virksomheter utføre inntrengningstesting. Én offentlig virksomhet er så langt gitt anledning til dette.

Sikkerhetslovens § 6-6 første ledd sier at NSM kan kontrollere om en virksomhets informasjonssystemer behandler sikkerhetsgradert informasjon utover det systemets sikkerhetsgodkjenning tillater. I forskrift åpnes det for at NSM kan la andre gjøre dette, men denne hjemmelen er så langt ikke tatt i bruk.[155]

Tilsvarende kan NSM etter sikkerhetsloven § 7-4 første ledd på anmodning «forsøke å forsere etablerte sikkerhetstiltak for å få tilgang til skjermingsverdige objekter eller infrastruktur» for å kontrollere om sikkerhetstiltakene er tilstrekkelige. NSM kan under nærmere angitte forutsetninger la andre virksomheter utføre testing av sikkerhetstiltak. Én offentlig virksomhet er så langt gitt anledning til å gjøre dette.[156]

NSM skal videre etter forskrift om virksomheters arbeid med forebyggende sikkerhet evaluere produkter og tjenester som virksomhetene ønsker å benytte dersom produktet eller tjenesten er avgjørende for tilgangen til gradert informasjon.[157] Kravene til slik evaluering kan oppfylles gjennom en sertifisering gitt av NSM. Andre kan utpekes til å utføre disse oppgavene, men NSM har så langt ikke utpekt akkrediterte laboratorier eller sertifiseringsorganer.

Hvis NSM gir adgang og legger til rette for at andre, også kommersielle aktører, kan utføre oppgaver, frigjøres kapasitet i direktoratet. Da blir det NSMs oppgave å godkjenne om en organisasjon er moden for å ta ansvaret og deretter komme tilbake på tilsyn. NSM bør stille krav, gi råd og føre tilsyn. Krav og veiledninger må oppdateres i lys av trussel- og risikovurderinger. NSM vil slik kunne gjøres bedre i stand til å vurdere behovene og legge planer fremover som fag- og tilsynsmyndighet.

[155] Forskrift om virksomheters arbeid med forebyggende sikkerhet § 62 første ledd.

[156] Ibid.

[157] Forskrift om virksomheters arbeid med forebyggende sikkerhet § 16.

En slik endring krever oppfølging av de virksomheter som oppgaver settes ut til. NSM må derfor fortsatt bruke ressurser på oppgavene.

10.7 Nasjonal sikkerhetsmyndighets tilsynsoppgaver

NSM skal føre tilsyn med etterlevelsen av sikkerhetsloven. Dette er en oppgave i kjernen av virksomheten. Direktoratet fører tilsyn med departementene, etater, fylkeskommunale og kommunale organer og virksomheter som er underlagt sikkerhetsloven etter vedtak eller i forbindelse med sikkerhetsgraderte anskaffelser.

I noen sektorer har ansvarlig departement gitt oppgaven med å føre tilsyn etter sikkerhetsloven til tilsynsmyndigheten i sektoren. Det er hittil pekt ut fem slike sektortilsyn; Havindustritilsynet, Jernbanetilsynet, Luftfartstilsynet, Nasjonal kommunikasjonsmyndighet og Norges vassdrags- og energidirektorat, se nærmere omtale i kapittel 6.

Dette er en god ordning. I disse sektorene fører ikke NSM direkte tilsyn med virksomheter underlagt sikkerhetsloven, men med at sektortilsynene følger opp virksomhetene på en forsvarlig måte.

Mens NSM har god innsikt i sikkerhetsloven og risikobildet nasjonalt, er det aktørene i sektoren som har mest kunnskap om egen sektor. Det må derfor legges til grunn at sektortilsynene og virksomhetene er best kvalifisert til å vurdere sårbarheter og risikoer. Etter sikkerhetsloven er det virksomhetene selv som har ansvaret for å vurdere hva som skal til for å oppnå et forsvarlig sikkerhetsnivå og å iverksette nødvendige tiltak. Dette gjelder særlig for sikkerhetslovens bestemmelser om objekt- og infrastruktursikkerhet.

Det bør derfor være dialog mellom tilsynsmyndighet og virksomhetene. NSM og sektortilsynene bør lytte til virksomhetenes egne vurderinger av hva som skal til for å oppnå et forsvarlig sikkerhetsnivå. Likeledes bør virksomhetene og sektortilsynene lære av NSM om hvilke krav som følger av sikkerhetsloven. Sektormyndighetene bør også trekkes med når NSM utarbeider rapporter om risiko og sårbarheter i sektorene, og kanskje mer enn i dag.

Der det er utpekt sektortilsyn, skal sikkerhetsmyndigheten etter sikkerhetsloven § 3-1 «likevel gjennomføre tilsyn når det følger av internasjonale forpliktelser eller når det er tvingende nødvendig». Dersom NSM av disse grunner skal føre tilsyn med virksomheter, bør det informeres så tidlig som mulig om dette til sektortilsynet. NSM bør i etterkant redegjøre om eventuelle avvik og pålegg.

Ansvarlig departement bør utpeke sektortilsyn som skal følge opp sikkerhetsloven der det er mulig. Det vil over tid avlaste NSM samtidig som det vil bevisstgjøre aktørene i sektoren i arbeidet med å følge opp sikkerhetsloven. Finanssektoren og helsesektoren fremstår her som aktuelle kandidater.

Flere sektortilsyn har overfor utvalget pekt på at NSM i sin tilsynsmyndighet i blant har operert på egen hånd, uten at sektortilsynet i tilstrekkelig grad er trukket inn. Det kan ha sammenheng med den uklarhet som utvalget har påpekt om hva som ligger i de såkalte «sektorovergripende» roller og ansvar i sikkerhetsloven § 2-2.

Utvalgets anbefaling om klargjøring av innholdet i lovens begreper innbefatter også forholdet mellom NSM og sektortilsyn.

10.8 Grensesnittet mellom Nasjonal sikkerhetsmyndighet og Direktoratet for samfunnssikkerhet og beredskap

Direktoratet for samfunnssikkerhet og beredskap (DSB) bistår Justis- og beredskapsdepartementet med å koordinere arbeidet med samfunnssikkerhet og beredskap. DSB har blant annet som oppgave å kartlegge risiko og ha oversikt over utfordringer for samfunnssikkerheten på tvers av sektorene. DSB har ledet arbeidet med å identifisere kritiske samfunnsfunksjoner etter KIKS-rammeverket. Det er et nasjonalt planleggingsgrunnlag som skal bidra til at departementenes ansvar for samfunnssikkerhet og beredskap blir ivaretatt på tvers av sektorgrensene, se nærmere omtale av arbeidet med kritiske samfunnsfunksjoner i kapittel 6, boks 6.2.

For NSMs oppgaver er sikkerhetsloven det sentrale utgangspunktet. Sikkerhetsloven omhandler nasjonal sikkerhet der de grunnleggende nasjonale funksjonene (GNF) er viktige. Etter sikkerhetsloven er det departementene som er ansvarlige for å identifisere GNF-er innenfor sine områder.[158]

I forarbeidene til sikkerhetsloven gjøres det klart at lovens formål er å beskytte funksjoner og verdier som er av nasjonal betydning og ikke funksjoner som bare har regional eller lokal betydning.[159] Det vises samtidig til at lokale eller regionale hendelser kan ha konsekvenser for sentrale samfunnsinstitusjoner og derfor anses å være av nasjonal betydning. Dette innebærer at arbeidet med kritiske samfunnsfunksjoner og arbeidet med grunnleggende nasjonale funksjoner overlapper. Inntrykket av overlapp forsterkes ved at det benyttes tilnærmet samme begreper om hva de skal beskytte. Sikkerhetsloven definerer nasjonale sikkerhetsinteresser blant annet som «samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet»,[160] mens de kritiske samfunnsfunksjonene etter KIKS-rammeverket defineres som «befolkningens og samfunnets grunnleggende behov og samfunnets funksjonalitet».[161]

Totalberedskapskommisjonen foreslo å slå sammen rammeverkene for KIKS og GNF. Kommisjonen anbefalte også å gjennomgå porteføljene til DSB og NSM «for å avklare eventuelle uklare grensesnitt og oppgavefordeling».[162]

Utvalget er enig i at arbeidet med GNF-ene etter sikkerhetsloven og de kritiske samfunnsfunksjonene etter KIKS-rammeverket må ses i sammenheng. Arbeidet må baseres på et felles kunnskapsgrunnlag og være godt koordinert. Sikkerhetstil-

[158] Sikkerhetslovens § 2-1 første ledd, bokstav a.

[159] NOU 2016: 19 *Samhandling for sikkerhet*, side 673f og Prp. 153 L (2016–2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)*, side 166.

[160] Sikkerhetsloven § 1-5 første ledd bokstav e).

[161] *Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* Direktoratet for samfunnssikkerhet og beredskap 2016.

[162] NOU 2023: 17 Nå er det alvor, side 99.

standen for GNF-ene vil påvirkes av sikkerhetstilstanden for de samfunnskritiske funksjonene etter KIKS. Samtidig har rammeverkene ulike formål og kan ikke uten videre slås sammen til ett felles rammeverk. De bør tvert imot holdes adskilt. Vi viser her til forarbeidene til sikkerhetsloven der det står at «[s]ikkerhetsloven skal trygge nasjonale sikkerhetsinteresser, mens det er andre lover som skal sikre den sivile samfunnssikkerheten».[163]

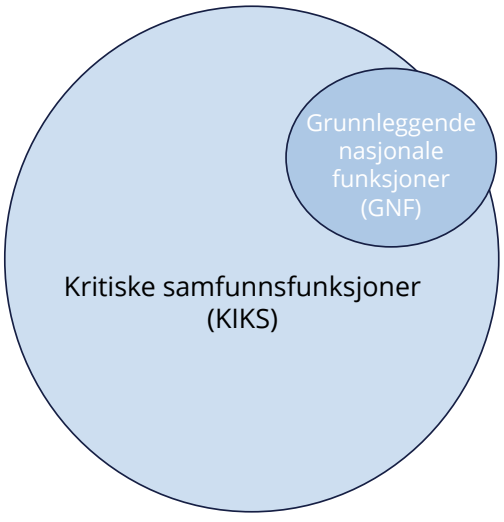
Mens identifisering av GNF skal bidra til å ivareta nasjonal sikkerhet, favner KIKS langt videre. Oversikten over kritiske samfunnsfunksjoner skal bidra til nødvendig koordinering på tvers av sektorgrensene i arbeidet med samfunnssikkerhet, se nærmere omtale i kapittel 6.

Et annet skille mellom rammeverkene er at sikkerhetsloven stiller krav om beskyttelse mot tilsiktede uønskede hendelser og ikke mot hendelser som kan skyldes tilfeldigheter, uhell eller naturskapte forhold, såkalt «all-risiko». Arbeidet med kritiske samfunnsfunksjoner skal styrke motstandsdyktigheten mot hendelser og trygge kontinuiteten til funksjoner, uavhengig av hvilke typer hendelser som kan oppstå.

Et tredje skille er at det er mer aktuelt at politi og eventuelt forsvar vil involveres når de skjermingsverdige verdiene er truet.

GNF-er vil dermed i hovedsak være en mindre delmengde av de kritiske samfunnsfunksjonene, jf. figur 10.3. Ifølge «Veileder i departementenes identifisering av grunnleggende nasjonale funksjoner» utgitt av NSM kan departementene bruke de kritiske samfunnsfunksjonene som et utgangspunkt i arbeidet med å identifisere GNF-er. Det er likevel andre kriterier som ligger til grunn for utvelgelsen av dem.

Figur 10.3 Overlapp mellom kritiske samfunnsfunksjoner og GNF [1)]



[1)] Figuren er inspirert av figur 6.2 i NOU 2016: 19 Samhandling for sikkerhet. Figuren illustrerer at nesten alle grunnleggende nasjonale funksjoner (GNF) etter sikkerhetsloven også er en samfunnskritisk funksjon etter KIKS. Unntak er «Transport av gass i rør til Europa» og «Kontroll med utvinning av petroleum på norsk sokkel» som begge er GNF-er, men ikke kritiske samfunnsfunksjoner.

[163] Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet (sikkerhetsloven)*, side 35.

Hovedinstruksene til de to direktoratene gir i dag inntrykk av vesentlig overlapp i oppgaver, se vedlegg 5. Det bør unngås. Justis- og beredskapsdepartementet bør gå gjennom instruksene med sikte på å oppdatere dem og klargjøre grensesnittet. Der det må være overlapp, bør det også være regler for samhandling.

Utvalget er kjent med at DSB og NSM har arbeidet med å skape et felles grunnlag for hvordan sammenhengen mellom KIKS og GNF skal forstås. Det er positivt. En slik felles forståelse må formidles til berørte sektorer og virksomheter og vedlikeholdes over tid gjennom faste ordninger for dialog og samarbeid.

Sammensatte trusler krever felles situasjonsforståelse, informasjonsdeling og samarbeid for å håndtere kriser og trusler effektivt. Dette vil framover kunne kreve et tettere samarbeid mellom NSM og DSB.

Et tiltak som kan vurderes, er å etablere en såkalt «liaisonfunksjon» for fysisk tilstedeværelse hos hverandre. Dette er en samarbeidsordning som blant annet er brukt en del i Forsvaret. En slik ordning vil kunne identifisere og konkretisere samarbeidsbehov, bidra til at samarbeidet kommer på plass og at det følges opp.

Det er krav i både NSMs og DSBs instrukser om at de skal samarbeide med andre myndigheter der det er relevant. Men dette er ikke tilstrekkelig. I tillegg bør det utformes regler for hvordan de skal arbeide sammen. Det er viktig at arbeidet i de to direktoratene er godt koordinert, og at de gir entydige signaler utad om arbeidet med nasjonal sikkerhet og samfunnssikkerhet. De etablerte arenaene for arbeidet med samfunnssikkerhet på nasjonalt, regionalt og kommunalt nivå bør benyttes. Når NSM for eksempel arbeider med å styrke situasjonsforståelsen i kommuner og fylker om deres betydning for nasjonal sikkerhet, er det viktig at dette koordineres med DSB og statsforvalternes løpende aktiviteter innen samfunnssikkerhet.

Et styrket samarbeid bør gjelde på blant annet på følgende områder:

– deling av informasjon med myndigheter og virksomheter i ulike sektorer for å bidra til bedret situasjonsforståelse
– veiledning av hvordan myndigheter og virksomheter skal forholde seg til ulike situasjoner
– håndtering av sårbarheter, hendelser og kriser
– planlegging, gjennomføring og oppfølging av funn fra tilsyn der tilsynsobjektene er felles for etatene
– internasjonalt arbeid, både mot enkeltland og i Norden, NATO og EU.

Regjeringen varslet i Totalberedskapsmeldingen at den vil foreslå en sektorovergripende lov som skal stille felles krav til grunnsikring hos virksomheter som er viktige for at samfunnet fungerer i fred, krise og krig, se kapittel 6.[164] Dette vil forsterke sammenhengen mellom oppfølging av kritiske samfunnsfunksjoner og arbeidet med nasjonal sikkerhet. Ifølge meldingen vil regjeringen som en del av lovarbeidet også vurdere blant annet grensesnittet mellom samfunnssikkerhetsinstruksen, sikkerhetsloven og den nye loven om grunnsikring av virksomheter. Det

[164] Meld. St. 9 (2024–2025) *Forberedt på krise og krig*.

er behov for en slik gjennomgang, men utvalget mener som nevnt at sikkerhetsloven fungerer etter hensikten.

Dette synes som et nokså omfattende lovarbeid som kan ta tid. For underliggende etater er det viktig å ha klare og oppdaterte rammer å forholde seg til også på kort sikt. Langvarige og store prosesser med lovarbeid ol. bør derfor ikke stå i veien for at instrukser og andre rammer for NSMs og DSBs oppgaver holdes oppdatert, og at grensesnittet mellom dem gjøres klarere.

10.9 Grensesnitt mot øvrige myndigheter

Utvalget har også vurdert NSMs grenseflater mot Etterretningstjenesten, Forsvaret, Politiets sikkerhetstjeneste (PST), Kripos, Sivil klareringsmyndighet, tilsynsmyndigheter og direktorater. Sivil klareringsmyndighet er omtalt i avsnitt 10.3 og tilsynene i avsnitt 10.7.

10.9.1 Etterretningstjenesten og PST

Arbeidsdelingen mellom Etterretningstjenesten og PST synes i det store og hele å være nokså klar. Etterretningstjenesten og PST skal vurdere trusler, mens NSM skal vurdere sårbarheter og risiko som følger av truslene. PST gir råd til myndigheter og virksomheter, og her kan det være gråsoner mot NSMs plikt til å veilede og å gi råd. PST og NSM inngikk i 2020 en avtale om sikkerhetsfaglig rådgiving.

10.9.2 Forsvaret

Forsvaret er en stor bruker av NSMs tjenester og leveranser. Dette er en naturlig konsekvens av at Forsvaret besitter store mengder gradert informasjon og råder over et høyt antall skjermingsverdige objekter og infrastruktur. NSM hadde i sin tid utspring fra den sentrale sikkerhetsorganisasjonen i Forsvaret, jf. omtale i kapittel 3. Forsvaret har fortsatt en egen sikkerhetsorganisasjon av betydelig størrelse ved Forsvarets sikkerhetsavdeling (FSA). Det har sammenheng med at FSA er klareringsmyndighet for forsvarssektoren. Arbeidsdelingen mellom NSM og Forsvaret om forebyggende sikkerhet synes etter utvalgets forståelse å være klar. Ikke desto mindre er det viktig med godt samarbeid, gode rutiner, avklarte ansvarsforhold og rettidig utveksling av informasjon. Gjensidig informasjonsutveksling om NATO-forhold er særlig viktig i denne sammenhengen.

Utvalget har vurdert om enkelte av NSMs oppgaver bør tilbakeføres til Forsvaret, herunder ulike oppgaver knyttet til krypto. I og med at disse oppgavene ikke utføres for Forsvaret alene og er forbundet med rollen som fagmyndighet etter sikkerhetsloven, har utvalget kommet til at NSM fortsatt bør ivareta dem. NSM bør imidlertid i større grad søke å bruke mulighetene i gjeldende regelverk til å la andre utføre oppgavene når forholdene ligger til rette for det, se nærmere omtale i avsnitt 10.6.

10.9.3 Kripos

NSMs grensesnitt mot politiet er særlig mot Kripos. NSM og Kripos er begge sentrale i håndteringen av alvorlige IKT-sikkerhetshendelser rettet mot kritisk infrastruktur. Samtidig har de til dels ulike roller. NSM ved Nasjonalt cybersikkerhetssenter (NCSC) bidrar til å gjenopprette berørte systemer og informerer andre virksomheter for å motvirke at skaden sprer seg. NSM informerer ved behov også regjeringen og allmennheten om hendelser som oppstår. Kripos ved Nasjonalt cyberkrimsenter (NC3) etterforsker hendelser for å avdekke hvem som står bak. Her kan det være ulike hensyn som skal ivaretas av henholdsvis NSM og Kripos. Mens NSM og de berørte virksomhetene som oftest er opptatt av å få systemene raskt opp, kan Kripos ha behov for å avvente gjenoppretting for å etterforske og sikre bevis. Disse hensynene kan dermed krysse hverandre. Ulike hensyn vil vurderes i «Felles cyberkoordineringssenter» (FCKS) der representanter fra NSM, Etterretningstjenesten, PST og Kripos deltar. Det er viktig at det er god kommunikasjon mellom aktørene og at de respekterer at hver av dem har ulike roller og oppgaver som skal ivaretas.

Virksomhetene vil som regel som nevnt ønske å få driften raskt i gang igjen og kan legge mindre vekt på de hensynene som kan være viktige for Kripos. Hvis Kripos kommer for sent til hendelsen, er det en risiko for at spor kan gå tapt. NSM skal i henhold til «Rammeverk for håndtering av IKT-hendelser» som er utgitt av Justis- og beredskapsdepartementet, varsle FCKS om alvorlige IKT-sikkerhetshendelser som rammer kritisk infrastruktur og kritiske samfunnsfunksjoner. Det er imidlertid virksomhetenes ansvar å anmelde saker til politiet.

Det er viktig at NSM tilstrekkelig raskt varsler virksomheter under sikkerhetsloven, samt øvrige virksomheter med samfunnskritisk funksjon om hendelser som oppstår slik at spredning til andre sektorer og virksomheter kan motvirkes. Utvalget antar det også kan være behov for at Kripos informerer både regjeringen og andre dersom etterforskningen tilsier det. Samtidig må vi understreke at etterforskning er en påtalestyrt virksomhet og ikke underlagt politisk kontroll eller politisk avklaring.

En eventuell uenighet blant deltakerne i FCKS vil måtte legges fram for Justis- og beredskapsdepartementet og Forsvarsdepartementet for beslutning, unntatt saker som «hører under den overordnede påtalemyndighet».[165]

Utvalget foreslår ikke endringer i ansvarsdelingen mellom NSM og Kripos i håndtering av hendelser som i stor grad følger av lov og instruks. Dagens system krever gode rutiner for informasjonsutveksling, samspill og for å kunne fatte raske beslutninger.

[165] Retningslinjer for cybersamarbeid fastsatt 20. mars 2017 med endringer, senest 2. februar 2022.

10.9.4 Digitaliseringsdirektoratet og Nasjonal kommunikasjonsmyndighet

Digitaliseringsdirektoratet (Digdir) har fagansvar for offentlig sektors arbeid med informasjonssikkerhet og skal veilede offentlige virksomheter på dette området. NSM skal i sin rolle som det nasjonale fagmiljøet for digital sikkerhet veilede om digital sikkerhet til både offentlige og private virksomheter. Det er dermed to miljøer for råd og veiledning om digital sikkerhet på statlig side. Aktører utvalget har snakket med, peker på at det for brukere kan være krevende å måtte forholde seg til råd og veiledning om digital sikkerhet fra flere ulike hold.

Digdir har også fagansvar for offentlig sektors arbeid med informasjonssikkerhet og er tilsynsmyndighet for såkalt «universell utforming av ikt (Uu-tilsynet)». Digdir følger opp aktiviteter i EU og på nordisk nivå og bidrar med å koordinere og følge opp internasjonale initiativ som Norge deltar i.

Også Nasjonal kommunikasjonsmyndighet (Nkom) har oppgaver innen digital sikkerhet. Nkom er tilsyns- og kontrollorgan for post, elektronisk kommunikasjon og elektroniske tillitstjenester i Norge. Nkom er også tilsynsmyndighet for datasentre, jf. ny lov om elektronisk kommunikasjon som trådte i kraft 1. januar 2025. Nkom har et særskilt ansvar for sikkerhet og beredskap i nett og tjenester for elektronisk kommunikasjon og ble i 2019 utpekt som sektortilsyn etter sikkerhetsloven.

Utvalget foreslår i avsnitt 10.5.2 å avgrense NSMs oppgaver innen digital sikkerhet til de som omhandler nasjonal sikkerhet etter sikkerhetsloven. Utvalget mener Digitaliserings- og forvaltningsdepartementet bør overta ansvaret for å samordne arbeidet med digital sikkerhet utenfor sikkerhetsloven og at oppgavene som tas ut av NSM, overføres til en etat under dette departementet. Digdir og Nkom fremstår her begge som egnede kandidater.

10.10 Kontaktpunkt i NATO

Utvalgets mandat presiserer at utvalgets anbefalinger skal ivareta «forpliktelsene en nasjonal sikkerhetsmyndighet har overfor andre land og internasjonale organisasjoner, spesielt Norges forpliktelser til NATO …» Utvalget er videre bedt om å vurdere «hva som inngår i kontaktpunktfunksjonen til NATO og hvem som er nærmest til å ivareta denne».

Med kontaktfunksjon til NATO menes vanligvis funksjonen som såkalt NATIONAL SECURITY AUTHORITY (NSA). NATO stiller ikke eksplisitte krav til hvem som skal ha denne funksjonen i medlemslandene, men det er et krav om at en slik skal finnes. Denne funksjonen skal være i stand til å påse at sikkerhetsavtalen mellom NATO-landenes krav til forebyggende sikkerhetstiltak gjennomføres i medlemslandene.

NSA-funksjonen skal videre være medlemslandenes hovedkontaktpunkt for NATO Office of Security (NOS) i spørsmål om sikkerhet. NSA-funksjonen kan også henvise NOS videre til annen kompetent myndighet på avgrensede felter. Hvem som har hatt denne funksjonen i Norge, har variert historisk, se boks 7.1.

Å være sikkerhetsmyndighet og å være kontaktfunksjon mot NATO er på denne bakgrunn to sider av samme sak. I Norge er det som nevnt NSM som har denne funksjonen, og det bør videreføres. Det er likevel viktig at NSM trekker andre etater og virksomheter med i forberedelsene og behandlingen av saker som følger av kontaktpunktfunksjonen. NSM må også dele informasjon fra møter i NATO med andre myndigheter som bør ha den. I den utstrekning det er hensiktsmessig og mulig, bør det også åpnes for at andre deltar sammen med NSM på møter eller andre former for fora i NATO-sammenheng.

10.11 Videre utvikling av organisasjonen Nasjonal sikkerhetsmyndighet

10.11.1 Økonomisk styring

Etter en periode med manglende økonomisk styring synes NSM nå å rette det opp.

Da Justis- og beredskapsdepartementet overtok det administrative ansvaret for NSM i 2019, overtok de også grunnfinansieringen av direktoratet. Forsvarsdepartementet finansierer i hovedsak tidsavgrensede prosjekter. NSM har overfor utvalget gitt uttrykk for at slik prosjektfinansiering er utfordrende og vanskelig å planlegge ut fra. NSM bør være tidlig i inngrep med Forsvarets investeringsplaner slik at leveranser til ulike prosjekter kan planlegges i tid og omfang.

10.11.2 Kultur og organisering

En effektiv organisasjon er avhengig av at det utvikles en sunn kultur med åpenhet og samarbeidsvilje internt og med kunnskapssøkende medarbeidere.

Det har vært en periode med uro i organisasjonen, og det er viktig nå å se framover. Utvalget har snakket med flere som har pekt på at kommunikasjonen internt i NSM synes å være mangelfull. Det har vært synlig og også hatt uheldige virkninger utad. Blant annet har det vært ulike faglige syn og tilnærming mellom dem som gir veiledning og råd og dem som fører tilsyn og kontroll.

Det bør skapes et samhold der medarbeiderne er stolte av å representere ett NSM. Å lage tydelige rammer for NSMs virksomhet, med sikkerhetsloven som kjerne, kan bidra til en slik utvikling.

10.12 Styringen av Nasjonal sikkerhetsmyndighet

10.12.1 Langsiktig planlegging

Ifølge Regelverket for økonomistyring i staten skal departementene «planlegge sin styring av virksomheten med både ettårig og flerårig perspektiv».[166] Ledelsen

[166] Regelverket for økonomistyring i staten, også omtalt som økonomiregelverket (ØR) er en felles instruks for departementene og de underliggende virksomhetene i statsforvaltningen. ØR inneholder hovedreglene, mens bestemmelsene og rundskrivene beskriver reglene mer detaljert og utdyper hovedreglene.

i virksomhetene skal «fastsette mål og resultatkrav og foreta prioriteringer med ettårig og flerårig perspektiv innenfor eget ansvarsområde». Dette ble tillagt vekt av utvalget som utredet NSMs leie av Snarøyveien 36 i 2024.[167] Selv om ettårsprinsippet i staten innebærer at bevilgninger vedtas for ett år av gangen, er det viktig at departementene og virksomhetene ser utfordringer og prioriteringer i et langsiktig perspektiv.[168] Både Forsvarsdepartementet og Justis- og beredskapsdepartementet bør strekke seg langt for å gi NSM forutsigbare rammebetingelser til å utvikle organisasjonen.

Planer framover om hvordan NSM skal utvikles som organisasjon, må bygge på hvilke oppgaver og hvilken rolle direktoratet skal ha i det samlede sikkerhetsarbeidet i Norge. Det er viktig at drøfting av dette inngår som en fast del av NSMs styringsdialog med Justis- og beredskapsdepartementet og Forsvarsdepartementet. Et langsiktig perspektiv bør også ligge til grunn når direktoratet gis nye oppgaver som skal finansieres. Satsingsforslag bør være forankret i en plan for virksomheten over tid som departementene må påse at direktoratene har. Her hviler det et ansvar både på de styrende departementene og på NSM.

I tråd med økonomiregelverket i staten følger det av instruksen til NSM at direktoratet skal utarbeide strategier i et årlig og et flerårig perspektiv og at «NSM skal ha en langsiktig tilnærming til videreutviklingen av egen organisasjon for å legge til rette for at organisasjonens kvalitet og leveringsevne ivaretas på lang sikt».[169] Vi ser få spor av en slik langsiktig planlegging.

Departementene har også lagt opp til at det normalt skal avholdes årlige strategimøter om utfordringer og videre utvikling av virksomheten i et mer langsiktig perspektiv. Et slikt møte med NSM er likevel ikke avholdt siden våren 2023. Styringen synes snarere å bære preg av kortsiktighet med nye oppdrag gjennom året blant annet i supplerende tildelingsbrev. Nye oppdrag i gjennomføringsåret som påvirker ressursfordelingen og prioriteringer internt, gjør det vanskelig for direktoratet å planlegge virksomheten på en god måte. NSM oppgir at det også har vært en økning i oppdrag der departementene ber om råd i rollen som sekretariat for statsråden, ofte med korte tidsfrister.

Utvalget er spørrende til at departementene og NSM ikke i større grad har hatt en dialog om utviklingen i et noe lengre tidsperspektiv, ikke minst i lys av de mange nye oppgavene som direktoratet er blitt tildelt. Denne utviklingen med stadig nye oppgaver synes ikke å ha vært forankret i en langsiktig plan. Det å få stadig nye oppgaver krever tid og kapasitet som ellers kunne vært brukt til å styrke oppfølgingen av kjerneoppgavene.

Det må legges større vekt enn hittil på at NSM i sine innspill til departementene om de årlige bevilgningene må være basert på planer for i alle fall fire til fem år for hvordan organisasjonen skal utvikles og oppgaver prioriteres. Departementene bør

[167] NSMs leie av Snarøyveien 36, punkt 7, side 74.

[168] https://dfo.no/fagomrader/styring-i-staten/tidsperspektiv-i-styringen/tidsperspektivet-i-virksomhetens-planer

[169] Hovedinstruks til Nasjonal sikkerhetsmyndighet, fastsatt av Justis- og beredskapsdepartementet og Forsvarsdepartementet med virkning fra 03.05.2019, punkt 4.2 Krav til virksomhetens planlegging, gjennomføring og oppfølging.

samtidig være avholdne med å gi NSM flere oppgaver. Langsiktig planlegging vil legge til rette for forutsigbarhet om omfang og innretning av FoU og FoU-relaterte prosjekter. Langsiktig planlegging kan også bidra til å avdekke behov og muligheter for samarbeid med tilgrensende aktører. Departementene må sørge for en samordnet, helhetlig og langsiktig tilnærming i både styringen og finansieringen av direktoratet. Nye oppdrag og styringssignaler bør som nevnt som hovedregel komme i de årlige tildelingsbrevene som sendes ut i desember.

10.12.2 Departementstilhørighet

Forsvarsdepartementet fikk det administrative ansvaret for NSM da direktoratet ble opprettet i 2003. Et mindretall i den sammensatte justis- og forsvarskomiteen mente da at dette ansvaret burde ligge i Justisdepartementet, se kapittel 3. Regjeringen Solberg overførte det administrative ansvaret for NSM fra Forsvarsdepartementet til Justis- og beredskapsdepartementet i 2019. Justis- og beredskapsdepartementet overtok også ansvaret for sikkerhetsloven i denne prosessen. Samtidig utnevnte regjeringen en egen samfunnssikkerhetsminister i Justis- og beredskapsdepartementet som skulle følge opp blant annet NSM. Overføringen skjedde uten noen forutgående utredning. Posten som samfunnssikkerhetsminister er senere bortfalt.

Utvalgets mandat har først og fremst vært å vurdere NSMs oppgaveportefølje og samspill med andre aktører i det forebyggende sikkerhetsarbeidet i Norge. Det er likevel utvalgets inntrykk at NSMs oppgaver påvirkes av hvilket departement som har det administrative ansvaret. Flere av oppgavene som direktoratet har fått etter 2019, har vært oppgaver i sivil sektor under Justis- og beredskapsdepartementets ansvarsområde.

Det har som nevnt stor verdi å ha én nasjonal sikkerhetsmyndighet med oppgaver både på sivil og militær side. Totalberedskapsmeldingen, som ble lagt fram i januar 2025, peker i retning av at sivil sektors medvirkning til nasjonal sikkerhet blir viktigere. Sammensatte trusler i form av digitale angrep, økonomisk virkemiddelbruk, påvirkningsoperasjoner mv. øker i omfang, jf. kapittel 9. Slike trusler rettes i stor grad mot sivil sektor, men kan utfordre nasjonale sikkerhetsinteresser. Utvalget legger derfor til grunn at NSM fortsatt skal styres av både Justis- og beredskapsdepartementet og Forsvarsdepartementet, men der ett av dem har det administrative ansvaret. Det er også riktig at det departementet som er administrativt ansvarlig, også har ansvaret for sikkerhetsloven.

Sivil sektors økte betydning for den nasjonale sikkerheten kan trekke i retning av at det er Justis- og beredskapsdepartementet som bør ha det administrative ansvaret for NSM også framover. Direktoratet ble overført til Justis- og beredskapsdepartementet nesten samtidig med at sikkerhetsloven ble revidert. Den nye sikkerhetsloven av 2018 la et klarere ansvar for å vurdere risikoen og sørge for en forsvarlig sikkerhet på den enkelte virksomhet. Behovet for veiledning og råd fra NSM har derfor økt og vil trolig øke videre framover.

En viktig grunn til at sivil sektor og samfunnssikkerhet har fått økt betydning for den nasjonale sikkerheten, er den økte digitaliseringen i samfunnet. Justis- og

beredskapsdepartementet har samordningsansvaret for digital sikkerhet på sivil side i regjeringsapparatet. Et digitalt angrep i sivil sektor kan slå ut funksjoner som rammer statssikkerheten og Forsvaret. Digital sikkerhet er derfor et område som er prioritert i NSM de siste årene. Oppgavene på dette området bør avgrenses til de som ligger nær kjerneoppgavene etter sikkerhetsloven, jf. avsnitt 10.5.2 ovenfor.

Samtidig kan det være hensyn som taler for at det er Forsvarsdepartementet som bør ha det administrative ansvaret for NSM. Direktoratet er en stor leverandør av tjenester til Forsvaret. Den sikkerhetspolitiske utviklingen kan tilsi at oppgavene framover i større grad må ses i sammenheng med risikoen for krig. Forsvarets langtidsplan legger opp til et stort forsvarsløft, blant annet som følge av utfordringene fra Russland. Dette vil også innebære en økning i NSMs oppgaver for å støtte Forsvaret.

NSMs oppgaver for Forsvaret vil trolig bli høyere prioritert med Forsvarsdepartementet som administrativt ansvarlig. I dagens finansieringsmodell har Justis- og beredskapsdepartementet i hovedsak ansvaret for ordinære driftsmidler til NSM, mens Forsvarsdepartementet i hovedsak stiller til rådighet prosjektmidler. Hvis NSM ikke har tilstrekkelig kapasitet til å ivareta de oppgavene som forsvarssektoren etterspør, vil Forsvarsdepartementet kunne måtte søke løsninger utenom NSM. Dette vil i så fall svekke den rollen som sikkerhetsmyndighet for både militær og sivil sektor som NSM er ment å ha.

Utvalget mener det er hensyn som trekker i begge retninger i en avveiing av hvilket departement som skal ha det administrative ansvaret for NSM.

Uavhengig av hvilket departement som er administrativt ansvarlig for NSM, må styringen være godt samordnet mellom departementene. Samfunnsoppdraget og organisasjonen må utvikles videre ut fra det oppdaterte risikobildet framover. Dette forutsetter at departementene har et langsiktig omforent perspektiv i styringen.

10.13 Endringer i regelverk

Utvalget er i mandatet bedt om å synliggjøre «eventuelle behov for justeringer i forskriftene til sikkerhetsloven og kgl. res» som følge av utvalgets forslag. Nedenfor peker vi på noen slike behov for justeringer der det først og fremst er NSMs hovedinstruks som påvirkes. I tillegg er det andre punkter som bør innarbeides i instruksen.

Som vist til i avsnitt 10.2 bør det klargjøres hvilket ansvar og hvilke oppgaver som følger av formuleringen i sikkerhetsloven § 2-2 om at «sikkerhetsmyndigheten har det sektorovergripende ansvaret for at forebyggende sikkerhetsarbeid i virksomhetene utføres i samsvar med loven». Etter sin ordlyd angir dette et stort ansvar, og det bør klargjøres hvor langt ansvaret strekker seg. En slik klargjøring bør blant annet fremkomme i NSMs hovedinstruks.

Generelt bør begrepene som brukes gi en presis beskrivelse av NSMs oppdrag. Ord som «ansvar», «overordnet» og «sektorovergripende» er omtrentlige og lite presise

og kan forvirre. Betegnelsen «ansvar» brukes hyppig i både loven og hovedinstruksen. Et juridisk ansvar vil si å bære følger av handlinger eller unnlatelser. En bedre beskrivelse er å si at NSM har oppgaver som berører flere sektorer.

Utvalget foreslår at det bør innføres egenfinansiering av NSMs tekniske sikkerhetsundersøkelser av rom (TSU). Dette krever et hjemmelsgrunnlag. For godkjenning av informasjonssystemer er det en slik hjemmel i forskrift om virksomheters arbeid med forebyggende sikkerhet § 50.

Utvalget foreslår å ta ut flere oppgaver innen digital sikkerhet utenfor sikkerhetsloven i avsnitt 10.5.2 og å legge disse oppgavene under Digitaliserings- og forvaltningsdepartementet. Det kan ha konsekvenser for ansvarsdelingen mellom departementene, jf. at Justis- og beredskapsdepartementet i kgl.res. 22. mars 2013 fikk ansvaret for å samordne IKT-sikkerhet på sivil side.

I instruksen bør det ikke sies at NSM er «det nasjonale fagmiljøet for digital sikkerhet», men «et nasjonalt fagmiljø for digital sikkerhet» (blant flere andre), jf. avsnitt 10.5.2. Flere bestemmelser i instruksen faller dessuten bort når oppgaver tas ut av NSM slik utvalget foreslår.

Det er betydelig og til dels unødig overlapp mellom hovedinstruksene til NSM og Direktoratet for samfunnssikkerhet og beredskap (DSB). Justis- og beredskapsdepartementet bør derfor rydde samtidig i de to instruksene med sikte på å få fram både likheter og ulikheter i oppgavene.

Departementet bør utforme regler for på hvilke områder og hvordan de to virksomhetene skal samhandle, og samtidig sørge for at oppgavene ikke overlapper. Det er viktig at de to direktoratene opptrer samlet overfor aktører de begge samarbeider med.

Gjeldende instruks er detaljert og har en rekke «skal-punkter». En slik detaljstyring kan innskrenke handlingsrommet til virksomhetens leder. Departementene bør i større grad fastsette mål og overlate til virksomhetsleder å planlegge og prioritere ressurser innenfor fastsatte rammer. Det vil også legge et bedre grunnlag for departementenes styringsdialog med NSM.

Det følger av instruksen at NSM skal utarbeide strategier både i et årlig og et flerårig perspektiv og at «NSM skal ha en langsiktig tilnærming til videreutviklingen av egen organisasjon for å legge til rette for at organisasjonens kvalitet og leveringsevne ivaretas på lang sikt». Som pekt på i avsnitt 10.12 skorter det på etterlevelsen av denne bestemmelsen. Erfaringene fra de foregående årene viser at det kan slå galt ut. Økonomireglementets krav på dette området bør derfor tillegges større vekt enn hittil i både instruksen og etterlevelsen av den.

Instruksen har et eget kapittel for sjef NSM. En slik inndeling er lite hensiktsmessig. De punktene som står her, bør stiles til virksomheten, ikke sjefen.

Generelt må instruksen gås gjennom og oppdateres. Det er blant annet ikke en samfunnssikkerhetsminister i dag, og det kan være andre forhold i instruksen som bør oppdateres. Instruksen bør fastsettes av Justis- og beredskapsdepartementet, som administrativt ansvarlig departementet. Justis og beredskapsdepartementet

må sørge for at instruksen er samordnet med Forsvarsdepartementet og eventuelle andre berørte departement, men det bør kun være ett departement som fastsetter instrukser.

Justis- og beredskapsdepartementet ga i 2017 ut «Rammeverk for håndtering av IKT-sikkerhetshendelser». Dette var før gjeldende sikkerhetslov trådte i kraft, og det har vært en rask utvikling på dette området siden da. Rammeverket bør derfor oppdateres.

10.14 Økonomiske og administrative konsekvenser

Utvalgets anbefalinger skal i henhold til mandatet være budsjettnøytrale. Utvalget har ikke tallfestet hva de enkelte forslagene betyr budsjettmessig. Forslagene bidrar etter vårt skjønn til å styrke arbeidet med forebyggende sikkerhet uten at statens kostnader samlet sett vil øke.

Utvalgets forslag kan i grove trekk deles inn i tre kategorier: Vi foreslår for det første at enkelte oppgaver innen digital sikkerhet overføres til andre myndigheter, se særlig avsnitt 10.5.2. Dernest foreslår vi at NSM i større grad enn i dag nytter mulighetene i regelverket til å delegere operative oppgaver til andre, se avsnitt 10.6. For det tredje foreslår vi at oppgavefordelingen mellom NSM og Direktoratet for samfunnssikkerhet og beredskap (DSB) tydeliggjøres og at Justis- og beredskapsdepartementet gir klare regler for samarbeidet mellom dem.

De to første av disse forslagene vil bidra til at NSM i større grad enn i dag kan konsentrere seg om sine kjerneoppgaver som fagmyndighet og tilsynsmyndighet etter sikkerhetsloven. Forslagene vil bidra til å styrke arbeidet med forebyggende nasjonal sikkerhet. Med en mer konsentrert oppgaveportefølje vil NSM ha bedre oversikt og bedre forutsetninger for å kunne planlegge og tilpasse ressursene der behovene forventes å bli størst. Dette vil også legge grunnlag for en mer effektiv virksomhet. NSM må planlegge driften innenfor en realistisk budsjettering.

Når oppgaver overføres eller delegeres til andre offentlige myndigheter, vil ressursbruken i NSM bli mindre. Samtidig vil ressursbruken i utgangspunktet øke tilsvarende hos de som overtar oppgavene. Netto bør arbeidsmengden i utgangspunktet være omtrent den samme. Det kan være behov for opplæring og enkelte investeringer hos de som overtar oppgavene i en overgangsfase. Utvalget antar likevel at departementenes og etatenes arbeid med digital sikkerhet samlet sett vil kreve økte bevilgninger i årene framover.

Oppgaver som settes ut til private og kommersielle aktører eller som finansieres gjennom brukerbetaling slik utvalget foreslår, fører til mindre statlige utgifter og høyere utgifter for brukere av tjenestene. Brukerbetaling er generelt hensiktsmessig fordi det gir insentiver hos bruker til å nærmere vurdere behovet for tjenestene som etterspørres.

Overføring av oppgaver vil kunne berøre NSMs ansatte. Ved overføring av oppgaver kan det være naturlig at det følger personell med til myndigheter som overtar

oppgavene. Ved delegering av oppgaver, vil antallet ansatte kunne gå ned. Utvalget antar at en slik eventuell nedskalering kan gjøres over tid.

Endringene som foreslås vil kreve administrativt arbeid og trolig endringer i organiseringen i NSM og andre berørte etater. Det vil innebære administrative forberedelser og merarbeid i en overgangsperiode.

Utvalgets forslag om å tydeliggjøre grensesnitt og saksbehandlingsrutiner mellom NSM og DSB vil kunne bidra til en mer effektiv drift i begge direktoratene og hos brukere av tjenestene.

Boks 10.1 Anbefalinger fra andre utvalg mv.

Flere offentlige utvalg har utredet sikkerhetspolitiske problemstillinger de senere årene. NSM arbeider i et samspill med mange aktører for å styrke landets sikkerhet. Ved å foreslå endringer på noen områder i dette samspillet, blir gjerne flere aktører berørt, også NSM. Nedenfor er det vist til tre utredninger som ble avgitt i 2023. Til sist omtales også en rapport fra Riksrevisjonen i 2022 om IKT-sikkerhet.

NOU 2023: 14 Forsvarskommisjonen av 2021
Forsvarskommisjonen la vekt på EOS-tjenestenes evne til å møte det sammensatte trusselbildet Norge står overfor. Sammensatte trusler må ifølge kommisjonen møtes med bedre situasjonsforståelse og styrket motstandsdyktighet i samfunn og befolkning. Videre skriver Forsvarskommisjonen (side 223):

«En helhetlig gjennomgang av roller, ansvar, organisering av oppgaver og mandater knyttet til de norske sikkerhets- og etterretningstjenestene (EOS-tjenestene) bør vurderes for å sikre god ressursutnyttelse og styrket evne til å møte det kompliserte og sammensatte trusselbildet. Det må sikres tilstrekkelig hjemmelsgrunnlag og kontroll med tjenestene.»

NSM er del av EOS-tjenestene. Forsvarskommisjonen mente EOS-tjenestenes evne «til å gi et samlet og overordnet råd til Statsministerens kontor og departementene bør styrkes og videreutvikles. Det er behov for å styrke det utadrettede arbeidet med tverrsektoriell situasjonsforståelse på lokalt, regionalt og sentralt nivå. Dette vil øke kunnskapen og bevisstheten om aktuelle trusler og trusselaktører, og sammenhengen mellom ulike politikkområder.»

NOU 2023: 17 Nå er det alvor – Rustet for en usikker fremtid (Totalberedskapskommisjonen)
Totalberedskapskommisjonen vurderte styrker og svakheter ved dagens beredskapssystemer og anbefalte blant annet «å arbeide for en sammenslåing av rammeverkene for kritiske samfunnsfunksjoner og grunnleggende nasjonale funksjoner». Rammeverket for kritiske samfunnsfunksjoner følges opp av Direktoratet for samfunnssikkerhet og beredskap mens rammeverket for grunnleggende nasjonale funksjoner (GNF) følges opp av NSM. To rammeverk gir ifølge kommisjonen betydelig ekstraarbeid, samtidig som det kan «svekke koordineringen av analyser, risikovurderinger, planverk og respons».

Kommisjonen anbefalte også «å gjennomgå porteføljene til Direktoratet for samfunnssikkerhet og beredskap og Nasjonal sikkerhetsmyndighet for å avklare eventuelle uklare grensesnitt og oppgavefordeling».

Boks 10.1 forts.

NOU 2023: 28 Investeringskontroll (Investeringskontrollutvalget)
Investeringskontrollutvalget skrev blant annet:

«Utvalget anbefaler at saker om investeringskontroll behandles i en egen organisatorisk enhet på etatsnivå. Vurderinger og saksbehandling, uavhengig av hvilken sektor investeringen gjelder, bør foretas av kontrollmyndigheten på selvstendig grunnlag. Dette vil sikre konfidensialitet rundt sensitive opplysninger, bedre effektiviteten, redusere risikoen for ulik behandling og gjøre ansvaret tydeligere i eventuelle klagesaker.

Samtidig ser utvalget at samarbeid med relevante etater kan bidra til synergieffekter, forhindre dobbeltarbeid og være ressursbesparende. Det bør derfor legges til rette for at opplysninger som er nødvendige for å vurdere den enkelte sak, kan hentes inn fra sikkerhetstjenester og sektormyndigheter på en effektiv måte, samtidig som kontrollmyndighetens selvstendighet ivaretas.

Utvalget mener det er flere hensyn som taler for at en ny ordning for investeringskontroll legges til en egen, ny myndighet, og at det er relevant å vurdere om denne bør organiseres sammen med den nye etaten for eksportkontroll og sanksjoner.»

Etaten som Investeringskontrollutvalget viser til, er Direktoratet for eksportkontroll og sanksjoner (DEKSA) som ble etablert 1. januar 2025. DEKSA er underlagt Utenriksdepartementet, og utenriksministeren har det konstitusjonelle ansvaret for fagområdene.

Investeringskontrollutvalget anbefalte også at reglene om eierskapskontroll i sikkerhetsloven tilpasses og innarbeides i ny lov om investeringskontroll. Det vil ifølge utvalget bidra til at alle meldinger om investeringskontroll behandles etter det samme regelverket.

Riksrevisjonen Dokument 3:7 (2022–2023) Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor
Anbefalingene er rettet mot Justis- og beredskapsdepartementet, men de berører også NSM.

Riksrevisjonen anbefalte at Justis- og beredskapsdepartementet «tar en tydeligere samordnings- og pådriverrolle for nasjonal digital sikkerhet i sivil sektor». Riksrevisjonen anbefalte videre at Justis- og beredskapsdepartementet skulle sørge for at «Nasjonal sikkerhetsmyndighet i samarbeid med de andre veiledningsaktørene gjør veiledningen på det digitale sikkerhetsområdet mer samordnet og tilgjengelig». Departementet bør ifølge Riksrevisjonen også sørge for at de etablerte arenaene for samordning utnyttes bedre og at alle departementene «har tilstrekkelig framdrift i arbeidet som følger av ny sikkerhetslov». Justis- og beredskapsdepartementet bør dessuten styrke

Boks 10.1 forts.

arbeidet «med å avdekke, håndtere og koordinere innsatsen mot alvorlige digitale hendelser».

I rapporten pekes det blant annet på at både omfang og overlapp i ulike regelverk er en utfordring. Sikkerhetsloven og samfunnssikkerhetsinstruksen er grunnlag for arbeidet med henholdsvis nasjonal sikkerhet og samfunnssikkerhet, der digital sikkerhet er en integrert del. Det er krevende for virksomheter å avklare hvilke regelverk de er omfattet av, hvem de skal forholde seg til og hvilke veiledere de skal benytte. Riksrevisjonen etterlyste ensartet og tilgjengelig veiledning og veiledningsmateriell.

Ifølge Riksrevisjonen er Nasjonalt cybersikkerhetssenter «en velfungerende samordningsarena innenfor forebyggende sikkerhetsarbeid. Senteret arrangerer jevnlige og hyppige møter med relevante tema og legger til rette for erfaringsutveksling mellom deltakerne. Deltakerne opplever begge deler som nyttig».

11 Vedlegg

Vedlegg 1: Viktige dokumenter

Nedenfor er det listet opp viktige dokumenter utvalget har innhentet informasjon fra. Ikke alle dokumentene er med her, som blant annet en rekke hjemmesider, flere lover i andre land og EU-direktiver og forordninger. Disse fremkommer i tekst og fotnoter.

Proposisjoner og meldinger:

Prop. 97 L (2015–2016) *Endringer i sikkerhetsloven (reduksjon av antall klareringsmyndigheter mv.*

Prop. 1 S (2017–2018) *For budsjettåret 2018 Justis- og beredskapsdepartementet.*

Prop. 153 L (2016–2017) *Lov om nasjonal sikkerhet (sikkerhetsloven).*

Prop. 57 S (2018–2019) *Endringer i statsbudsjettet 2019* og Innst. 236 S (2018–2019).

Prop. 78 S (2021–2022) (Ukrainaproposisjonen) og Innst. 270 S (2021–2022).

Prop. 95 L (2022–2023) *Endringer i sikkerhetsloven (eierskapskontroll og lovens virkeområde).*

Prop. 109 LS (2022–2023) *Lov om digital sikkerhet (digitalsikkerhetsloven) og samtykke til godkjenning av EØS-komiteens beslutninger nr. 21/2023 og 22/2023 om innlemmelse i EØS-avtalen av direktiv (EU) 2016(1148 og forordningene (EU) 2018/151 og (EU) 2019/881.*

Prop. 19 S (2023–2024) *Endringar i statsbudsjettet 2023* og Innst. 143 S (2023–2024).

Prop. 104 S (2023–2024) *Tilleggsbevilgninger og omprioriteringer i statsbudsjettet 2024* og Innst. 447 S (2023–2024).

Prop. 34 S (2023–2024) Tillegg til *Prop. 30 S (2023–2024) om ny saldering av statsbudsjettet 2023* og Innst. 150 S (2023–2024).

Prop. 87 S (2023–2024) *Forsvarsløftet- for Norges trygghet. Langtidsplan for forsvarssektoren 2025–2036.*

Prop.1 S (2024–2025) for budsjettåret 2025 under Forsvarsdepartementet.

Prop. 1 S (2024–2025) for budsjettåret 2025 under Justis- og beredskapsdepartementet.

St.meld. nr. 17 (2002–2003) *Samfunnssikkerhet - Veien til et mindre sårbart samfunn*

St.meld. nr. 17 (2006–2007) *Eit informasjonssamfunn for alle.*

Meld. St. 38 (2016–2017) *IKT-sikkerhet. Et felles ansvar*

Meld. St. 10 (2019–2020) *Høytflyvende satellitter – jordnære formål.*

Meld. St. 9 (2024–2025) *Totalberedskapsmeldingen – Forberedt på kriser og krig.*

Offentlige utredninger og rapporter:

NOU 2000:20 *Et nytt forsvar*

NOU 2000:24 *Et sårbart samfunn*

NOU 2015: 13 *Digital sårbarhet – sikkert samfunn. Beskytte enkeltmennesker og samfunn i en digitalisert verden*.

Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enhver tid? Temarapport fra Direktoratet for samfunnssikkerhet og beredskap 2016.

NOU 2016: 19 *Samhandling for sikkerhet. Beskyttelse av grunnleggende samfunnsfunksjoner i en omskiftelig tid.*

NOU 2018: 14 *IKT-sikkerhet i alle ledd – Organisering og regulering av nasjonal IKT-sikkerhet.*

NOU 2023: 14 *Forsvarskommisjonens vurderinger* (Forsvarskommisjonen).

NOU 2023: 17: *Nå er det alvor – Rustet for en usikker fremtid.*

NOU 2023: 28 *Investeringskontroll. En åpen økonomi i usikre tider* (Investeringskontrollutvalget).

Rapporten *NSMs leie av Snarøyveien 36*, avlagt 1. mars 2024 fra et utvalg oppnevnt av regjeringen 15. desember 2023.

Riksrevisjonen:

Dokument 3:7 (2022–2023) *Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor.*

Trussel- og risikovurderinger fra EOS-tjenestene:

Etterretningstjenesten (2025). *Fokus 2025: Etterretningstjenestens vurdering av aktuelle sikkerhetsutfordringer*

Politiets sikkerhetstjeneste (PST) (2025). *Nasjonal trusselvurdering 2025.*

Nasjonal sikkerhetsmyndighet (NSM) (2025). *Risiko 2025. Et sikkert Norge i en usikker verden.*

Lover, forskrifter kongelige resolusjoner:

Kronprinsregentens resolusjon 4. juli 2003 nr. 900, *Fordeling av ansvar for forebyggende sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet*

Lov av 20. juni 2018 nr. 24 om nasjonal sikkerhet (sikkerhetsloven).

Lov av 13. desember 2024 nr. 76 om elektronisk kommunikasjon (ekomloven).

Forskrift 20. desember 2018 nr. 2053 om virksomheters arbeid med forebyggende sikkerhet (virksomhetsikkerhetsforskriften).

Forskrift 20. desember 2018 nr. 2054 om sikkerhetsklarering og annen klarering (klareringsforskriften).

Forskrift 20. desember 2018 nr. 2055 om kryptosikkerhet.

Kongelig resolusjon 22. mars 2013 om overføring av samordningsansvaret for forebyggende IKT-sikkerhet fra Fornyings-, administrasjons og kirkedepartementet til Justis- og beredskapsdepartementet.

Kongelig resolusjon 20. desember 2018 Ikraftsetting av lov 1. juni nr. 24 om nasjonal sikkerhet med overgangsregler, fordeling av myndighet, videreføring av forskrifter m.m.

Kongelig resolusjon 16. oktober 2023 om endringer i regjeringens sammensetning, statsrådenes ansvarsområder og endringer i departementsstrukturen og departementsnavn.

Kongelig resolusjon 20. desember 2023 om endringer i departementsstrukturen og ansvarsdelingen mellom departementene.

Høringsbrev 11. september 2024 til forskrift til digitalsikkerhetsloven, Justis- og beredskapsdepartementet

Høringsnotat 4. januar 2023 om forslag til ny lov om beskyttelse av norsk forsvarsteknologi og sikkerhetsgraderte patenter, Forsvarsdepartementet

Instrukser, retningslinjer, veiledere mv.:

C-M(2002)49 - REV1, Security Within The North Atlandtic Treaty Organization (NATO), 20. November 2020

NATO Agreement for the Mutual Safeguarding of Secrecy of Inventions relating to Defence and for which Applications for Patents have been made, 21. September 1961

Instruks for Direktoratet for samfunnssikkerhet og beredskaps koordinerende roller, fastsatt ved kgl.res. 24. juni 2005, jf. St.meld. nr. 17 (2001–2002).

Instruks for Politiets sikkerhetstjeneste, fastsatt ved kgl. res. 19. august 2005 med hjemmel i lov 4. august 1995 nr. 53 om politiet (politiloven) §29.

Instruks for departementenes arbeid med samfunnssikkerhet (samfunnssikkerhetsinstruksen) fastsatt av Justis- og beredskapsdepartementet 2017 med hjemmel i delegeringsvedtak 10. mars 2017 nr. 312.

Rammeverk for håndtering av IKT-sikkerhetshendelser. Fastsatt av Justis- og beredskapsdepartementet 2017.

Retningslinjer for cybersamarbeid fastsatt 20. mars 2017 med endringer, senest 2. februar 2022.

Regelverket for økonomistyring i staten, fastsatt 12. desember 2003 med endringer, senest 20. desember 2022.

Veileder i departementenes identifisering av grunnleggende nasjonale funksjoner, utgitt av NSM 28. mai 2020.

Hovedinstruks for Nasjonal sikkerhetsmyndighet. Fastsatt av Justis- og beredskapsdepartementet og Forsvarsdepartementet med virkning fra 3. mai 2019.

Justis- og beredskapsdepartementets hovedinstruks til Politiets sikkerhetstjeneste. Fastsatt av Justis- og beredskapsdepartementet med virkning fra 20. mai 2019.

Instruks om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste, fastsatt ved kgl.res. 13. oktober 2006 og sist endret 18. juni 2021.

Hovedinstruks for politiet. Fastsatt av Justis- og beredskapsdepartementet med virkning fra 21. juli 2022.

Hovedinstruks til Direktoratet for samfunnssikkerhet og beredskap. Fastsatt av Justis- og beredskapsdepartementet med virkning fra 1. januar 2024.

Hovedinstruks til Sivil klareringsmyndighet (SKM) fastsatt av Justis- og beredskapsdepartementet med virkning fra 1. januar 2025.

NSMs årsrapport for perioden 2015–2024.

EU-direktiver og forordninger (utvalgte):

Europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen (NIS1-direktivet).

Europaparlaments- og rådsdirektiv (EU) 2022/2555 av 14. desember 2022 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen (NIS2-direktivet).

Europaparlaments- og rådsdirektiv (EU) 2022/2557 av 14. desember 2022 om kritiske enheters motstandsdyktighet (CER direktivet).

Europaparlaments- og rådsforordning (EU) 2019/881 av 17. april 2019 om ENISA (Den europeiske unions cybersikkerhetsbyrå), om cybersikkerhetssertifisering av informasjons- og kommunikasjonsteknologi.

Europaparlaments- og rådsforordning (EU) 2021/784 av 29. april 2021 om håndtering av spredning av terrorrelatert innhold på internett.

Europaparlaments- og rådsforordning (EU) 2022/2065 av 19. oktober 2022 om digitale tjenester i det indre marked.

Europaparlaments- og rådsforordning (EU) 2022/2554 av 14. desember 2022 om digital operasjonell motstandsdyktighet i finanssektoren.

Europaparlamentets- og rådsforordning (EU) 2024/1689 av 13. juni 2024 om fastsettelsen av et harmonisert regelverk om kunstig intelligens.

Europaparlaments- og rådsforordning (EU) 2024/2847 av 23. oktober 2024 om horisontale cybersikkerhetskrav til produkter med digitale elementer.

Europaparlaments- og rådsforordning (EU) 2025/38 av 19. desember 2024 om fastsettelse av tiltak for å styrke solidariteten og kapasiteten i Unionen til å oppdage, forberede seg på og reagere på trusler og hendelser innen cybersikkerhet.

Vedlegg 2: Liste med forkortelser som er brukt i utredningen

BFF = Beredskapssystem for forsvarssektoren, inngår sammen med Sivilt beredskapssystem i Nasjonalt beredskapssystem (NBS).

CER-direktivet = EUs direktiv om kritiske enheters motstandsdyktighet.

CERT = Computer Emergency Respone Team. Det kreves lisens fra Carnegie Mellon University for å bruke betegnelsen.

CSIRT = Computer Security Incident Respons Team. Generisk term som betyr det samme som CERT.

DEKSA = Direktoratet for eksportkontroll og sanksjoner. Underlagt Utenriksdepartementet.

DFD = Digitaliserings- og forvaltningsdepartementet.

DigDir = Digitaliseringsdirektoratet. Underlagt Digitaliserings- og forvaltningsdepartementet.

DSB = Direktoratet for samfunnssikkerhet og beredskap. Underlagt Justis- og beredskapsdepartementet.

DSS = Departementenes sikkerhets- og serviceorganisasjon. Underlagt Digitaliserings- og forvaltningsdepartementet.

EOS = Etterretnings-, overvåkings- og sikkerhetstjenestene (Etterretningstjenesten, Politiets sikkerhetstjeneste og Nasjonal sikkerhetsmyndighet).

FCKS = Felles cyberkoordineringssenter. Etablert 2017. Her møtes EOS-tjenestene og Kripos for informasjonsdeling, diskusjon ogkoordinering knyttet til håndtering av alvorlige cyberhendelser. NSM har administrativ ledelse av FCKS.

FD = Forsvarsdepartementet

FFI = Forsvarets forskningsinstitutt

FMA = Forsvarsmateriell

FO/S = Forsvarets overkommando/Sikkerhetsstaben. Delt i 2003 i FSA og NSM.

FSA = Forsvarets sikkerhetsavdeling. Forsvarssjefens rådgiver og utøver innen defensiv sikkerhet og operativ sikkerhet (militær kontraetterretning) i Forsvaret.

FSJ = Forsvarssjefen. Etatssjef for Forsvaret.

Havtil = Havindustritilsynet (tidligere Petroleumstilsynet). Underlagt Energidepartementet.

JD = Justis- og beredskapsdepartementet

KIKS = Kritisk infrastruktur og kritiske samfunnsfunksjoner

Kripos = Kriminalpolitisentralen. Særorgan i politiet. Underlagt Politidirektoratet.

NBS = Nasjonalt beredskapssystem, delt i Beredskapssystem for forsvarssektoren (BFF) og Sivilt beredskapssystem (SBS). Er hjemlet i beredskapsloven og samordnet med NATOs Crisis Response System Manual (NRSM).

NC3 = National Cyber Crime Center (Datakrimavdelingen i Kripos).

NCSC = Nasjonalt cybersikkerhetssenter (inngår som en avdeling i NSM). Etablert 2019. Et partnerskap mellom NSM og en rekke offentlige og private virksomheter knyttet til digital sikkerhet.

NESS = Nasjonalt etterretnings- og sikkerhetssenter. Her møtes EOS-tjenestene og Kripos for felles analyse og vurdering av etterretnings-, sabotasje-, terror- og påvirkningstrusselen (sammensatt virkemiddelbruk).

NIS-direktivet = EUs direktiv for høyt felles sikkerhetsnivå i nettverk og informasjonssystemer.

Nkom = Nasjonal kommunikasjonsmyndighet. Underlagt Digitaliserings- og forvaltningsdepartementet.

NorCERT = Nasjonal CERT for Norge. Etablert i 2006. Inngår i dag i NCSC og i sikkerhetsloven som den nasjonale responsfunksjon.

NorSIS = Norsk senter for informasjonssikring. Etablert i 2006. Fokus på rådgiving innen digital sikkerhet til allmennheten og små og mellomstore bedrifter. Fra 1. januar 2024 en del av NSM.

NSA = National Security Authority. Kontaktpunkt/funksjon i NATO-landene med ansvar knyttet til sikkerhet for NATO-gradert informasjon.

NSM = Nasjonal sikkerhetsmyndighet. Direktorat for forebyggende defensiv sikkerhet. Underlagt Justis- og beredskapsdepartementet og Forsvarsdepartementet.

NSR = Næringslivets sikkerhetsråd

NVE = Norges vassdrags- og energidirektorat. Underlagt Energidepartementet.

PST = Politiets sikkerhetstjeneste. Norges innenlands etterretningstjeneste (sikkerhetsetterretninger) og offensiv sikkerhetstjeneste. Underlagt Justis- og beredskapsdepartementet og Riksadvokaten.

RNB = Revidert nasjonalbudsjett.

SBS = Sivilt beredskapssystem, inngår sammen med Beredskapssystem for forsvarssektoren i Nasjonalt beredskapssystem (NBS).

SERTIT = Frivillig sertifiseringsordning for IT-sikkerhet i produkter og systemer. Etablert 1999. Administreres av NSM.

SKM = Sivil klareringsmyndighet. Ansvarlig for klareringssaker i sivil forvaltning, med unntak av for PST som er egen klareringsmyndighet. Klarerer etter avtale også for NSM. Direktorat underlagt Justis- og beredskapsdepartementet.

SRM = Sektorvise responsmiljøer. Håndteringskapasitet i den enkelte samfunnssektor til støtte for virksomhetene og NSM som nasjonal responsfunksjon. Skal være anerkjent av og ha en ansvarslinje til sektordepartement.

VDI = Varslingssystem for digital infrastruktur. System av sensorer som er plassert på internettforbindelsene til en rekke private og offentlige virksomheter. Hensikten er å varsle og verifisere dataangrep ved hjelp av skadevare. NSM har ansvar for drift og utvikling av systemet.

Vedlegg 3: Institusjoner og personer utvalget har møtt

Justis- og beredskapsdepartementet: departementsråd Heidi Heggenes, ekspedisjonssjef Unni Gunnes og avdelingsdirektør Annette Tjaberg.

Forsvarsdepartementet: departementsråd Frede Hermansen.

Utenriksdepartementet: departementsråd Torgeir Larsen og fagdirektør Kjell-Kåre Mikkelsen.

Digitaliserings- og forvaltningsdepartementet: departementsråd Christine Hamnen, ekspedisjonssjef Siri Halvorsen, avdelingsdirektør Christina Christensen, avdelingsdirektør Catharina Nes, fagdirektør Hilde Sverdrup Müller og utredningsleder Live Heltberg.

Energidepartementet: departementsråd Andreas H. Eriksen.

Nasjonal sikkerhetsmyndighet (NSM): direktør Arne Christian Haugstøyl og avdelingslederne Martin Albert-Hoff, Øyvind Karlstad Hageland, Geir Arild Engh-Hellesvik og Kristin Wist. I tillegg har utvalget møtt to tidligere direktører i NSM, Kjetil Nilsen og Lars Christian Aamodt.

Etterretningstjenesten: sjef Nils Andreas Stensønes.

Politiets sikkerhetstjeneste (PST): sjef Beate Gangås og avdelingsdirektør Inger Haugland.

Stortingets kontrollutvalg for EOS-tjenestene (EOS-utvalget): daværende leder Astri Aas-Hansen, utnevnt til Justis- og beredskapsminister 4. februar 2024 og direktør for EOS-utvalgets sekretariat Henrik Gudmestad Magnusson.

Forsvaret: forsvarssjef Eirik Kristoffersen og oberstløytnant Jan Heen.

Politidirektoratet: daværende politidirektør Benedicte Bjørnland og seksjonssjef Nicolay Bjertnæs Nakstad.

Kripos: assisterende direktør Ketil Haukaas og leder for Nasjonalt cyberkrimsenter (NC3) Olav Skard.

Direktoratet for samfunnssikkerhet og beredskap: direktør Elisabeth Aarsæther og avdelingsdirektør Elisabeth Longva.

Direktoratet for eksportkontroll og sanksjoner: direktør Harriet Berg.

Digitaliseringsdirektoratet: direktør Frode Danielsen og avdelingsdirektør Guri K. Lande.

Norges vassdrags- og energidirektorat (NVE): direktør Kjetil Lund og direktør for tilsyn og beredskap Kristian Markegård.

Havindustritilsynet: fagleder sikring Ingvild Klaveness og fagdirektør Finn Carlsen.

Nasjonal kommunikasjonsmyndighet: direktør John-Eivind Velure, sikkerhetsdirektør Svein Sundfør Scheie og fungerende seksjonssjef Sander Norrøne Ask.

Finanstilsynet: direktør Per Mathis Kongsrud, avdelingsdirektør Knut Haugan og seksjonssjef Olav Johannessen.

Equinor: Vice President Security Jan Aarvold, Lead EU Policy Adviser Ingvild Stub og Special Advisor Political and Public Affairs Global Tarjei Skirbekk.

Gassco: Senior Vice President Staff and Business support Randi Viksund og leder for Digital Governance and Security Alf Johan Grevstad.

Telenor Norge: myndighetskontakt Eirik Øwre Thorshaug og sikkerhetsdirektør Christer Eneroth.

Norges Bank: direktør Therese Steen.

BITS AS: daglig leder Eivind Gjemdal og avdelingsleder Brynjel Johnsen.

Mnemonic: Chief Executive Officer and Co-Founder Tønnes Ingebrigtsen og Manager, Governance, Risk & Compliance Gjermund Vidhammer.

Norwegian Cybersecurity Cluster: leder Sigrun Hanssen Bock og medlem Trond Solberg.

Fagforeningene i NSM: Fredrikke Henden Clark (Politiets fellesforbund), Christian Reusch (Parat) og Torgeir Vidnes (Tekna).

Politiets Fellesforbund: Kari Anne Kristiansen og Lasse Hekkås.

Flygeledernes forening: leder Robert Gjønnes.

Næringslivets sikkerhetsråd (NSR): direktør Odin Johannessen.

Fra akademia: Sissel Haugland Jore og Ole Andreas Hegdal Engen, begge professorer ved Institutt for sikkerhet, økonomi og planlegging ved Universitetet i Stavanger.

Tidligere direktør Frode Forfang, som på oppdrag fra Justis- og beredskapsdepartementet utreder oppgavefordelingen innenfor personellsikkerhet.

Vedlegg 4: Grunnleggende nasjonale funksjoner (GNF) og kritiske samfunnsfunksjoner

Kritiske samfunnsfunksjoner[170]	**Grunnleggende nasjonale funksjoner (GNF) etter sikkerhetsloven**[171]
Elektronisk kommunikasjonsnett og –tjenester (Ekom)	– Evne til å ivareta kommunikasjonstjenester basert på norsk nummerplan (tale og tekst) – Evne til å ivareta grunnleggende internettilgang – Evne til å ivareta datalagring og prosesseringskapasitet i Norge – Krisekommunikasjon til befolkningen
IKT-sikkerhet i sivil sektor	
Satellittbasert kommunikasjon og navigasjon	– Satellittbasert overvåkning og jordobservasjon – Romovervåking – Posisjonsbestemmelse, navigasjon og tidsbestemmelse – Satellittbasert kommunikasjon
Kraftforsyning	– Nasjonal kraftforsyning – Transport av gass i rør til Europa – Kontroll med utvinning av petroleum på norsk sokkel
Vann- og avløp	
Forsyningssikkerhet	– Matvareforsyning – Trygg vannforsyning
Transport	– Transport
Finansiell stabilitet	– Sikre samfunnets evne til å formidle finansielle tjenester
Helse og omsorg	– Helseberedskap – Kritiske offentlige ytelser til befolkningen – Evne til å finansiere offentlig virksomhet

[170] Prop. 1 S (2016–2017) for budsjettåret 2017 under Justis- og beredskapsdepartementet, Tabell 1.7 side 35 og 36.

[171] Oversikt over innmeldte grunnleggende nasjonale funksjoner – Nasjonal sikkerhetsmyndighet Rekkefølgen på listen av GNFer er i noen grad tilpasset listen med kritiske samfunnsfunksjoner.

Lov og orden	– Lov og orden – Nasjonale sikkerhetstjenester – Gjennomføring av frie, direkte og hemmelige valg til Stortinget, kommunestyrer, fylkesting og Sametinget – Norsk utenrikstjeneste
Redningstjeneste	
Styring og kriseledelse	– Alle departementenes virksomhet, handlefrihet og beslutningsdyktighet
Forsvar	– Evne til etterretning, situasjonforståelse og rettidig varsling – Evne til å håndtere episoder og sikkerhetspolitiske kriser og nødvendig forsvare norsk eller alliertes territorium. – Evne til kommando og kontroll over norske og allierte styrker – Evne til beskyttelse av norske og allierte styrker, samfunnskritiske funksjoner, samt kritiske digitale funksjoner for Forsvaret. – Sikre at Forsvaret og forhåndsutpekte kritiske brukere får tilgang til tilstrekkelig drivstoff
Natur og miljø	

Vedlegg 5: Utdrag av NSMs hovedinstruks og DSBs instrukser

Tema	Hovedinstruks for NSM (3. mai 2019)	Instrukser for DSB
Formål	Instruksen angir NSMs myndighet og ansvarsområder samt departementenes forutsetninger og krav til virksomhetens systemer, rutiner og styringsprosesser.	Instruksens virkeområde er styring og kontroll i DSB. Formålet med instruksen er å beskrive DSBs samfunnsoppdrag.
Risikobilde	«NSM skal vedlikeholde et **helhetlig risikobilde** innen forebyggende sikkerhet og produsere en årlig rapport om sikkerhetstilstanden, blant annet basert på trusselvurderinger fra E og PST. NSM skal foreslå tiltak for å bedre sikkerhetstilstanden». (Hovedinstruksen, s. 4)	«DSB skal ha **oversikt over risiko** og sårbarhet i samfunnet, være pådriver i arbeidet med å forebygge ulykker, kriser og andre uønskede hendelser, og bidra til god beredskap og effektiv ulykkes- og krisehåndtering». (DSBs Hovedinstruks, s. 2)
IKT-sikkerhet **Digital sikkerhet**	«NSM skal som det nasjonale fagmiljøet for digital sikkerhet, understøtte og bidra til utøvelsen av JDs og FDs ansvar på det digitale sikkerhetsområde. Ref. JDs samordningsansvar for digital sikkerhet i sivil sektor (kgl.res. 10. mars 2017)». «NSM skal vedlikeholde et særskilt risikobilde for digital sikkerhet som omfatter statssikkerhet, samfunnssikkerhet og individsikkerhet, og skal foreslå tiltak, gi anbefalinger og fremme forhold til krav innen digital sikkerhet i samfunnet, samt følge opp med råd og veiledning». «NSM skal koordinere arbeidet mellom myndigheter som har en rolle innenfor forebyggende digital sikkerhet, og skal legge til rette for hensiktsmessig samhandling mellom disse ...». (Hovedinstruksen, s. 3)	«IKT-sikkerheten er en integrert del av arbeidet med samfunnssikkerhet». (Samfunnssikkerhetsinstruksen s. 1)

Samarbeid med andre aktører	«NSM skal samarbeide med andre relevante aktører innen forebyggende sikkerhet. NSM skal medvirke til at ansvarsforhold er avklart. Det skal særlig søkes å unngå overlapping i myndighetsutøvelse. Dersom det ikke oppnås hensiktsmessig avklaring av ansvarsforhold eller det er andre forhold av betydning vedrørende samarbeid med andre relevante aktører, skal saken forelegges JD og FD». (Hovedinstruksen, s. 3)	Fra samfunnssikkerhetsinstruksen kap. VI: «JD har en generell samordningsrolle på samfunnsikkerhetsområdet. … DSB understøtter departementet i samordningsrollen». «JD har ansvar for et helhetlig, systematisk og risikobasert arbeid med samfunnssikkerhet på nasjonalt nivå på tvers av alle sektorer». Dette innebærer blant annet å «sørge for at problemstillinger på tvers av flere sektorer og kritiske samfunnsfunksjoner blir håndtert og bistå departementene med å avklare ansvars-forhold».

Forebyggende sikkerhet / samordning	«NSM er på vegne av JD og FD tilsynsmyndighet og fagmyndighet innenfor **forebyggende sikkerhet** i henhold til sikkerhetsloven». (Hovedinstruksen, s. 3) «NSM skal bidra til å styrke samfunnets kunnskap, forståelse, motivasjon og evne til å ivareta forebyggende sikkerhet, herunder digital sikkerhet på en best mulig måte». (Hovedinstruksen s. 4) Sjef NSM: utøve et overordnet og sektorovergripende ansvar for forebyggende sikkerhetsarbeid i hht. Sikkerhetsloven. (Hovedinstruksen, s. 5) Sjef NSM: er rådgiver i spm. om forebyggende tiltak mot sikkerhetstruende virksomhet som kan ramme nasjonale sikkerhetsinteresser. (Hovedinstruksen, s. 5)	DSB har en samordningsrolle og skal bistå JDs «ansvar for et helhetlig, systematisk og risikobasert samfunnssikkerhetsarbeid på tvers av sektorer». (Samfunnssikkerhetsinstruksen kap. VI). «DBS skal ha oversikt over risiko og sårbarhet i samfunnet, være pådriver i arbeidet med å **forebygge ulykker, kriser og andre uønskede hendelser**, og bidra til god beredskap og effektiv ulykkes- og krisehåndtering». (Hovedinstruksen s. 3). Samordningsrolle innenfor totalforsvarsområdet, samt ivareta og videreutvikle DSBs samarbeid med relevante enheter i Forsvaret. (Se Hovedinstruksen s. 4) Bidra i arbeidet med å oppdatere SBS. (Se Hovedinstruksen s. 4) Tilsyn med departementenes arbeid med samfunnssikkerhet i tråd med samfunnssikkerhetsinstruksen. (Se Hovedinstruksen s. 4)

Naturhendelser vs. villede handlinger	Sikkerhetslovens § 1-5 andre ledd: «definisjon av sikkerhetstruende virksomhet: *tilsiktede handlinger som direkte eller indirekte kan skade nasjonale sikkerhetsinteresser*»	«Samfunnssikkerhet defineres som samfunnets evne til å verne seg mot og håndtere hendelser som truer grunnleggende verdier og funksjoner og setter liv og helse i fare. Slik hendelser kan være utløst av naturen, være et utslag av tekniske eller menneskelige feil eller bevisste handlinger». (Se veileder til samfunnssikkerhetsinstruksen s. 4, NOU 2006: 6 Når sikkerheten er viktigst, Meld. St. 10 (2016–2017) Risiko i et trygt samfunn, DSB 2016 Samfunnets kritiske funksjoner. Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?)
NATO	«NSM er Norges representant i internasjonale fora, herunder NATO, innen forebyggende sikkerhet, og i bi- og multilateralt samarbeid på fagområdet. NSM skal representere Norge i NATOs sikkerhetskomité.»	«DSB skal bidra til å ivareta norske interesser i NATOs sivile beredskapsarbeid». (Se Hovedinstruksen s. 6)

Reguleringer vi har sett på i sammenligningen:

– DSBs Hovedinstruks og Instruks om DBSs koordinerende rolle (24. juni 2005)
– Veileder til samfunnssikkerhetsinstruksen fra 3.9.2019.
– Samfunnssikkerhetsinstruksen (1. september 2017)
– NSMs Hovedinstruks
– Sikkerhetsloven

Utgitt av: Justis- og beredskapsdepartementet

Bestilling av publikasjoner:
Departementenes sikkerhets- og serviceorganisasjon
publikasjoner.dep.no
Telefon: 22 24 00 00
Publikasjoner er også tilgjengelige på:
www.regjeringen.no
Publikasjonskode: G-0460 B

Trykk: Departementenes sikkerhets- og
serviceorganisasjon 04/2025 – opplag 80