DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Meld. St. 9

(2022–2023)

Melding til Stortinget

Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet

Så åpent som mulig, så sikkert som nødvendig

DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Meld. St. 9

(2022–2023)

Melding til Stortinget

Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet

Så åpent som mulig, så sikkert som nødvendig

Innhold

DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT

Meld. St. 9

(2022–2023)

Melding til Stortinget

Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet

Så åpent som mulig, så sikkert som nødvendig

Tilråding fra Justis- og beredskapsdepartementet 9. desember 2022, godkjent i statsråd samme dag.
(Regjeringen Støre)

1 Sammendrag

Den sikkerhetspolitiske situasjonen gjør det nødvendig med kraftfulle tiltak for å ivareta nasjonal sikkerhet. Russlands angrep på nabolandet Ukraina 24. februar 2022 har skapt en helt ny situasjon i Europa. Sammensatte trusler er egnet til å ramme samfunnet bredt, og ivaretagelse av nasjonal sikkerhet er stadig mer krevende fordi dagens utfordringsbilde er komplekst og berører alle samfunnsområder.

De siste årene har det vært flere enkelteksempler som har vist hvor viktig det er å ha både regulatoriske virkemidler og evne til å tenke langsiktig for å sikre nasjonal kontroll og nasjonal sikkerhet. Salget av det norskregistrerte selskapet Bergen Engines AS i 2021 er et slikt eksempel. Selskapet var produsent og leverandør av motorer og generatorer til både sivile sektorer og forsvarssektoren i Norge og andre allierte land. En av de potensielle kjøperne var et russisk kontrollert selskap. Etter stor oppmerksomhet politisk og i media, og en vurdering av salget opp mot sikkerhetsloven, ble transaksjonen stoppet. Saken er et eksempel på hvor viktig det er at staten har virkemidler både til å avdekke og for å kunne gripe inn der det er nødvendig. I 2014 ble det foreslått å selge deler av statens aksjer i Kongsberg Gruppen, en viktig aktør innen forsvarsproduksjon. Saken vakte stor politisk debatt, og salget ble ikke gjennomført.

Disse sakene illustrerer hvor viktig nasjonal kontroll er som virkemiddel for å ivareta nasjonal sikkerhet. Regjeringen mener at staten må ta en aktiv rolle for å sikre nasjonal kontroll og ivareta norsk sikkerhet. Denne stortingsmeldingen gir uttrykk for dette.

Konsesjonslovgivningen har en lang historie i Norge. Foruten å sikre eier- og bruksforhold som samfunnet er mest tjent med, bidrar den også til bosetting og langsiktig og god forvaltning av landbruksressursene. Regjeringen mener denne lovgivningen er helt nødvendig i et langsiktig perspektiv.

For kort tid siden kjøpte staten Meraker Brug. Med sitt areal på om lag 1,2 millioner mål var dette en av landets største privateide eiendommer. Eiendommen utgjør 90 prosent av arealet i Meråker kommune. Å sikre nasjonalt eierskap til enkelte eiendommer er et viktig virkemiddel for å sikre nasjonal kontroll.

En av statens viktigste oppgaver er å ivareta nasjonal sikkerhet. Regjeringen vil i denne meldingen tydeliggjøre strategisk retning, prioriteringer og tiltak for å ivareta nasjonal og digital sikkerhet på utvalgte områder. Regjeringens strategiske retning fremheves nedenfor. Tiltak som fremgår av meldingen bygger opp under den strategiske retningen.

Regjeringen vil bruke nasjonalt eierskap og kontroll for å styrke nasjonal sikkerhet

Vi står overfor et skjerpet risikobilde og utfordres av stater med sikkerhetspolitiske ambisjoner som ikke samsvarer med våre nasjonale sikkerhetsinteresser. Regjeringen vil forsterke innsatsen for å styrke samfunnets kollektive motstandskraft. Nasjonal kontroll på områder som er strategisk viktige for nasjonal sikkerhet er en meget viktig del av dette. Nasjonalt eierskap er et av flere virkemidler for å oppnå dette. Regjeringen ønsker økt nasjonal kontroll for å bidra til økt kompetanse, forutsigbarhet og tillit, som grunnlag for verdiskapning og fremtidige investeringer i Norge. Virkemidler for å oppnå ulik grad av nasjonal kontroll må tilpasses og avveies mot andre viktige samfunnshensyn i en demokratisk stat. Det kan være hensyn som et fritt og åpent samfunn eller kunnskaps-, nærings-, handels- og sikkerhetspolitiske og økonomiske. Risikoaksept vil være en del av disse vurderingene. Prinsippet «så åpent som mulig, så sikkert som nødvendig» understreker disse avveiningene.

Regjeringen vil tilrettelegge for økt oversikt over verdier som er strategisk viktige for nasjonal sikkerhet

En grunnleggende forutsetning for å ivareta nasjonal sikkerhet er at myndighetene har oversikt over hvilke verdier og virksomheter som har betydning for nasjonal sikkerhet. I lov om nasjonal sikkerhet (sikkerhetsloven) er det en egen metodikk for hvordan våre verdier skal kartlegges. Kartleggingen av grunnleggende nasjonale funksjoner gir departementene oversikt over virksomheter og verdier som har avgjørende og vesentlig betydning for statens evne til å ivareta nasjonale sikkerhetsinteresser. Virksomhetene eller verdiene som har avgjørende betydning blir underlagt sikkerhetsloven med krav til å iverksette forebyggende sikkerhetstiltak. Kartleggingen er kompleks, og viser omfattende gjensidige avhengigheter mellom virksomheter innenfor samme samfunnssektor, på tvers av sektorer og at avhengigheter endres relativt ofte. Særlig gjør dette seg gjeldende for digitale informasjonssystemer og infrastrukturer. Et målrettet og effektivt forebyggende sikkerhetsarbeid krever prioritering av arbeidet med å oppdatere og forbedre kartleggingen som gjøres i tråd med bestemmelsene i sikkerhetsloven. I dette arbeidet vil en også måtte vurdere og prioritere tiltak ut fra hvor kostnadskrevende og effektive forebyggende tiltak vil kunne være. Regjeringen vil prioritere arbeidet med å revidere og oppdatere oversikter i alle samfunnssektorer.

Regjeringen vil i tillegg vurdere hvordan vi kan få bedre oversikt over verdier som ikke dekkes av sikkerhetsloven, men som likevel kan ha betydning for vår nasjonale sikkerhet. Dette kan være fysiske, digitale og andre verdier. Samtidig må en oversikt over verdier ses i sammenheng med trussel- og risikobildet, for å forstå egne sårbarheter og for å kunne ivareta egen sikkerhet. Regjeringen vil i denne meldingen presentere tiltak for ytterligere å styrke oversikten over verdier av betydning for nasjonal sikkerhet. Med en god oversikt over våre verdier vil myndighetene bedre kunne vurdere relevante virkemidler for å ivareta nasjonal sikkerhet, blant annet gjennom forebyggende sikkerhetstiltak med hjemmel i sikkerhetsloven, bruk av øvrig relevant regelverk og nasjonalt eierskap.

Regjeringen vil aktivt bruke regulering som virkemiddel for å ivareta nasjonal sikkerhet

Regjeringen er opptatt av at sikkerhetsloven er tilpasset det til enhver tid gjeldende trussel- og risikobildet og vil derfor fremme forslag til justeringer i loven når det er nødvendig. Regjeringen ser også behov for å gjennomgå annet relevant regelverk for å forsikre seg om at hensyn til nasjonal sikkerhet inngår som vurderingskriterium, der det er relevant. Videre ser regjeringen behov for å styrke lovgivningen på enkelte områder for å kunne ivareta nasjonal sikkerhet, blant annet knyttet til digital sikkerhet og datasentre. Regjeringen vurderer å fremme et forslag til lov om digital sikkerhet for å ansvarliggjøre virksomheter og sikre gjennomføring av nasjonale råd og anbefalinger. Regjeringen har også oppnevnt et offentlig utvalg som skal utrede behovet for regelverk

eller en ordning for å screene økonomisk aktivitet mot virksomheter som ikke er underlagt sikkerhetsloven.

Regjeringen vil styrke samfunnets motstandskraft og robusthet gjennom økt kompetanse og kunnskap om forhold av betydning for nasjonal sikkerhet og digital motstandskraft

Kompetanse og kunnskap om risiko, trusler, sårbarheter og effektive mottiltak er en forutsetning for å kunne beskytte våre verdier mot uønskede hendelser. Regjeringen vil synliggjøre kompetansebehovene i samfunnet og legge til rette for langsiktig forskning av betydning for nasjonal sikkerhet. Regjeringen vil legge til rette for at privatpersoner, virksomheter og myndigheter er bevisst sikkerhetsutfordringene og har nødvendig kunnskap om hvordan de kan møte dem på en god måte. Tiltakene som fremmes i denne meldingen vil bidra til å øke kompetanse- og kunnskapsnivået i samfunnet.

2 Innledning

Regjeringen vil i denne meldingen tydeliggjøre strategisk retning, prioriteringer og tiltak for å ivareta nasjonal sikkerhet på utvalgte områder. Strategisk viktige bedrifter, naturressurser, infrastrukturer og teknologier vies særskilt oppmerksomhet. Regjeringen vil også trekke frem utvalgte områder innenfor digital sikkerhet. Denne meldingen er avgrenset mot det brede samfunnssikkerhets- og beredskapsperspektivet.

Regjeringen er i meldingen opptatt av å forsterke innsatsen for å styrke samfunnets kollektive motstandskraft. Kunnskap, kompetanse og bevissthet på alle nivåer i samfunnet er avgjørende for å oppnå dette. Det dreier seg om forståelse av trussel- og risikobildet, hvorfor nasjonal sikkerhet er viktig, hvordan det treffer den enkelte og hvilke relevante tiltak som bør gjennomføres. I Norge har vi høy grad av tillit – både til hverandre og myndighetene. Høy grad av tillit gjør oss mer motstandsdyktige mot andre staters påvirkningsoperasjoner, som kan ha som formål å skape politisk og sosial uro. Men også i Norge kan denne tilliten være under press, og den kan være skjevt fordelt mellom ulike grupper i befolkningen. Vi må derfor styrke forståelsen, kunnskapen og bevisstheten om både trusler og tiltak i hele befolkningen. Dersom statens virkemidler ikke er forståelige og forutsigbare, og befolkningen har mangelfull kunnskap, kan det over tid undergrave tilliten til myndighetene. I et åpent samfunn som Norge må vi ta høyde for at ulike typer av lovlig aktivitet kan misbrukes, blant annet til etterretningsformål. Det vil være ulike hensyn som står mot hverandre, og en restrisiko vil alltid finnes.

Ved siden av å initiere, utvikle og gjennomføre tiltak gjennom egne virkemidler har Justis- og beredskapsdepartementet en samordnings- og pådriverrolle for forebyggende nasjonal sikkerhet og digital sikkerhet på sivil side. Dette innebærer at Justis- og beredskapsdepartementet blant annet skal utforme regjeringens politikk, herunder etablere nasjonale krav og anbefalinger, på tvers av ulike samfunnsområder. Forsvarsdepartementet har det overordnede ansvaret for forebyggende nasjonal sikkerhet og digital sikkerhet i forsvarssektoren.

Nedenfor gis det en omtale av et skjerpet trussel- og risikobilde, samt hva som legges i begrepene nasjonal kontroll og digital sikkerhet. I kapittel 3 omtales virkemidler for å styrke nasjonal kontroll og bygge digital motstandskraft. Nasjonal kontroll over verdier av betydning for nasjonal sikkerhet følger i kapittel 4. Kapittel 5 omtaler økonomiske og administrative konsekvenser.

2.1 Et skjerpet trussel- og risikobilde

Vi står overfor et skjerpet trussel- og risikobilde og utfordres av stater med sikkerhetspolitiske ambisjoner som ikke samsvarer med våre nasjonale sikkerhetsinteresser. Økt konfrontasjonsvilje hos ikke-vestlige stater, russisk bruk av militærmakt og energi som våpen er eksempler på dette. Invasjonen av Ukraina har skapt varige endringer i forholdet mellom Russland og vestlige land.

Økt globalisering, stormaktsrivalisering og stadige endringer i den sikkerhetspolitiske situasjonen påvirker i stor grad det nasjonale trusselbildet og gir oss sikkerhetsmessige utfordringer. Nordområdenes økte strategiske betydning og vår rolle som energileverandør gjør at Norge er særlig utsatt for etterretnings- og sabotasjevirksomhet og annen uønsket aktivitet. I tillegg påvirker klimaendringene nasjonal sikkerhet over tid. Videre fremgår det av perspektivmeldingen at det årlige budsjettmessige handlingsrommet vil reduseres i kommende tiår, sammenlignet med foregående.[1]

Tradisjonelle skillelinjer mellom fred, krise og væpnet konflikt er blitt mindre tydelige. Statlige aktører som Russland og Kina utøver ofte aktivitet som i utgangspunktet kan være lovlig virksomhet for å fremme egne strategiske mål. Dette fremstår som en del av normalbildet, men samtidig kan aktiviteten skade vår nasjonale sikkerhet. Vi må ta høyde for at enkelte stater forsøker å påvirke poli-

[1] Meld. St. 14 (2020–2021) *Perspektivmeldingen 2021.*

Figur 2.1 Vi står overfor et skjerpet trussel- og risikobilde.

Foto: NSM

tiske beslutninger, meningsdannelse og ordskiftet i Norge. Diplomatiske, informasjonsmessige, militære, økonomiske, finansielle, etterretningsmessige og juridiske virkemidler fra enkelte stater kan enkeltvis eller i kombinasjon utgjøre sammensatte trusler som rettes mot Norge. De siste årene har trusler knyttet til utenlandske investeringer og oppkjøp som kan benyttes for å få innsikt i og tilgang til teknologi og ressurser av strategisk betydning, blitt tydeligere.

Stadig flere verdier av betydning for nasjonal sikkerhet forvaltes og behandles i det digitale rom. Digitalisering og teknologiutvikling medfører økt effektivisering og fornyelse, men introduserer samtidig nye sårbarheter, avhengigheter og konsentrasjonsrisiko. Dette kan utnyttes av en trusselaktør og må derfor håndteres. Den raske utviklingstakten og endringene i den sikkerhetspolitiske situasjonen gjør det stadig mer krevende for virksomheter å opprettholde et forsvarlig sikkerhetsnivå gjennom hele krisespennet.

Boks 2.1 Sammensatte trusler

Sammensatte trusler er en betegnelse på strategier for konkurranse og konfrontasjon under terskelen for direkte væpnet konflikt, som kan kombinere diplomatiske, informasjonsmessige, militære, økonomiske, finansielle, etterretningsmessige og juridiske virkemidler for å nå strategiske målsettinger. Sammensatte trusler kan forekomme i sikkerhetspolitiske gråsoner, der formålet er å skape splid og destabilisering. Virkemiddelbruken kan være bredt distribuert og kombinere åpne, fordekte og skjulte metoder. Virkemiddelbruken kan være rettet mot konkrete aktiviteter eller situasjoner, eller være innrettet mer langsiktig for å skape tvil, undergrave tillit og ved dette svekke våre demokratiske verdier. Sammensatte trusler er i sin natur komplekse og utfordrer tidlig varsling, omforent situasjonsforståelse samt effektiv og samordnet håndtering.

Figur 2.2 Digitaliseringen introduserer nye sårbarheter og risikoer.

Foto: NSM

2.2 Nasjonal kontroll og digital sikkerhet

Nasjonal kontroll

Nasjonal kontroll er ikke et mål i seg selv, men ett av flere virkemidler for å ivareta nasjonal sikkerhet.

Nasjonal kontroll over virksomheter og verdier som har betydning for nasjonal sikkerhet kan oppnås gjennom

- reguleringer i lov eller forskrift, for eksempel sikkerhetsloven med forskrifter, som pålegger virksomheter plikter.
- helt eller delvis statlig eierskap.
- helt eller delvis nasjonalt eierskap, som omfatter virksomheter utover staten, som kommune og fylkeskommune, i tillegg til privat norsk eierskap.
- tilstrekkelig oversikt hos myndighetene over verdier som har betydning for nasjonal sikkerhet, enten de er underlagt sikkerhetsloven eller ikke.
- offentlig-privat, sivil-militært og internasjonalt samarbeid.
- råd og veiledning til aktører som eier verdier av betydning for nasjonal sikkerhet.
- ulike kombinasjoner av ovennevnte.

Boks 2.2 Nasjonal sikkerhet

Nasjonal sikkerhet, slik begrepet er benyttet i denne meldingen, er statens evne til å ivareta nasjonale sikkerhetsinteresser. De nasjonale sikkerhetsinteressene er definert i sikkerhetsloven § 1-5 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 og e) samfunnets grunnleggende funksjonalitet og befolkningens grunnleggende sikkerhet.

Regjeringen vil styrke den nasjonale kontrollen gjennom en mer aktiv bruk av tilgjengelige virkemidler. Regjeringen vil prioritere å forbedre oversikten over virksomheter og verdier som har betydning for nasjonal sikkerhet, bruke virkemidler som relevant regelverk og nasjonalt eierskap, og øke kunnskapsnivået i samfunnet om risiko, trusselaktører og forebyggende sikkerhetsarbeid.

Nasjonal kontroll som virkemiddel må brukes på en slik måte at det bidrar til forutsigbarhet og tillit, og at det ikke fører til unødvendige begrensninger for verdiskapning og utenlandske investeringer i Norge, eller for norsk markedsadgang i utenlandske markeder. Nasjonal kontroll som begrenser utenlandsk aktivitet i Norge kan medføre politiske og økonomiske kostnader for det norske samfunnet, og berøre utenriks- og handelspolitiske hensyn og samarbeidet med andre land. Det er derfor viktig å ha en tilnærming som avveier sikkerhet og kontroll opp mot andre viktige samfunnshensyn, som for eksempel et fritt og åpent samfunn eller behovet for å gi næringsaktører best mulig rammevilkår og forutsigbarhet. Kost-nytte og risikoaksept vil være en del av disse vurderingene. Sikkerhetslovens formålsbestemmelse understreker at «sikkerhetstiltak [skal] gjennomføres i samsvar med grunnleggende rettsprinsipper og verdier i et demokratisk samfunn».

Digital sikkerhet

Digitalisering bidrar til bedre tjenester, mer effektiv ressursbruk og produktivitetsøkning i samfunnet. Digitaliseringen bringer også verden tettere sammen. Digitaliseringens bakside er at vi blir mer sårbare. Vårt samfunn er i dag helt avhengig av at kritiske samfunnsfunksjoner fungerer. Det igjen forutsetter at digitale systemer som understøtter disse kritiske samfunnsfunksjonene virker overalt og hele tiden. Men digitale systemer blir stadig mer komplekse, og endringstakten er høy. Med et skjerpet trusselbilde og et økt antall digitale angrep, er det desto viktigere med forebyggende sikkerhetsarbeid. Regjeringen vil derfor styrke samfunnets kollektive motstandskraft mot digitale trusler.

Boks 2.3 «Bergen Engines-saken»

Rolls-Royce plc varslet 15. desember 2020 norske myndigheter om at de ville starte en prosess med å selge det norskregistrerte selskapet Bergen Engines AS. Transmashholding Group (TMH Group) var en av de potensielle kjøperne, og kjøpet ble planlagt gjennomført av TMH International AG, et sveitsiskregistrert selskap som er 100 prosent eid av russiskregistrerte TMH Group. Rolls-Royce offentliggjorde 4. februar 2021 signeringen av en avtale med TMH om planlagt salg av Bergen Engines AS.

Bergen Engines AS er produsent og leverandør av blant annet motorer og generatorer til både sivil og militær sektor i Norge og flere allierte land, blant annet USA og Nederland. Et salg av Bergen Engines AS ville innebære overføring av virksomhetens teknologi, kompetanse, materiell, faste eiendommer, kundeportefølje og kontrakter om service- og vedlikeholdsavtaler. På bakgrunn av informasjonen om transaksjonsprosessen startet norske myndigheter et arbeid for å kartlegge alle forhold i tilknytning til det mulige salget av Bergen Engines AS.

8. mars 2021 ble Rolls-Royce varslet av Nasjonal sikkerhetsmyndighet om at norske myndigheter hadde til vurdering om transaksjonen skulle stanses i medhold av sikkerhetsloven. Videre at norske myndigheter forutsatte at en eventuell kunnskapsoverføring i tilknytning til selskapsgjennomgang (due diligence) og beslektet aktivitet ble stanset inntil dette var avklart. Rolls-Royce bekreftet 12. mars 2021 at både transaksjonsprosessen og all kunnskapsoverføring til TMH var midlertidig stanset i påvente av en endelig avgjørelse fra norske myndigheter. Også TMH bekreftet det samme 15. mars 2021.

26. mars 2021 fattet norske myndigheter vedtak med hjemmel i sikkerhetslovens § 2-5 første ledd, at Rolls-Royce plc og deres datterselskaper ble pålagt å stanse salget av aksjene i det norske selskapet Bergen Engines AS til selskaper i TMH. Vedtaket stanset enhver overføring av aksjer, eiendeler, eiendom, industriell eller teknologisk informasjon eller andre rettigheter i Bergen Engines AS til TMH. Bergen Engines AS ble senere solgt til britiske Langley Holdings.

Figur 2.3 NSM har registrert en markant vekst i antall digitale angrep.

Foto: Shutterstock

Digital sikkerhet har utviklet seg fra i hovedsak å være et teknisk fagområde til å bli et globalt strategisk tema. Digital sikkerhet omfatter både tekniske og administrative sikringstiltak, og innebærer beskyttelse av både systemer og informasjonen i disse. Digital sikkerhet handler derfor om beskyttelse av «alt» som er sårbart fordi det er koblet til eller på annen måte er avhengig av informasjons- og kommunikasjonsteknologi.

På strategisk nivå dreier digital sikkerhet seg om sikkerhetspolitikk, hvor utfordringer i stor grad må løses gjennom internasjonalt, sivil-militært og offentlig-privat samarbeid. Enkelte staters brede virkemiddelbruk som kan være i strid med våre nasjonale sikkerhetsinteresser understreker betydningen av at digital sikkerhet er en integrert del av øvrig sikkerhetsarbeid.

Krigen i Ukraina og eksplosjonene på gassrørledninger i Østersjøen har aktualisert viktigheten av arbeidet med sikkerhet, herunder digital sikkerhet. Som følge av disse hendelsene har beredskapen mot blant annet digitale angrep som kan ramme petroleumssektoren eller andre kritiske virksomheter økt. I tillegg er kraft og ekom eksempler på infrastrukturer hvor digital motstandskraft er av stor betydning. I arbeidet med digital sikkerhet er det særlig viktig å identifisere avhengigheter, arbeide bredt med sikkerhet og se tiltak i sammenheng. Strategisk viktig infrastruktur blir særlig viktig i dette bildet og omtales nærmere i punkt 4.3.

Samfunnets samlede digitale sikkerhet avhenger av det forebyggende arbeidet i hver enkelt virksomhet. Virksomhetsledere er ansvarlige for at virksomheten evner å forebygge og håndtere hendelser. I tråd med Justis- og beredskapsdepartementets samordningsansvar for digital sikkerhet på sivil side, gir myndighetene nasjonale råd og anbefalinger og stiller ressurser tilgjengelig så langt det er mulig når en alvorlig hendelse inntreffer. Nasjonal sikkerhetsmyndighet (NSM) er det nasjonale fagmiljøet for digital sikkerhet. Nasjonalt cybersikkerhetssenter (NCSC) er en del av NSM og bidrar til å beskytte grunnleggende nasjonale funksjoner (GNF), offentlig forvaltning og næringsliv mot digitale angrep. Politiets sikkerhetstjeneste (PST) og det øvrige politi er også sentrale aktører, og Nasjonalt cyberkrimsenter (NC3) ved Kripos bidrar inn i arbeidet både nasjonalt og internasjonalt. Etterretningstjenesten (E-tjenesten) skal bidra til å forebygge, avdekke og motvirke utenlandske trusler mot Norge og norske interesser, herunder i det digitale domenet.

De siste årene er det etablert et godt kunnskapsgrunnlag om digital sikkerhet, slik at både virksomheter og myndigheter er bedre i stand til å iverksette riktige tiltak. Imidlertid har NSM registrert en markant vekst i antall digitale angrep

de siste årene. NSM har uttalt at omlag 80 prosent av hendelsene de håndterer kunne vært unngått hvis grunnleggende sikkerhetstiltak var blitt fulgt. Det er derfor viktig å øke bevisstgjøringen og styrke det forebyggende arbeidet. Samtidig må virksomheter og myndighetene ha kompetanse og kapasitet til å avdekke og håndtere uønskede hendelser.

3 Virkemidler for å styrke nasjonal kontroll og bygge digital motstandskraft

Staten har en rekke virkemidler for å ivareta nasjonal kontroll og bygge digital motstandskraft. Virkemidlene må vurderes både enkeltvis og i sammenheng, og de vil variere, avhengig av hvor man befinner seg i krisespennet, hvor stor grad av kontroll som er ønskelig i ulike sammenhenger og eventuelle kostnader knyttet til dette. Virkemidler for å ivareta nasjonal kontroll må også vurderes i lys av Norges folkerettslige forpliktelser, herunder frihandelsavtaler med tredjeland. Statlige trusselaktører vil, etter hvert som vi styrker vår evne til å motstå deres virkemidler, tilpasse sin bruk av virkemidler som kan ramme våre nasjonale sikkerhetsinteresser. Våre tiltak må derfor tilpasses og utvikles over tid for å møte utfordringene.

På generelt grunnlag er det viktig å gi tilstrekkelig prioritet til virkemidler som har en forebyggende effekt. Hendelseshåndtering vil ofte være dyrere og mer inngripende enn forebygging. Forebyggingsperspektivet er viktig på alle nivåer i samfunnet, fra enkeltmennesker opp til virksomhets- og myndighetsnivå. PST, politiet og NSM har et særskilt ansvar her. Samtidig må samfunnet ha tilstrekkelige ressurser for å håndtere hendelser når de først har inntruffet.

Endrede økonomiske rammer stiller høyere krav til prioriteringer og effektiv ressursutnyttelse. Det innebærer at prioritering av den forebyggende delen av arbeidet blir viktigere og vil gi krevende avveininger mellom ulike hensyn, behov og ønsker. Tiltak som økt nasjonalt eierskap og kontroll gjennom oppkjøp av strategisk viktige bedrifter, naturressurser eller infrastrukturer har for eksempel en direkte kostnad. Behovet for nasjonal kontroll av hensyn til nasjonal sikkerhet kan også medføre kostnader for samfunnet og næringslivet. For eksempel dersom dette medfører økt rapporteringsplikt eller legger begrensninger på privat eierskap, tilgang til internasjonal kapital, næringslivssamarbeid og forholdet til andre stater. Norge har forpliktelser gjennom EØS-avtalen og andre folkerettslige avtaler, som WTO-regelverket og frihandelsavtaler, som må ivaretas dersom man ønsker å innføre eierskapsbegrensninger. Risikoaksept er et annet viktig element, herunder en vurdering av tilstrekkelig nasjonal kontroll og digital sikkerhet. Samfunnets ressursbruk og forholdsmessighet for å oppnå nasjonal kontroll og digital motstandskraft må vurderes opp mot effekt. Det skal i den forbindelse gjennomføres kost-nyttevurderinger. De mange hensynene nevnt her må veies mot hensynet til å ivareta nasjonal sikkerhet og sammen utgjøre et godt beslutningsgrunnlag.

Boks 3.1 Digitale angrep koster i gjennomsnitt 20 millioner kroner

En global studie fra IBM viser at 83 prosent av verdens bedrifter har opplevd minst ett dataangrep de siste to årene. Kostnaden for et gjennomsnittlig digitalt angrep mot en bedrift har økt med 13 prosent på bare to år. Regningen ligger i snitt på rundt 20 mill. kroner i Norden og 40 mill. kroner globalt.

Da Norsk Hydro i 2019 ble rammet av et omfattende digitalt angrep lammet det selskapet fullstendig, og kostnadene ved angrepet var på 800 mill. kroner. Et annet eksempel er det danske shippingselskapet A.P. Møller-Mærsk. A.P. Møller-Mærsk ble i 2017 rammet av et dataangrep hvor kostnadene den gang ble estimert til mellom 200-300 mill. dollar.

3.1 Regulering må følge samfunnsutviklingen

Regulering er det primære virkemiddelet for å sørge for nasjonal kontroll og er også et kostnadseffektivt virkemiddel. Juridiske virkemidler består som regel av ulike påbud eller forbud, kombinert med en adgang til å kunne gi tillatelser, rettigheter og plikter eller fritak knyttet til disse. Regulering er et sterkt, men ofte nødvendig virke-

Figur 3.1 Satellittbasert kommunikasjon, overvåkning og jordobservasjon er blant de grunnleggende nasjonale funksjonene.

Foto: Shutterstock

middel. Det skaper forutsigbarhet og er en forutsetning for likeverdig behandling i en rettsstat.

3.1.1 Sikkerhetsloven – vårt viktigste verktøy for å ivareta nasjonal sikkerhet

Sikkerhetsloven står i en særstilling for å ivareta nasjonal sikkerhet. Verdier som er av betydning for våre nasjonale sikkerhetsinteresser skal etter sikkerhetsloven utpekes og sikres i tråd med lovens krav. Departementene utpeker grunnleggende nasjonale funksjoner (GNF) og kan fatte vedtak om at virksomheter som er av avgjørende betydning for GNF skal underlegges sikkerhetsloven.[1] Denne verdikartleggingen er en kontinuerlig prosess som dekker alle samfunnsområder. Kartleggingsarbeidet er komplekst, og viser blant annet at det er omfattende gjensidige avhengigheter på tvers av samfunnsområdene, og at avhengigheten endres relativt raskt. Det er behov for å oppdatere og forbedre oversikten for at det forebyggende sikkerhetsarbeidet skal bli så målrettet og effektivt som mulig. Dette vil prioriteres for alle samfunnsområder og gjøres i tråd med Justis- og beredskapsdepartementets pådriver- og samordningsrolle innenfor arbeidet med forebyggende nasjonal sikkerhet på sivil side.

Regjeringen er opptatt av at sikkerhetsloven er tilpasset det til enhver tid gjeldende trussel- og risikobildet, og vil derfor fremme nødvendige forslag til tilpasninger av regelverket. Gjennom revisjoner av sikkerhetsloven styrkes loven som virkemiddel for å ivareta nasjonal sikkerhet. Se punkt 4.2.1 om forslag til endringer i sikkerhetslovens kapittel 10 om eierskapskontroll.

Virksomheter som er underlagt sikkerhetsloven må ha tilstrekkelig kompetanse til å følge opp lovens krav. En felles sikkerhetsforståelse, sikkerhetskultur og grunnsikring av verdiene som er viktige for nasjonal sikkerhet må bygges over tid. Justis- og beredskapsdepartementet har bedt departementene kartlegge egen sikkerhets-

[1] Grunnleggende nasjonale funksjoner er definert i sikkerhetsloven 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».

Boks 3.2 Endringer i politiloven og politiregisterloven

Justis- og beredskapsdepartementet har i Prop. 31 L (2022–2023) foreslått endringer i politiloven og politiregisterloven om PSTs etterretningsoppdrag og bruk av åpent tilgjengelig informasjon. I proposisjonen foreslås det at PST skal utarbeide analyser og etterretningsvurderinger om forhold i Norge som kan true nasjonale sikkerhetsinteresser. I tillegg foreslås det at PST kan behandle åpent tilgjengelig informasjon dersom det antas å være nødvendig for utarbeidelse av analyser og etterretningsvurderinger, selv om den enkelte opplysning isolert sett ikke er nødvendig. Forslagene vil bidra til at PST i større grad kan vurdere sannsynlig fremtidig trusselutvikling i Norge og hvilke trusselaktører vi vil stå overfor i Norge i fremtiden, og vil være et viktig tiltak for å ivareta nasjonal sikkerhet.

kompetanse i løpet av 2022 og vil følge opp tilbakemeldingene overfor departementene (se punkt 3.4.1 for nærmere omtale).

3.1.2 Praktisering av eksisterende regelverk

Regjeringen mener at flere eksisterende regelverk på ulike samfunnsområder kan bidra til å ivareta nasjonal kontroll, også utover sikkerhetsloven.[2] Enkelte regelverk har ikke hensynet til nasjonal sikkerhet som vurderingskriterium i dag, mens andre regelverk allerede har bestemmelser som ivaretar sikkerhetsperspektivet. Regjeringen mener at det er et handlingsrom for å ivareta nasjonal sikkerhet i eksisterende regelverk på ulike samfunnsområder, og at handlingsrommet bør utnyttes bedre.

Praktisering av ulike regelverk kan ikke ses isolert, men må ses på tvers av samfunnsområder. Ulike tillatelsesordninger og forvaltningsperspektiv kan skape blindsoner, noe som kan utnyttes av fremmede stater på bekostning av nasjonale sikkerhetsinteresser. Vår evne til å verne om nasjonal sikkerhet er derfor avhengig av at den enkelte sektor og myndighetene i fellesskap er bevisst trusselbildet, egne verdier og avhengigheter, innenfor og på tvers av samfunnsområder. Samvirkeprinsippet er her viktig. I tillegg er Justis- og beredskapsdepartementet og Forsvarsdepartementet viktige som pådrivere for samordning mellom sivil og militær side.

Regjeringen vil gjennomgå relevant eksisterende lovverk for å påse at hensyn til nasjonal sikkerhet inngår som vurderingskriterium der det er aktuelt.

Med tanke på strategisk viktige verdier, bedrifter, eiendom, infrastruktur, naturressurser og teknologi er relevante regelverk som kan vurderes nærmere blant annet konsesjonslovgivning, plan- og bygningsloven, vannfallsrettighetsloven, energiloven, og havne- og farvannsloven. Dette innebærer ikke at hensyn til nasjonal sikkerhet alltid vil veie tyngst, men at det som et minimum skal vurderes. Hensikten er å stille krav til dem som forvalter lovverket og dem som skal etterleve det for å forebygge at uønskede aktører får innsikt, kontroll og innflytelse over verdier som er av betydning for nasjonal sikkerhet. Det er hensiktsmessig å gjøre eventuelle justeringer i relevant regelverk som del av annen lovgjennomgåelse. Lovverkene må også ses i sammenheng, for å unngå unødvendig dobbeltregulering.

3.1.3 Eksportkontroll

Eksportkontrolloven[3] og tilhørende forskrift[4] gjelder eksport av nærmere angitte varer, teknologi, herunder immaterielle ytelser, tekniske datapakker eller produksjonsrettigheter for varer, samt visse tjenester. Formålet er å sikre at eksport som kan brukes til militære formål eller til masseødeleggelsesvåpen ikke bidrar til konvensjonell, militær kapasitetsbygging i land av bekymring, og sikre at eksporten er i samsvar med norske utenriks- og sikkerhetspolitiske interesser.

Kontrollen med eksport av strategiske varer og teknologi øker i kompleksitet i takt med den sikkerhetspolitiske utviklingen og endringer i trusselbildet mot norske interesser. Land vi ikke har sikkerhetssamarbeid med etterspør strategiske varer, teknologi, tjenester og kunnskap fra Norge for å styrke sin militære evne. Dette omfatter både konvensjonell militær kapasitetsbygging og programmer for masseødeleggelsesvåpen, men også utstyr som kan benyttes til etterretningsvirksomhet eller kartlegging av kritisk infrastruktur i Norge. Norske teknologi-

[2] Enkelte relevante regelverk vil omtales i kap. 4.

[3] Lov om kontroll med eksport av strategiske varer, tjenester og teknologi mv.

[4] Forskrift om eksport av forsvarsmateriell, flerbruksvarer, teknologi og tjenester.

miljøer utsettes for stadige forsøk på omgåelser av eksportkontrollregelverket.

Regjeringen vil klargjøre og styrke eksportkontrollregelverket og tydeliggjøre praktiseringen av kontroll av kunnskapsoverføring i og fra Norge. Dette innebærer å tydeliggjøre hva som er en eksportkontrollregulert kunnskapsoverføring og å innta en bestemmelse om lisensplikt for kunnskapsoverføring i eksportkontrollforskriften.

Utenriksdepartementet gjennomførte våren 2022 en alminnelig høring av forslag til endringer i eksportkontrollforskriften. Utenriksdepartementet er i prosess med å vurdere høringsinnspillene og vil følge opp forskriftsarbeidet videre i 2023.

3.1.4 Forslag om ny lov om digital sikkerhet

Regjeringen vurderer å fremme et forslag til lov om digital sikkerhet. Sentralt i dette er å ansvarliggjøre virksomheter og sikre gjennomføring av nasjonale råd og anbefalinger.

Regjeringen legger opp til at lovforslaget skal gjelde for tilbydere av samfunnsviktige tjenester innenfor samfunnsområdene energi, transport, helse, vannforsyning, banktjenester, finansmarkedsinfrastruktur og digital infrastruktur. I tillegg gjelde for tilbydere av digitale tjenester, nærmere bestemt tilbydere av skytjenester, digitale markedsplasser og digitale søkemotorer. En nærmere presisering av hva som skal til for at en virksomhet er å anse som en samfunnsviktig tjeneste vil fremkomme i forskrift. Loven vil forplikte virksomheter til å gjennomføre sikkerhetstiltak og varsle om alvorlige digitale hendelser. Dette gjelder for enkelte samfunnsområder som har en særlig viktig rolle for å opprettholde kritisk samfunnsmessig og økonomisk aktivitet. Det vil ved videreutvikling av loven særlig ses på utvidelse av virkeområde, og hvordan sikre at nasjonale råd og anbefalinger blir fulgt opp av virksomheter i større utstrekning. Loven vil legge til rette for innføring av EUs NIS-direktiv.[5]

Regjeringen vil fortløpende vurdere regulering for å sikre forsvarlig digital sikkerhet hos virksomheter som understøtter viktige funksjoner i samfunnet. Blant annet vil EUs reviderte NIS-direktiv kunne ha betydning for hvordan lov om digital sikkerhet videreutvikles. Andre relevante EU-regelverk er Cybersecurity Act som omhandler European Union Agency for Cybersecurity (ENISA) sitt mandat og et felles-

Boks 3.3 Et langsiktig strategisk arbeid

Norske myndigheter har jobbet strategisk med digital sikkerhet over lang tid gjennom større utredninger, stortingsmeldinger, strategier og tiltaksutvikling. Norge fikk som det andre landet i verden en nasjonal strategi for digital sikkerhet allerede i 2003. I 2019 ble Norge det første landet som utga en fjerde strategi. Internasjonalt anses Norge å være et modent land på området og for mange en attraktiv samarbeidspartner. Denne stortingsmeldingen bygger videre på et langsiktig arbeid hvor styrket råd og veiledning og behov for ytterligere regulering er identifisert som viktige områder.

europeisk rammeverk for frivillig sertifisering av IT-produkter, tjenester og prosesser. Denne forordningen jobbes det med å få inkorporert i EØS-avtalen. EU har også nylig lansert lovforslaget Cyber Resilience Act med minstekrav til digital sikkerhet i produkter og tjenester. Et lovforslag om digital operasjonell motstandsdyktighet for finanssektoren, Digital Operational

Boks 3.4 EUs forslag til revidert NIS-direktiv

EU vedtok i november 2022 et nytt direktiv, NIS2. Direktivets virkeområde er utvidet sammenliknet med NIS-direktivet ved å legge til nye samfunnsområder. Enheter som regelverket vil gjelde for vil bli klassifisert ut fra deres betydning og delt i kategorier som henholdsvis grunnleggende og viktige, og underlagt forskjellige tilsynsregimer. Det nye direktivet styrker også sikkerhetskravene til virksomhetene med en minimumsliste over grunntiltak som må anvendes, og gir mer presise bestemmelser for varsling av hendelser. I tillegg adresseres sikkerheten i forsyningskjeder og leverandørforhold. Medlemslandene i EU gis en frist på 21 måneder til å innføre direktivet nasjonalt, da oppheves samtidig gjeldende NIS-direktiv.

[5] Europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for et høyt felles sikkerhetsnivå i nettverks- og informasjonssystemer i EU.

Resilience Act, er også til behandling i EU. Målet med forslaget er å sikre at alle deltakere i det finansielle systemet har de nødvendige tiltakene på plass for å redusere faren for digitale angrep og andre uønskede hendelser. Forslaget bygger på NIS-direktivet og vil ha forrang foran NIS-direktivets regler der det er aktuelt når det er trådt i kraft. Det foreslåtte regelverket vurderes å være EØS-relevant.

3.2 Nasjonalt eierskap for å sikre nasjonal kontroll

På enkelte områder bidrar nasjonalt eierskap til å sikre nasjonal kontroll. Det gjelder for eksempel innenfor energi- og naturressurser, viktig infrastruktur og strategisk viktige deler av norsk næringsliv. Nasjonalt eierskap omfatter statlig, fylkeskommunalt og kommunalt eierskap, samt privat norsk eierskap. Blant annet på grunn av komplekse verdikjeder og eierstrukturer, innebærer ikke nasjonalt eierskap nødvendigvis nasjonal kontroll.

Med «statlig eierskap» menes statens direkte eierskap i selskaper. Siden 2002 har det i hver stortingsperiode blitt lagt frem en eierskapsmelding for Stortinget om statens samlede direkte eierskap i selskaper. I eierskapsmeldingen redegjøres det for hvorfor staten eier direkte i selskaper, hva staten eier og hvordan staten utøver sitt eierskap. I gjeldende eierskapsmelding[6] er samfunnssikkerhet og beredskap en av begrunnelsene for når statlig eierskap kan være et hensiktsmessig tiltak. Av eierskapsmeldingen fremgår følgende:

> «Regulering er det primære virkemiddelet for å ivareta hensyn knyttet til nasjonal sikkerhet, samfunnssikkerhet og beredskap. Eksempler på slik regulering er næringsberedskapsloven, kraftberedskapsforskriften, sikkerhetsloven og ekomloven. Statlige overføringer til produsenter, kontraktsinngåelser med private aktører eller andre former for samarbeid med næringslivsaktører administrert og forvaltet gjennom respektive sektordepartement er eksempler på andre virkemidler.
>
> Staten kan i særskilte tilfeller vurdere det som nødvendig å unngå at uønskede interesser kan få tilgang til informasjon, innflytelse på eller kontroll over selskaper som har betydning for nasjonal sikkerhet, samfunnssikkerhet eller beredskap, noe som blant annet kan gjøres ved å underlegge selskapene sikkerhetsloven eller eie en gitt andel i enkelte selskaper.».
>
> «Statlig eierskap begrunnet med samfunnssikkerhet og beredskap tilsier normalt en statlig eierandel på mer enn halvparten. Det bidrar til å hindre at uønskede interesser får aksjemajoritet og dermed innsikt og innflytelse gjennom styreposisjon.».

Offentlig eierskap (statlig, fylkeskommunalt eller kommunalt eierskap) kan gi det offentlige store inntekter, legge til rette for en ønsket samfunnsutvikling og demokratisk kontroll. Samtidig kan offentlig eierskap være ressurskrevende, ha økonomiske kostnader, kreve betydelig oppfølging og være politisk sensitivt. Nasjonal kontroll kan oppnås ved ulike virkemidler og er ikke nødvendigvis det samme som offentlig eierskap. Å ha kontroll kan også dreie seg om å forebygge at uønskede aktører får kontroll, eventuelt disponerer eiendom, ressurser eller infrastruktur som kan gi dem innsikt, innflytelse eller reduserer vårt eget politiske eller økonomiske handlingsrom. Dette kan også oppnås gjennom private norske eierskap i selskaper, eiendom eller andre aktiva.

Kontroll med hvem som er reelle eiere av for eksempel infrastruktur, naturressurser eller eiendom av betydning for nasjonal sikkerhet er viktig. Regjeringen ønsker bedre oversikt over dette. Det

Boks 3.5 Statlig eierskap som virkemiddel for samfunnssikkerhet og beredskap

Hensyn til samfunnssikkerhet og beredskap har vært en begrunnelse for statlig eierskap over tid. Staten drev egenproduksjon av forsvarsmateriell gjennom Kongsberg Våpenfabrikk, Horten Verft og Raufoss Ammunisjonsfabrikker. Disse virksomhetene ble opprettet på 1800-tallet og var underlagt Forsvaret, og ble i 1947 skilt ut som egne selskaper. Selskapene gikk etter hvert også inn i annen industriproduksjon. Staten har videreført eierskapet til ammunisjonsvirksomheten gjennom Nammo, og til produksjon av annet militært materiell gjennom Kongsberg Gruppen.

[6] Meld. St. 6 (2022–2023) *Et grønnere og mer aktivt eierskap – Statens direkte eierskap i selskaper.*

vil gi innsikt i om eierskapet kan være en utfordring for nasjonal sikkerhet. Informasjon om utenlandsk eierskap blir registrert av en rekke institusjoner, både norske og internasjonale, men informasjonen blir i dag i liten grad systematisert. Dette krever derfor et utstrakt samarbeid nasjonalt og internasjonalt. Behovet for oversikt over strategisk viktige områder er nærmere omtalt i kapittel 4.

3.3 Samarbeid nasjonalt og internasjonalt

Samarbeid og informasjonsdeling på tvers av samfunnsområder, tjenester, myndighetsområder, offentlig-privat og over landegrenser er avgjørende i arbeidet med nasjonal sikkerhet. For eksempel sitter ulike private og offentlige aktører med mye relevant informasjon som kan bidra til økt innsikt og felles forståelse av utfordringsbildet. Det bidrar til bedre beslutningsgrunnlag og tilpasset bruk av virkemidler og gjør oss i bedre stand til å beskytte verdier med betydning for nasjonal sikkerhet både i fred, krise og væpnet konflikt. Økt kunnskap og involvering av alle nivåer i samfunnet må være en integrert del for å møte trussel- og risikobildet. Gjennom å styrke den enkeltes sikkerhet bidrar vi til å styrke vår kollektive sikkerhet.

3.3.1 Samarbeidet mellom etterretnings- og sikkerhetstjenestene

Utstrakt samarbeid og informasjonsutveksling mellom etterretnings- og sikkerhetstjenestene våre er grunnleggende for å ivareta nasjonal sikkerhet. Informasjon om og forståelse av trussel- og risikobildet er avgjørende for at ulike aktører kan identifisere egne sårbarheter og ivareta egen sikkerhet. En forutsetning for dette er hensiktsmessige rammer og verktøy, spesielt for håndtering og formidling av høygradert informasjon.

For å bidra til økt informasjonsutveksling og koordinering mellom E-tjenesten og PST i arbeidet med konkrete saker ble samarbeidet ytterligere styrket sommeren 2021, gjennom etableringen av Felles etterretnings- og kontraterrorsenter. I november 2022 besluttet regjeringen å opprette et nasjonalt etterretnings- og sikkerhetssenter (NESS). I NESS skal PST, E-tjenesten, NSM og (det øvrige) politiet samarbeide for å styrke vår nasjonale evne til å oppdage og forstå sammensatte trusler – og våre egne sårbarheter – samt for å sikre god beslutningsstøtte til myndighetene. Samarbeidet bygger videre på det forsterkede samarbeidet mellom PST og politiet etablert i februar i år, for å utvikle et nasjonalt situasjonsbilde knyttet til sammensatt virkemiddelbruk. Tiltaket understreker regjeringens prioritering av arbeidet mot sammensatte trusler.

Felles cyberkoordineringssenter (FCKS) er et permanent, samlokalisert fagmiljø bestående av representanter fra NSM, E-tjenesten, PST og

Boks 3.6 Etterretnings- og sikkerhetstjenestene

Politiets sikkerhetstjeneste (PST) er Norges nasjonale innenlands etterretnings- og sikkerhetstjeneste, underlagt Justis- og beredskapsdepartementet. PST har som oppgave å forebygge og etterforske alvorlig kriminalitet mot nasjonens sikkerhet. Som ledd i dette skal tjenesten identifisere og vurdere trusler knyttet til etterretning, sabotasje, spredning av masseødeleggelsesvåpen, terror og ekstremisme. Vurderingene skal bidra i utformingen av politikk og støtte politiske beslutningsprosesser.

Etterretningstjenesten (E-tjenesten) er Norges utenlands etterretningstjeneste. Tjenesten er en del av Forsvaret, men arbeidet omfatter både sivile og militære problemstillinger. E-tjenestens hovedoppgaver er å varsle om ytre trusler mot Norge og prioriterte norske interesser, støtte Forsvaret og forsvarsallianser Norge deltar i og understøtte politiske beslutningsprosesser med informasjon av spesiell interesse for norsk utenriks-, sikkerhets- og forsvarspolitikk.

Nasjonal sikkerhetsmyndighet (NSM) er nasjonal fagmyndighet for forebyggende sikkerhet etter sikkerhetsloven. NSM gir blant annet råd om beskyttelsen av og fører tilsyn med sikring av skjermingsverdig informasjon, informasjonssystemer, objekter og infrastruktur. Videre er NSM nasjonalt fagmiljø for digital sikkerhet og har et ansvar på nasjonalt nivå for å oppdage, varsle og koordinere håndtering av alvorlige digitale angrep.

Figur 3.2 PST er Norges nasjonale innenlands etterretnings- og sikkerhetstjeneste.

Foto: Justis- og beredskapsdepartementet

Kripos. Arbeidet til FCKS bidrar til å øke den nasjonale evnen til å motstå alvorlige digitale angrep og vedlikeholde et helhetlig trussel- og risikobilde for det digitale rom. I tillegg bidrar de med viktig strategisk analyseproduksjon, som grunnlag for beslutninger på myndighetsnivå.

3.3.2 Nasjonalt cybersikkerhetssenter i NSM (NCSC)

NSM har gjennom NCSC etablert en arena for nasjonalt og internasjonalt samarbeid innen deteksjon, håndtering, analyse og rådgivning knyttet til digital sikkerhet. Senteret omfatter partnere fra næringsliv, akademia, forsvar og offentlig sektor som bidrar aktivt inn i et gjensidig samarbeid for et mer robust digitalt Norge. I dag deltar om lag 50 virksomheter, og stadig flere kommer til. Partnerprogrammet skal styrkes, både for å åpne for flere partnere, og for å legge til rette for mer informasjonsdeling.

Med flere partnere øker behovet for å dele partnernettverket inn i målgrupper. Dette er viktig for å bygge tillit og dele informasjon internt i nettverket, og for å nå ut med bedre tilpasset informasjon til den enkelte virksomhet på en mer effektiv måte. NCSC er viktig i NSMs arbeid med råd og veiledning, deteksjon og hendelseshåndtering (se punkt 3.5 og 3.6).

For å styrke arbeidet med forskning, innovasjon og kompetanse innenfor digital sikkerhet, følger Norge opp EUs forordning om opprettelse av et nettverk av nasjonale koordineringssentre for digital sikkerhet. I den forbindelse skal det etableres et senter som skal bygge opp og samordne den nasjonale delen av det europeiske kompetansefellesskapet innenfor digital sikkerhet og generelt stimulere til forskning, innovasjon og kompetanseutvikling nasjonalt. En viktig oppgave for senteret vil være å fremme og gi veiledning til søkere i de europeiske investeringsprogrammene DIGITAL og Horisont Europa innenfor cybersikkerhetsrelaterte utlysninger. Senteret forutsettes også å kunne tildele EU-midler og nasjonal medfinansiering til tredjeparter. DIGITAL og Horisont Europa er investerings- og forskningsprogrammer i EU som Norge allerede deltar i.

Justis- og beredskapsdepartementet arbeider for at NSM og Norges forskningsråd etablerer Norges nasjonale koordineringssenter for digital

Figur 3.3 Nasjonalt cybersikkerhetssenter i NSM.
Foto: NSM

sikkerhet. Senteret skal samarbeide med øvrige miljøer i Norge innenfor digital sikkerhet.

3.3.3 Internasjonalt samarbeid

I en internasjonal økonomi og et digitalisert samfunn, hvor avhengigheter, virkemiddelbruk og trusselaktører ikke forholder seg til landegrenser, er det viktig med internasjonalt samarbeid for å oppnå nasjonal kontroll. Det omfatter blant annet å arbeide for ansvarlig statlig oppførsel i det digitale rom og søke å benytte eksisterende kanaler, som EUs screeningmekanisme, for tilgang til informasjon om sikkerhetstruende økonomisk aktivitet.

Erfaringer fra våre allierte, NATO, FN og EU kan gi nyttig innsikt om beste praksis på tvers av nasjonale grenser og bidra til å tilpasse nasjonale regelverk for å ha en felles tilnærming der det er hensiktsmessig. I lys av Finlands og Sveriges NATO-søknader vil det være særlig relevant å søke fellesnordiske løsninger der det er mulig, gitt våre liknende styresett, verdisyn og trussel- og risikobilde. Ved at Norge tar en tydelig rolle internasjonalt og kan vise til nasjonale tiltak og prioriteringer, vil Norge også kunne oppfattes som en forutsigbar og pålitelig alliert og partner, noe som er viktig for vår posisjon i internasjonalt samarbeid.

For Norge er en hovedprioritet i det internasjonale arbeidet å jobbe for en styrket etterlevelse av gjeldende folkerett blant FNs medlemsstater. Norge offentliggjorde i 2021 sine nasjonale posisjoner på utvalgte folkerettslige problemstillinger i det digitale rom for å bidra til en styrket felles forståelse av hvordan folkeretten kommer til anvendelse. Tjenester og produkter vi benytter er ofte helt eller delvis produsert og utviklet i andre deler av verden. Dette krever et samarbeid om internasjonale standarder som ivaretar sikkerhetsperspektivet.

Regjeringen vil at Norge skal jobbe for et tett, forpliktende og forutsigbart internasjonalt samarbeid om nasjonal sikkerhet og motarbeide sammensatte trusler sammen med allierte, partnere, NATO, FN og EU.

Regjeringen vil at Norge skal delta aktivt internasjonalt for en styrket etterlevelse av gjeldende folkerett. Norge skal bidra i arbeidet med utarbeidelse av internasjonale frivillige normer og standarder innenfor det digitale rom. Regjeringen vil også styrke samarbeidet med internasjonale partnere for

å fremme et åpent, sikkert, stabilt og fredelig digitalt rom.

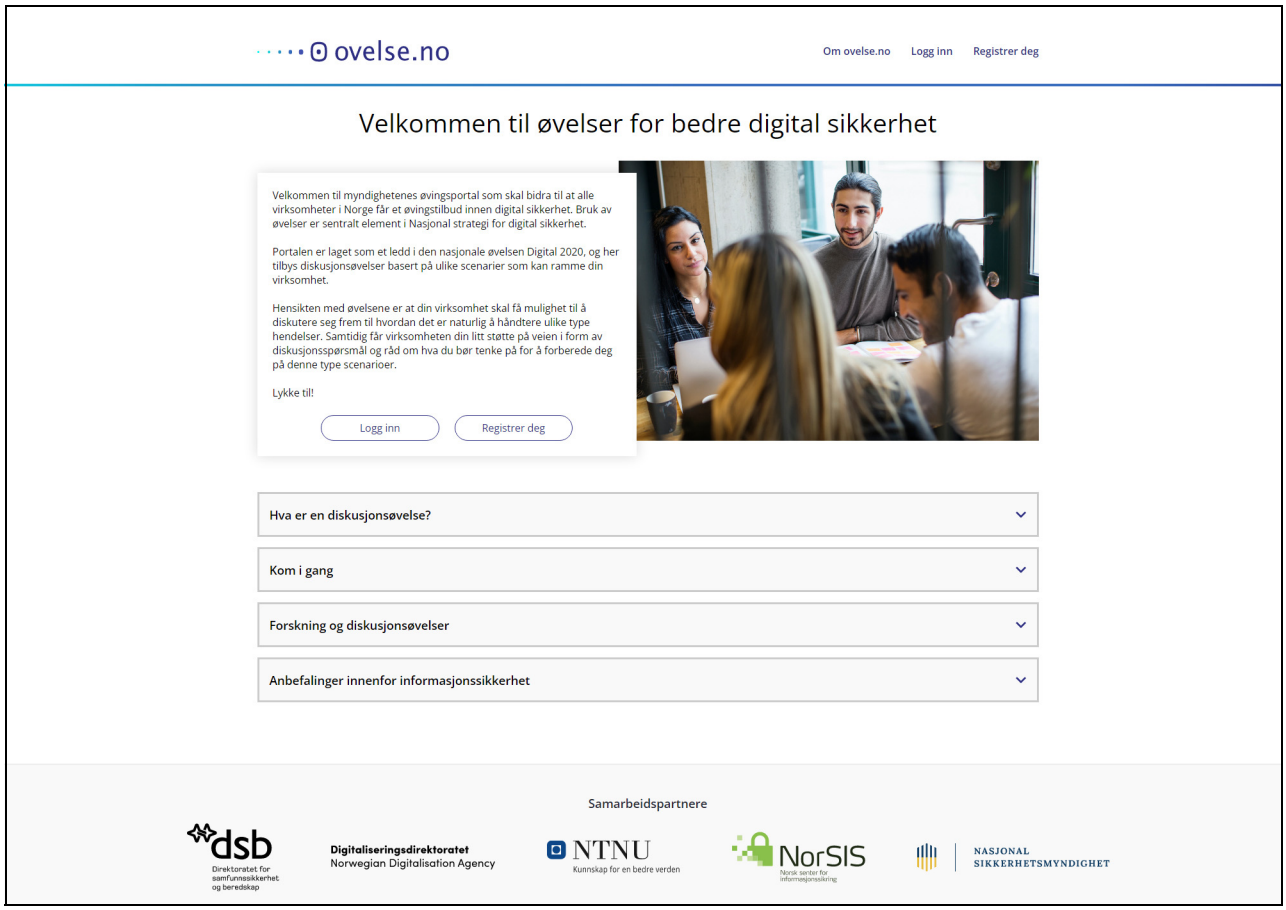
3.4 Kompetanse og bevisstgjøring

3.4.1 Sikkerhetsfaglig kompetanse i samfunnet

Kompetanse om trusler, sårbarheter og effektive tiltak er en forutsetning for å kunne beskytte verdier mot uønskede hendelser. Manglende kompetanse om risiko og kjennskap til egne verdier og sårbarheter bidrar til dårligere sikkerhetsstyring og en svakere sammenheng mellom faktisk risikobilde og tiltak som reduserer risiko. Det er flere eksempler på at kombinasjonen av mangelfull verdiforståelse og åpenhetskultur har ført til at informasjon om eksempelvis eiendom og infrastruktur som er av betydning for nasjonal sikkerhet har ligget åpent tilgjengelig på internett. Dette kan være risiko- og sårbarhetsanalyser eller oversikt over samfunnskritisk infrastruktur. Virksomheter og offentlige organer som forvalter verdier av betydning for nasjonal sikkerhet må vurdere hensynet til nasjonal sikkerhet i tilstrekkelig grad når slik informasjon gjøres tilgjengelig.

Tekniske sikkerhetstiltak alene vil ikke stoppe potensielle trusselaktører. Det er derfor nødvendig å bygge en god sikkerhetskultur i hele samfunnet. Dette forutsetter at alle – privatpersoner, virksomheter og myndigheter – er bevisst sikkerhetsutfordringene og har nødvendig basiskunnskap om mottiltak som er relevante for dem. Dette øker robusthet, men også bevissthet og forståelse for sikkerhet hos den enkelte. Det er særlig viktig å styrke verdiforståelsen og kompetansen om trusler, sårbarheter og effektive sikkerhetstiltak blant toppledere og beslutningstakere. God sikkerhetskultur kommer til uttrykk gjennom virksomhetens totale sikkerhetsatferd.

Norsk senter for informasjonssikring (NorSIS) gjennomfører på vegne av norske myndigheter Nasjonal sikkerhetsmåned hvert år i oktober. Dette er et eksempel på et bevisstgjøringstiltak som når bredt ut i samfunnet. Målet med kampanjen er å styrke virksomheters og den enkelte innbyggers kompetanse om digital sikkerhet. Et annet eksempel er den nasjonale øvelsesportalen,



Figur 3.4 Plattformen ovelse.no er myndighetenes øvingsportal som skal bidra til at alle virksomheter i Norge får et gratis øvingstilbud innen digital sikkerhet. Skjermdump: ovelse.no

Boks 3.7 Kritisk medieforståelse

Kritisk medieforståelse er viktig for befolkningens motstandskraft. Dette er et høyt prioritert område for Medietilsynet, som annethvert år gjennomfører en undersøkelse om kritisk medieforståelse i befolkningen. Kartleggingen omfatter blant annet eksponering for og håndtering av desinformasjon og falske nyheter, kunnskap om forskjeller på redaksjonelt og kommersielt innhold, personvern, kildekunnskap og tillit til medier. Medietilsynet iverksetter tiltak og råd for at befolkningen skal være godt rustet til å navigere og forstå mediene. Tenk, som er skoleavdelingen til faktasjekktjenesten Faktisk.no, utvikler undervisningsopplegg om kritisk mediebruk og kildebevissthet til bruk i skolen.

ovelse.no, som gir norske virksomheter et gratis øvingstilbud om digital sikkerhet.

For å legge til rette for god oppfølging av sikkerhetsloven, har Justis- og beredskapsdepartementet bedt departementene kartlegge lederstillinger som har roller og ansvar knyttet til departementenes grunnleggende nasjonale funksjoner. Disse lederne har behov for sikkerhetsklarering og sikkerhetsfaglig kompetanse innen sikkerhetsstyring, risikovurdering, verdivurdering og grunnleggende digital sikkerhet.

Justis- og beredskapsdepartementet har også anbefalt at alle departementer, i samsvar med sikkerhetsloven, kartlegger hvilke lederstillinger i underliggende virksomheter som krever sikkerhetsklarering og sikkerhetsfaglig kompetanse. Resultatet skal oversendes Justis- og beredskapsdepartementet innen utgangen av 2022. Departementet vil deretter vurdere behovet for ytterligere kompetansetiltak i offentlige virksomheter for å ivareta våre nasjonale sikkerhetsinteresser.

Boks 3.8 Nasjonal strategi for digital sikkerhetskompetanse

Nasjonal strategi for digital sikkerhetskompetanse fra 2019 legger til rette for en langsiktig oppbygging av kompetanse, herunder den nasjonale kapasiteten innen forskning, utvikling, utdanning og bevisstgjøringstiltak rettet mot befolkningen og virksomheter. Strategien er utarbeidet av Justis- og beredskapsdepartementet i samarbeid med Kunnskapsdepartementet.

Boks 3.9 Nasjonal folkeopplysningskampanje

NorSIS vil på oppdrag fra Justis- og beredskapsdepartementet, jf. Prop. 78 S (2021–2022), gjennomføre en nasjonal folkeopplysningskampanje om digital sikkerhet. Formålet med kampanjen er å øke sikkerhetsbevisstheten og kompetansen bredt i befolkningen. Kampanjen vil bli gjennomført i samarbeid med relevante aktører som NSM og politiet. Kampanjen er direkte rettet mot befolkningen og små- og mellomstore bedrifter, og vil ha et formspråk og budskap som er lett å forstå. Et av temaene som vil bli løftet frem er tiltak som kan bidra til økt digital sikkerhet blant befolkningen, slik som totrinnspålogging på ulike tjenester. For å nå ut bredt er det planlagt at kampanjen i stor grad vil foregå i sosiale medier. Kampanjen vil ha oppstart i desember 2022, og fortsette utover i 2023.

3.4.2 Tilstrekkelig nasjonal spesialistkompetanse

Undersøkelser av tilbud og etterspørsel viser et behov for flere utdannede innen digital sikkerhet. De siste årene er det iverksatt en rekke tiltak for å redusere kompetansegapet. Flere tiltak er å anse som langsiktige. For eksempel har den fulle effekten av nye studieplasser i IKT-relaterte fag enda ikke kommet i form av uteksaminerte kandidater.

Regjeringen vil kartlegge kompetansesituasjonen innenfor digital sikkerhet og vurdere tiltak basert på arbeidslivets behov.

Innenfor enkelte områder av betydning for nasjonal sikkerhet er det behov for personell med spesialistkompetanse på doktorgradsnivå. Personellet må kunne drive forskning og utvikling på områder der de behandler informasjon som kan få avgjørende skadefølger for nasjonal sikkerhet om informasjonen blir kjent for uvedkommende.

Et tilstrekkelig antall uteksaminerte kandidater på masternivå er en forutsetning for å sikre flere

Boks 3.10 Balanse mellom en fortsatt åpen og internasjonalt orientert kunnskapssektor og økende vektlegging av sikkerhetspolitiske hensyn

Økt internasjonalisering har i lang tid vært et mål for norsk høyere utdannings- og forskningspolitikk og et viktig virkemiddel for økt kvalitet og relevans i norsk utdanning og forskning. God tilrettelegging av langsiktig samarbeid med sterke fagmiljøer i andre land er avgjørende for videreutviklingen av Norge som kunnskapsnasjon og for norske bidrag til løsninger på de utfordringene vi som samfunn står overfor. Dette omfatter også land vi ikke har et sikkerhetspolitisk samarbeid med.

I Norge, som i andre likesinnede land og i EU, OECD osv., diskuteres det i dag hvordan man kan tilrettelegge for en god balanse mellom en fortsatt åpen og internasjonalt orientert kunnskapssektor og økende vektlegging av sikkerhetspolitiske hensyn. I tråd med dette er «ansvarlighet» innført som et grunnleggende prinsipp i gjeldende strategi for høyere utdannings- og forskningssamarbeid med prioriterte land utenfor EU.[1]

Det er iverksatt flere tiltak for å tilrettelegge for samarbeid innen høyere utdanning og forskning på prioriterte områder samtidig som nasjonale interesser ivaretas. Dette omfatter et fast rundebord for akademisk samarbeid med Kina, som koordineres av Kunnskapsdepartementet, og «Møteplass Kina», som organiseres av Forskningsrådet og Direktoratet for høyere utdanning og kompetanse. Rundebordet retter seg mot strategisk ledelse, mens målgruppen for «Møteplass Kina» er de som jobber mer operativt med høyere utdannings- og forskningssamarbeid ved norske universiteter, høyskoler og forskningsinstitutter. I tillegg foregår det et arbeid med å utvikle nasjonale retningslinjer for ansvarlig internasjonalt samarbeid, som vil foreligge i løpet av første halvår 2023.

[1] Panoramastrategien (2021–2027) regjeringen.no.

forskerutdannende og andre høyt kompetente med sikkerhetsklarering til fagområdene digital sikkerhet og kryptologi. Innenfor gruppen «naturvitenskapelige fag, håndverksfag og tekniske fag» var over 90 prosent av studentene norske i 2021. Andelen utenlandske studenter på studieprogrammer innenfor digital sikkerhet varierer mellom studieprogrammene, men lå samlet på bare fem prosent i 2021.[7] Å øke antall studieplasser innenfor digital sikkerhet og andre IKT-fag vil derfor kunne være et bidrag til å øke andelen forskere og andre høyt kompetente som vil kunne få sikkerhetsklarering.

Eventuelle endringer i studiekapasiteten vurderes i forbindelse med de årlige statsbudsjettene. Regjeringen forventer samtidig at universiteter og høyskoler selv vurderer omfanget av digital sikkerhet i sine studieporteføljer og fastsetter det i henhold til arbeidslivets behov og de studiesøkendes ønsker, slik de skal gjøre for alle sine utdanninger, herunder også for doktorgradsutdanningene.[8]

Rekruttering av doktorgradskandidater som kan sikkerhetsklareres er en utfordring innenfor ulike teknologiområder allerede i dag. De siste ti årene har godt over 60 prosent av dem som avlegger doktorgrad innenfor teknologi ved et norsk lærested utenlandsk statsborgerskap.[9] Andelen med utenlandsk statsborgerskap som søker rekrutteringsstillinger innen matematikk, naturvitenskap og teknologi var nær 90 prosent i perioden 2016-2018.[10] Dette er en utvikling som må tas på alvor.

Regjeringen vil videreføre øremerkede midler til nærings-ph.d.- og offentlig sektor-ph.d.-ordningene i Forskningsrådet rettet mot digital sikkerhet og kryptologi. Midlene er tilgjengelige for alle kvalifiserte søkere som har sikkerhetsklarering.

Å rekruttere kandidater som kan sikkerhetsklareres til doktorgradsutdanning i digital sikkerhet og kryptologi vil også kreve målrettet innsats fra universiteter og høyskoler. Som omtalt over, forventer regjeringen at utdanningsinstitu-

[7] Statistikk om høyere utdanning fra Direktoratet for høyere utdanning og kompetanse.

[8] Innst. 425 S (2020–2021) og Meld. St. 19 (2020–2021) Styring av statlige universiteter og høyskoler.

[9] SSB 2022. Artikkel: Rekordmange utenlandske statsborgere blant de nye doktorene i 2021.

[10] NIFU 2019. Attraktive akademiske karrierer? Søking, rekruttering og mobilitet i UH-sektoren. Rapport 2019:10.

Boks 3.11 Offentlig-privat samarbeid om sikkerhetstesting og undersøkelser av kritiske systemer

Norge må ha kompetanse og kapasitet til å verifisere og validere utstyr og systemer som integreres i systemer som er kritiske for samfunnets evne til å fungere. Over flere år har NTNU, i tett samarbeid med kraftbransjen, jobbet med å bygge opp en slik kapasitet som kan brukes til sikkerhetstesting og undersøkelser av maskinvare og integrerte systemer. Statkraft, Statnett, Eidsiva, KraftCERT, NVE, NSM og Energi Norge har vært pådrivere for det offentlig-private samarbeidsinitiativet. Sammen med partnere gjør NTNU nå en investering på ca. 15 mill. kroner for å etablere et laboratoriemiljø for å møte dette behovet. Investeringen gjøres i tilknytning til Norwegian Cyber Range.

sjonene fastsetter omfanget på doktorgradsutdanningene i henhold til arbeidslivets behov og de studiesøkendes ønsker. Ved ansettelser i rekrutteringsstillinger hvor arbeidstakeren vil komme i situasjoner som krever enten sikkerhetsklarering, adgangsklarering eller autorisasjon skal universiteter og høyskoler sørge for at den som tilsettes, får de nødvendige klareringer, slik sikkerhetsloven krever.

De fleste stipendiater i teknologiske fag vil ikke ha behov for sikkerhetsklarering i løpet av sin doktorgradsutdanning, men de kan komme til å trenge sikkerhetsklarering i den jobben de går til etter avlagt doktorgrad. På enkelte fagområder av betydning for nasjonal sikkerhet vil det derfor være ønskelig å sikre at det utdannes et tilstrekkelig antall doktorer som har mulighet til å bli sikkerhetsklarert etter utdanning. Med dagens regelverk for sikkerhetsklarering og ansettelser i statlige stillinger, er det uklart hvordan universiteter og høyskoler kan regulere inntaket av stipendiater for å oppfylle ønsket om å utdanne doktorer som kan sikkerhetsklareres. Samtidig er det uklart hvor stort behov arbeidslivet har for doktorer som kan sikkerhetsklareres. Før regjeringen går i gang med å vurdere regelverket, bør behovet kartlegges.

Regjeringen vil utrede arbeidslivets behov for doktorgradskompetanse til stillinger hvor det kreves sikkerhetsklarering.

3.5 Råd og veiledning – brukeren i fokus

En størst mulig felles forståelse for sikkerhet, trussel- og risikobildet i samfunnet, fra privatpersoner til bedrifter og offentlig virksomheter, er viktig for nasjonal sikkerhet og nasjonal kontroll. Som en del av dette inngår informasjon om trussel- og risikobildet, hvorfor nasjonal sikkerhet er viktig, hvilke virkemidler myndighetene har til rådighet, hvilke krav som stilles til ulike offentlige og private aktører og hvordan det treffer den enkelte. Summen av enkelttiltak bidrar til en større motstandsdyktighet i samfunnet overfor uønskede hendelser.

3.5.1 Etablering av nasjonal portal og støtteverktøy for digital sikkerhet

Regjeringen vil lansere en nasjonal portal for digital sikkerhet og et støtteverktøy til alle norske virksomheter for å tilgjengeliggjøre nasjonale råd og anbefalinger i tråd med Prop. 78 S (2021–2022).

Råd og veiledning om digital sikkerhet er ofte lite kjent og blir i begrenset grad systematisk fulgt opp og prioritert av virksomhetene. Portalen skal være en felles inngangsport for ulike brukergrupper, men utformet slik at alle får ensartede råd tilpasset sin brukergruppe. Dette skal ikke kreve forutgående kunnskap om roller og ansvar

Boks 3.12 Nasjonale råd og anbefalinger om digital sikkerhet følges i for liten grad

Justis- og beredskapsdepartementet og Forsvarsdepartementet gjennomførte i 2021 en spørreundersøkelse blant norske virksomheter om den nasjonale strategien for digital sikkerhet og kjennskap til nasjonale råd og anbefalinger om digital sikkerhet. Resultatene viser at de virksomheter som kjenner til de nasjonale anbefalingene i strategien og NSMs grunnprinsipper benytter disse i stor grad i sin virksomhet. Dette gjelder både offentlig og privat sektor, uavhengig av virksomhetens størrelse. Et fåtall av virksomhetene har fulgt opp samtlige anbefalinger. Hovedårsaken opplyses å være manglende tid, men også at virksomhetene er usikre på hvordan de skal gå frem.

innenfor området. Arbeidet med å utvikle portalen startet opp høsten 2022 med planlagt lansering i løpet av 2023. Innholdet i portalen skal utarbeides av sentrale aktører med roller og ansvar knyttet til digital sikkerhet. NSM leder arbeidet, og skal etablere, forvalte og drifte portalen.

Økt sikkerhet i den enkelte virksomhet er viktige bidrag til samfunnets kollektive sikkerhet. For å bidra til et mer systematisk arbeid med digital sikkerhet, vil NSM tilby et støtteverktøy til alle norske virksomheter gjennom den nasjonale portalen. Verktøyet vil gjøre det lettere for virksomheter å evaluere egen sikkerhetstilstand og bidra til at nasjonale råd blir bedre kjent og i større grad blir implementert av virksomheter.

3.5.2 Kraftsamling av statlige veiledningsressurser

Flere statlige myndigheter gir råd og veiledning om digital sikkerhet, og myndighetenes arbeid på området kan for omverdenen fremstå fragmentert og lite koordinert.[11] Portalen og støtteverktøyet beskrevet i punkt 3.5.1 vil bidra til bedre samordning og tilgjengeliggjøring av råd og veiledning. Regjeringen vil vurdere ytterligere tiltak for å forsterke samordningen på myndighetsnivå og gjøre det enklere for sluttbrukeren.

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.

3.5.3 En sikker digital nettverksarkitektur («Zero Trust»)

I løpet av det siste tiåret har arbeidet med en sikker nettverksarkitektur i økende grad tatt utgangspunkt i at man ikke kan ha større tillit til maskiner og tjenester i virksomhetens interne nettverk enn man har til vilkårlige maskiner og tjenester på det åpne internett. En følge av dette er at digitale identiteter, autentisering og tilgangsstyring har blitt sentrale virkemidler for å etablere en sikker nettverksarkitektur. Denne tilnærmingen har fått betegnelsen «Zero Trust»-arkitektur.

Regjeringen vil sørge for at norske anbefalinger om sikker nettverksarkitektur oppdateres i takt med utviklingen av internasjonale standarder på området.

[11] NOU 2018: 14 *IKT-sikkerhet i alle ledd.*

3.6 Nasjonal deteksjonsevne og hendelseshåndtering

3.6.1 Nasjonal hendelseshåndtering

En stor del av truslene mot Norge skjer i det digitale rom. NSM har over tid erfart en kraftig økning av digitale angrep. Ifølge NCSC er dette en trend som forventes å fortsette i tiden fremover. De digitale angrepene mot Stortinget i 2020 og 2021 var angrep på vårt demokrati og viser alvorlighetsgraden i det digitale risikobildet. Norge gikk for første gang til det skritt å foreta en offentlig attribusjon til en annen stat. Det ble kunngjort at Russland sto bak. Året etter ble det offentliggjort at det andre datainnbruddet mot Stortinget ble gjennomført fra Kina.

For å bidra til å møte utfordringsbildet er NSM styrket med 15 mill. kroner i 2022, jf. Innst. 270 S (2021–2022) til Prop. 78 S (2021–2022). Bevilgningen innebærer en utvidelse av antall stillinger i NCSC og skal forbedre evnen til koordinering, analyse og håndtering av hendelser og praktisk bistand til rammede virksomheter.

Sektorvise responsmiljøer er et viktig tiltak for å sikre deling av informasjon og støtte til håndtering av digitale angrep. De fleste sektorer har etablert slike miljøer eller inngått ulike former for samarbeid om dette. Responsmiljøene er bindeleddet mellom NSM og de enkelte virksomhetene i ulike sektorer. På oppdrag fra Justis- og beredskapsdepartementet er det gjennomført en ekstern evaluering av ordningen med sektorvise responsmiljøer. Det overordnede inntrykket er at samarbeidet mellom de ulike aktørene funge-

Boks 3.13 Oljefondet opplever cyberangrep hver dag – digitale angrep er fondets største bekymring

Norges Bank Investment Management har den daglige oppgaven med å forvalte Statens pensjonsfond utland («Oljefondet») og gjør en stor innsats for å redusere sannsynligheten og konsekvensene av digitale hendelser mot egen virksomhet. De erfarer at antall angrep øker og at angriperne stadig benytter mer avanserte metoder og virkemidler. Dermed har cybersikkerhet blitt en av de største bekymringene for fondets sjef.

rer godt, at det er god utveksling av informasjon, metoder, erfaringer og kompetanse på tvers av miljøene, og at ordningen med sektorvise responsmiljøer har gitt et mer samlet sikkerhetshetsmiljø i Norge. En hovedkonklusjon er at den nasjonale innsatsen bør kraftsamles for å sikre grunnleggende nasjonale funksjoner. I tillegg bør forebyggende digital sikkerhet i større grad inkluderes i den nasjonale modellen for hendelseshåndtering og balanseres mot operativt arbeid. Gitt kompetansemangelen innenfor digital sikkerhet er det også viktig at den nasjonale modellen for hendelseshåndtering er bærekraftig over tid.

Regjeringen vil videreutvikle det nasjonale rammeverket for håndtering av digitale hendelser. Dette for å sikre en bærekraftig hendelseshåndteringsmodell i tråd med samfunnets behov.

3.6.2 Digital motstandskraft i kommunesektoren

Uønskede digitale hendelser i kommuner kan få store konsekvenser for tjenestene til innbyggerne, og medføre store kostnader for kommunene og det norske samfunnet. Selv om digital sikkerhet i kommunene håndteres innenfor den bredere samfunnssikkerheten, gjør et hybrid trusselbilde det nødvendig å arbeide for bedre digital motstandskraft også ut fra et nasjonalt sikkerhetsperspektiv. I en presset økonomisk situasjon vil det også for kommunene være krevende å gjøre nødvendige prioriteringer og skaffe kompetanse innen digital sikkerhet.

I februar 2022 deltok over 200 kommuner i et møte med justis- og beredskapsministeren og kommunal- og distriktsministeren. Formålet var å øke oppmerksomheten om digital sikkerhet i

Boks 3.14 Team Norway

På oppdrag fra Justis- og beredskapsdepartementet og Forsvarsdepartementet, koordinerer NSM og Cyberforsvaret norsk deltagelse i den internasjonale cyberøvelsen Locked Shields. Hensikten med norsk deltagelse er å trene responsmiljøer på tvers av sivil og militær sektor i hendelseshåndtering. NSM og Cyberforsvaret har gjennom etableringen av «Team Norway» fulgt opp strategien om utstrakt offentlig-privat og sivil-militært samarbeid for å møte digitale trusler.

Figur 3.5 Norge har deltatt flere ganger i den internasjonale øvelsen Locked Shields.

Foto: NATO CCDCOE, Ardi Hallismaa

Boks 3.15 Østre Toten kommune utsatt for løsepengevirus

Østre Toten kommune ble 9. januar 2021 utsatt for et krypteringsvirus med krav om løsepenger som satte store deler av kommunens nettverk tilbake til manuell styring i lang tid. Aktøren hadde stjålet betydelige mengder data. Kommunens operative evne ble sterkt redusert da de fleste av kommunens digitale tjenester var nede. Situasjonen ble ytterligere forverret den 29. mars, da deler av de stjålne dataene ble publisert på det mørke nettet. Kommunen måtte håndtere sensitive personopplysninger på avveie, og informere og støtte personer som ble rammet. Hendelsen medførte i praksis at alarmsystem på sykehjem ble erstattet med bjeller, låsesystemet på kommunens bygninger ikke fungerte, og at helsestasjonens journaler var utilgjengelige. Hendelsen har kostet kommunen rundt 34 mill. kroner.

kommunesektoren, orientere om et endret trussel- og risikobilde og komme i dialog med kommunene om hvor staten kan bidra slik at de står bedre rustet til å forebygge og håndtere uønskede digitale hendelser. Som en oppfølging av kommunearrangementet ønsker regjeringen at kommunene får et permanent responsmiljø som dekker kommunenes behov.

Regjeringen vil bidra til forebygging av uønskede digitale hendelser i kommunesektoren og vil utpeke et sektorvis responsmiljø som kan dekke kommunenes behov.

3.6.3 Etablere neste generasjons nasjonale deteksjonsevne

For nasjonal digital sikkerhet er såkalte «avanserte vedvarende trusler» den dimensjonerende trusselen. Aktørene bak vurderes ofte å være statlige aktører som over tid jobber systematisk med å opprette tilganger til relevante systemer.

Varslingssystem for digital infrastruktur (VDI) fungerer som en «digital innbruddsalarm» for å oppdage angrep. VDI er et nettverk av sensorer som utplasseres hos utvalgte offentlige og private virksomheter som har kritisk infrastruktur. Sensorene gjør det mulig for NSM å oppdage og verifisere digitale angrep.

For å øke effekten av systemet, vil både antallet virksomheter som deltar i VDI-samarbeidet og analysekapasiteten for å håndtere større informasjonsmengder øke. NSM er styrket med 30,3 mill. kroner til dette tiltaket, jf. Innst. 270 S (2021–2022) til Prop. 78 S (2021–2022). Neste generasjons VDI utvides med flere ulike komponenter som er designet til å fungere sammen og vil totalt sett være mer effektivt enn i dag. Utvidelsen er også et viktig bidrag for å se helheten og arbeidet med et nasjonalt situasjonsbilde i det digitale domenet.

Regjeringen har en ambisjon om å videreutvikle nasjonal deteksjonsevne. Utviklingen på dette område vil imidlertid kreve en langsiktig satsning, som også inkluderer infrastruktur. Sentralt i dette er videreutviklingen av VDI og eventuelle krav til VDI-sensorer for viktige leverandører som understøtter sentrale funksjoner i samfunnet. Det vil vurderes økt analysekapasitet og teknisk kapasitet i NSM for å avdekke sikkerhetstruende hendelser.

4 Nasjonal kontroll over verdier av betydning for nasjonal sikkerhet

Det er viktig å sikre nasjonal kontroll over verdier som har betydning for nasjonal sikkerhet.[1] Eksempler de siste årene viser at økonomisk virkemiddelbruk overfor verdier som infrastruktur, bedrifter, eiendom, naturressurser og teknologi kan benyttes til sikkerhetstruende aktivitet, og dette er en særlig utfordring.

Statlige aktører kan benytte økonomiske virkemidler for å utnytte sårbarheter, styrke effekten av andre maktmidler eller bidra til å legitimere disse maktmidlene. Dette kommer i konflikt med våre nasjonale sikkerhetsinteresser. Investeringer og oppkjøp kan for eksempel brukes som virkemiddel for å få innsikt i sensitiv informasjon knyttet til beredskapsordninger, kritisk infrastruktur eller politiske beslutningsprosesser. Økonomiske virkemidler kan også gi tilgang til teknologi og ressurser av strategisk betydning.

Forskningsbasert kunnskap om sikkerhetstruende økonomisk virkemiddelbruk er avgjørende for å treffe riktig med tiltakene for å styrke motstandskraften mot denne aktiviteten. Justis- og beredskapsdepartementet har gitt flere forskningsoppdrag til Forsvarets forskningsinstitutt (FFI) og Norsk utenrikspolitisk institutt (NUPI). Oppdragene omfatter blant annet utenlandske investeringer og eierskap i Norge.

4.1 Oversikt over verdier og verdikjeder

4.1.1 Kartlegging av virksomheter og verdier

En grunnleggende forutsetning for å ivareta nasjonal sikkerhet er at myndighetene har oversikt over hvilke verdier og hvilke virksomheter som har betydning for nasjonal sikkerhet. En slik oversikt er nødvendig for å kunne vurdere hvilke av virkemidlene beskrevet i kapittel 3 som er relevante og hensiktsmessige for å ivareta nasjonal kontroll. Det er behov for bedre oversikt over utenlandsk eierskap i blant annet selskaper og eiendom. Behovet for nye verktøy, som utvikling av registre, tilgang til og bruk av databaser og analyseverktøy, må vurderes nærmere. Bruk av slike verktøy må ikke bryte med konfidensialitetshensyn.

I sikkerhetsloven er det en egen metodikk for kartlegging av verdier som har avgjørende eller vesentlig betydning for statens evne til å ivareta nasjonale sikkerhetsinteresser (grunnleggende nasjonale funksjoner). Kartleggingen viser blant annet at nasjonal sikkerhet ivaretas av svært mange virksomheter på alle samfunnsområder og at det er omfattende avhengigheter både innenfor samme sektor og på tvers av sektorene. Kartleggingsarbeidet er komplekst, og avhengighetene endres relativt ofte. Regjeringen vil derfor prioritere arbeidet med kartleggingen for at den skal være tilstrekkelig oppdatert og detaljert til at virkemiddelbruken blir så treffsikker som mulig.

Regjeringen mener det også er behov for å få bedre oversikt over virksomheter og verdier som sikkerhetsloven ikke gjelder for, men som likevel kan ha en betydning for nasjonal sikkerhet. Dette vil dreie seg om virksomheter og verdier som har mindre enn vesentlig betydning for nasjonal sikkerhet, men som samlet sett eller i en gitt kontekst vil kunne ha en slik betydning at det kan være aktuelt å iverksette tiltak. Det kan være fysiske, digitale og andre verdier, som for eksempel forskningsinformasjon og kunnskap, infrastruktur, bedrifter, eiendom eller naturressurser. En oversikt over slike verdier kan gi sentrale og lokale myndigheter innsikt i verdier av betydning for nasjonal sikkerhet innenfor deres ansvarsområde og vil supplere oversikten som sentrale myndigheter har fra kartlegging i tråd med sikkerhetsloven. Basert på dette totalbildet kan myndighetene vurdere relevante virkemidler for å ivareta nasjonal sikkerhet, herunder nasjonalt eierskap og kontroll. Hvordan oversikten skal følges opp, for eksempel knyttet til ansvar og roller, virkemidler og regelverk, må vurderes nærmere. Det vil være nødvendig å se en slik oversikt i sammenheng med annet relevant arbeid, slik som endringer i sikkerhetsloven og

[1] I slike vurderinger vil alltid ulike hensyn måtte avveies, som omtalt under punkt 2.2.

Figur 4.1 Kraftforsyning er en viktig del av Norges infrastruktur.

Foto: Shutterstock

screening av økonomisk aktivitet mot virksomheter som ikke er underlagt sikkerhetsloven. Regjeringen vil intensivere dette arbeidet.

Regjeringen vil vurdere hvordan man på en hensiktsmessig måte kan få bedre oversikt over virksomheter og verdier som ikke dekkes av sikkerhetsloven, men som likevel kan ha betydning for nasjonal sikkerhet.

4.1.2 Økt oversikt over våre avhengigheter og verdikjeder

Sentrale tjenester og funksjoner i samfunnet er i stor grad avhengige av lange og til dels uoversiktlige verdikjeder. En verdikjede kan forklares som en struktur av leveranser mellom virksomheter. Verdikjeden representerer en avhengighet virksomheter imellom, for å få levert tjenester eller produkter. Slike verdikjeder kan omfatte fysisk infrastruktur, digitale avhengigheter, eierskap og underleverandører. Verdikjedene er ofte komplekse og uoversiktlige med mange avhengigheter, som ofte går på tvers av landegrenser.

Svikt i verdikjeder kan få store konsekvenser. Covid-19-pandemien og krigen i Ukraina har vist oss hvordan sårbarheter i internasjonale verdi- og forsyningslinjer kan utfordre forsyningssikkerheten. Dersom kraftforsyningen faller ut, vil store deler av samfunnet stoppe opp. Utfall i den digitale infrastrukturen fører til utilgjengelighet av digitale tjenester i det området som er rammet. Utfall av satellittbaserte tjenester vil få konsekvenser for blant annet Forsvaret, redningstjenester, skips- og luftfart og deler av finansnæringen.

Trusselaktører kan utnytte sårbarheter i verdikjeder som er viktige for nasjonal sikkerhet, og/eller sikre kontroll over sentrale deler av verdikjeder gjennom for eksempel eierskap. Sårbarheter i en verdikjede kan resultere i at det utføres sikkerhetstruende aktivitet mot underleverandører i verdikjeden, enten som et mål i seg selv eller som et ledd i å nå mål høyere opp i verdikjedene.

Norge har en åpen økonomi og er et digitalisert samfunn. Det medfører at vi har mange komplekse verdikjeder som strekker seg ut over våre grenser og som det vil være krevende å ha kontroll over. Digitale verdikjeder har fått stor internasjonal oppmerksomhet gjennom verdikjedeangrep de siste årene (se tekstboks 4.1 om SolarWinds). Den enkelte virksomhet har ansvar for å

Boks 4.1 SolarWinds

Det amerikanske IT-selskapet SolarWinds ble desember 2020 utsatt for et leverandørkjedeangrep. Angrepet var en sofistikert og omfattende cyberoperasjon hvor trusselaktøren klarte å etablere en bakdør i et av programmene til SolarWinds. Bakdøren ble så med i en oppdatering av programmet som SolarWinds selv distribuerte til sine kunder, over 18.000 virksomheter verden over. Amerikanske myndigheter har senere gått ut og pekt på at aktøren bak angrepet sannsynligvis hadde russisk opphav.

Noe av alvorlighetsgraden lå i typen program som ble rammet. Det er designet for å utføre nettverksovervåking og vil derfor som regel ha vide tilganger til virksomhetens infrastruktur. Ved å infiltrere dette fikk aktøren et svært gunstig utgangspunkt for å komme seg videre inn i nettverket og omgå sikkerhetsmekanismer.

Saken hadde omfattende konsekvenser for de som ble rammet, herunder amerikanske myndighetsorganer og store teknologiselskaper som Microsoft. Etter å ha fått tilgang til virksomheter som hadde installert oppdateringen med bakdøren, spisset aktøren sine kapasiteter mot utpekte mål. Det indikerte at aktøren ikke agerte på alle tilganger den hadde oppnådd, men heller prioriterte enkelte virksomheter som ble utsatt for mer målrettede metoder for videre kompromittering.

NSM arbeidet tett med nasjonale og internasjonale samarbeidspartnere for å kartlegge omfanget av hendelsen. Anbefalinger fra Cybersecurity and Infrastructure Security Agency i USA (CISA), FireEye og Microsoft ble fulgt, og NSM oppfordret alle virksomheter som brukte programvaren i sin infrastruktur til å sette seg inn tilgjengelig dokumentasjon. Flere av SolarWinds' kunder i Norge hadde installert en kompromittert versjon av programmet. De store konsekvensene uteble fordi bakdøren ikke ble utnyttet. Denne type leverandørkjedeangrep er likevel noe NSM forventer mer av i tiden fremover, med potensielt betydelige konsekvenser for norske mål.

ha oversikt og kontroll på sine verdikjeder, i den grad det er mulig. Økt tjenesteutsetting krever bedre oppfølging av leverandører, herunder at virksomheter har god nok bestillerkompetanse og gjør tilstrekkelige sikkerhetsfaglige vurderinger.

Vi er avhengige av internasjonalt samarbeid for å oppnå nasjonal kontroll over verdikjeder, både fysiske og digitale. Norge skal jobbe for et tett, forpliktende og forutsigbart internasjonalt samarbeid for å identifisere verdikjeder som er av betydning for nasjonal sikkerhet og for å redusere svikt i disse verdikjedene.

Regjeringen vil igangsette et samarbeidsprosjekt mellom Kommunal- og distriktsdepartementet og Justis- og beredskapsdepartementet for å vurdere behov for tiltak innen risikostyring av digitale verdikjeder.

Det vil i dette prosjektet gjennomføres en kartlegging av utvalgte verdikjeder knyttet til kritisk digital infrastruktur som er av betydning for nasjonal sikkerhet, som vil danne grunnlag for etablering av effektiv veiledning og hensiktsmessig regulering overfor norske virksomheter. Kartleggingen vil også kunne bidra til å utvikle tiltak og legge grunnlag for en revisjon av NSMs grunnprinsipper for IKT-sikkerhet. I tillegg vil en slik kartlegging kunne bidra i arbeidet med utpeking av grunnleggende nasjonale funksjoner og deres kritiske digitale avhengigheter, samt i arbeidet

Boks 4.2 Beredskapslager for legemidler

En motstandsdyktig helseberedskap må være tilpasset utfordringsbildet og den sikkerhetspolitiske situasjonen vi står i. Covid-19-pandemien har også synliggjort internasjonale avhengigheter og sårbarheter. Det er bygd opp et nasjonalt beredskapslager for smittevernutstyr, der de regionale helseforetakene eier varebeholdningen, står for innkjøp, rullering og utvikling av lageret. Regjeringen viderefører lageret i 2023, og det inneholder blant annet åndedrettsvern, munnbind, hansker, øyebeskyttelse, smittefrakker og heldekkende dresser og har et volum tilsvarende seks måneders pandemiforbruk.

Boks 4.3 Leverandørkjedesikkerhet i kraftforsyningen

I 2021 viste en undersøkelse gjennomført av Norges vassdrags- og energidirektorat (NVE) at cyberangrep primært rammet administrative IT-systemer i kraftbransjen og at angrep kunne flytte seg til selskapene via leverandører som var angrepet. NVE har forskriftsfestet krav til leveranser av driftskontrollsystemer til de mest kritiske anleggene, og anbefaler bransjen å gjøre seg kjent med trussel- og risikorapportene fra PST, E-tjenesten og NSM, samt å vurdere landrisiko. NVE samarbeider også med bransjeforeninger, for å heve kunnskapsgrunnlaget og videreutvikle relevant veiledningsmateriale.

Boks 4.4 Fremmede stater tilegner seg kompetanse og teknologi gjennom oppkjøp

I «Bergen Engines-saken» ble oppkjøp som et virkemiddel for å tilegne seg teknologi satt på spissen. I kgl.res. 21/1898, vedtaket som stanset salget av Bergens-bedriften, heter det: «Norsk industri og norske kunnskaps- og forskningsinstitusjoner er mål for russisk etterretningsvirksomhet. Russland viser særlig interesse for bedrifter som har unik kompetanse og teknologi, blant annet innenfor forsvarsindustri og maritim sektor. Det vestlige sanksjonsregimet fører til at Russland søker alternative metoder for å tilegne seg kritisk teknologi og kompetanse for å videreutvikle egne militære kapasiteter. Bruk av private aktører er et eksempel på en slik metode, noe som gjør det mer utfordrende å oppdage og forhindre fordekte anskaffelser.»

med å utpeke samfunnsviktige og vesentlige tjenester som del av arbeidet med lov om digital sikkerhet. Rammeverket for risikostyring av digitale verdikjeder vil inngå som kunnskapsgrunnlag i arbeidet.[2]

4.2 Strategisk viktige bedrifter

Norge har en åpen økonomi som er tett integrert med verdensøkonomien. Åpenhet for utenlandske investeringer er positivt for økonomisk vekst og velstand, men gjør oss samtidig sårbare overfor fremmede stater med fiendtlige hensikter. Uønskede oppkjøp ble i PSTs nasjonale trusselvurdering for 2021 fremhevet som en betydelig trussel mot norske interesser. Bekymringen ble gjentatt i trusselvurderingen for 2022 og ble underbygget av trussel- og risikovurderinger fra de øvrige etterretnings- og sikkerhetstjenestene.

For å sikre nasjonal kontroll over strategisk viktige bedrifter bruker staten allerede flere virkemidler. Sikkerhetsloven har bestemmelser om eierskapskontroll i virksomheter underlagt loven, og statlig eierskap benyttes som virkemiddel i enkelte tilfeller. Begrunnelsene for statlig eierskap fremgår for øvrig av eierskapsmeldingen, og omtales i punkt 3.2. Det er behov for å få bedre oversikt og kontroll med eierstrukturer i strategisk viktige bedrifter i Norge for å identifisere eventuell sikkerhetstruende aktivitet. Eksempler på strategisk viktige bedrifter kan være forsvars- og sikkerhetsindustrien, også de som ikke er underlagt statlig eierskap. Selv om det gjøres mye på dette området, og regjeringen ytterligere styrker mulighetene til å få bedre oversikt og kontroll, vil det alltid være en restrisiko som må håndteres.

4.2.1 Eierskapskontroll og screeningsmekanisme hjemlet i sikkerhetsloven

Sikkerhetslovens kapittel 10 gir myndighetene anledning til å kontrollere eierskap i virksomheter som er underlagt sikkerhetsloven. Bestemmelsen i § 2-5 gir myndighetene i ytterste konsekvens mulighet til å gripe inn i økonomisk aktivitet mot virksomheter som ikke er underlagt sikkerhetsloven etter nærmere bestemte vilkår. Sikkerhetsloven § 2-5 er imidlertid ment som en sikkerhetsventil.

Norge har en screeningmekanisme basert på sikkerhetslovens kapittel 10 og § 2-5. Mekanismen består av et departementsnettverk, ledet av Justis- og beredskapsdepartementet, samt et etatsnettverk ledet av NSM. NSM ble i 2021 utpekt som nasjonalt kontaktpunkt for varsler om sikkerhetstruende økonomisk virksomhet. Prosess og krite-

[2] Risikostyring i digitale verdikjeder. Direktoratet for samfunnssikkerhet og beredskap (dsb.no).

Figur 4.2 Bedrifter innen forsvars- og sikkerhetsindustrien er eksempler på strategisk viktige bedrifter.
Foto: Frank Holm

rier for håndtering av saker under kapittel 10 er beskrevet i loven, mens det i 2022 ble laget retningslinjer for departementenes håndtering av saker som gjelder mulig sikkerhetstruende aktivitet i virksomheter som ikke er underlagt sikkerhetsloven og hvor det kan bli aktuelt å bruke § 2-5. Det er et mål at norske myndigheter skal ha mulighet til å fange opp, vurdere og eventuelt gripe inn i økonomisk aktivitet som kan true nasjonal sikkerhet. Samtidig er det viktig at Norges folkerettslige forpliktelser ivaretas og at det ikke legges unødvendige eller uforholdsmessige byrder på næringslivet eller begrensinger på handelen med andre land. Dette er utfordrende siden håndtering av sikkerhetstruende økonomisk aktivitet treffer i skjæringspunktet mellom sikkerhetsinteresser og næringslivs-, utenrikspolitiske og handelspolitiske hensyn. De ulike departementene jobber derfor tett sammen for å vurdere de ulike hensynene opp mot hverandre.

Regjeringen tar sikte på å legge frem forslag til endringer i sikkerhetslovens kapittel 10 om eierskapskontroll mv. tidlig 2023.

Lovforslaget har som hovedformål å styrke evnen til å beskytte våre nasjonale sikkerhetsinteresser mot andre staters økonomiske virkemiddelbruk ved å øke myndighetenes tilgang til informasjon om endringer i eierskap i virksomhetene som er underlagt loven. Formålet er også å klargjøre regler om stans av erverv mv., slik at loven ikke begrenser norske virksomheters muligheter til å tiltrekke seg investeringer ut over det som er nødvendig for å beskytte nasjonale sikkerhetsinteresser.

Lovforslaget innebærer at departementene gis økt mulighet til å gjøre bestemmelsene i sikkerhetsloven, inkludert bestemmelsene om eierskapskontroll i sikkerhetsloven kapittel 10, gjeldende for flere virksomheter enn i dag. Videre foreslås det å senke terskelen for at erverv i virksomheter må meldes inn til myndighetene, samt at både avhender og virksomheten, i tillegg til erververer er forpliktet til å sende melding om erverv.

Dette vil styrke myndighetenes mulighet til inngripen i tilfeller der en aktørs forsøk på å oppnå kontroll eller betydelig innflytelse over en norsk virksomhet vurderes å være i strid med nasjonale sikkerhetsinteresser.

4.2.2 Screening av økonomisk aktivitet mot virksomheter som ikke er underlagt sikkerhetsloven

Den nasjonale screeningmekanismen er etablert med utgangspunkt i sikkerhetsloven kapittel 10 og § 2-5. Det vil være tilfeller av potensielt sikkerhetstruende økonomisk aktivitet mot norske virksomheter som ikke fanges opp gjennom meldeplikten etter kapittel 10 for virksomheter underlagt sikkerhetsloven. Det er derfor behov for blant annet å se nærmere på en eventuell mekanisme for å fange opp potensielt sikkerhetstruende økonomisk aktivitet for virksomheter som ikke kapittel 10 gjelder for. § 2-5 er som nevnt under 4.2.1 ment å fungere som en sikkerhetsventil, ikke som grunnlag for ordinære prosesser. Hjemmelen gir derfor ikke detaljer om sektorer, kriterier eller prosess for behandling av saker om potensielt sikkerhetstruende økonomisk aktivitet.

Regjeringen har oppnevnt et offentlig utvalg som skal utrede behovet for regelverk eller en ordning for å screene økonomisk aktivitet mot virksomheter som ikke er underlagt sikkerhetsloven. Dette skal ses i sammenheng med dagens screeningmekanisme og forslaget til endringer i sikkerhetslovens bestemmelser om eierskapskontroll.

Utvalget skal se hen til hvordan relevante land håndterer screeningsaker og ta dette med i sine vurderinger. Utvalget skal også se hen til arbeidet til en tverrdepartemental arbeidsgruppe opprettet av Utenriksdepartementet som vurderer fremtidig organisering av eksportkontrollen.[3] En kartlegging gjennomført av NUPI (2021) av et utvalg lands screeningmekanismer viser at det er stor variasjon i hvordan ulike vestlige lands screeningmekanisme er satt opp, men at flere EU-land er i prosess med å harmonisere sine regelverk og mekanismer opp mot kravene som stilles i EUs screeningforordning fra 2019.[4]

4.2.3 Behov for å styrke den nasjonale kontrollen med eiendommer av betydning for nasjonal sikkerhet

E-tjenesten, PST og NSM har i sine trussel- og risikovurderinger pekt på at utenlandsk eierskap i eiendommer i enkelte geografiske områder kan innebære en trussel mot nasjonale sikkerhetsinteresser.

Enkelte eiendommer kan ha en sikkerhetsmessig betydning fordi de ligger i nærheten av kritisk infrastruktur, som havner, forsvarsanlegg eller kraftforsyning. Dette kan blant annet være næringseiendommer, ferieboliger, landbruks- og skogeiendommer eller annen type eiendom. Med «eiendom av sikkerhetsmessig betydning» menes eiendom som på grunn av beliggenhet kan legge til rette for sikkerhetstruende virksomhet mot et skjermingsverdig objekt eller infrastruktur.

I Bergen Engines-saken ble eiendommens beliggenhet vektlagt i begrunnelsen for å stanse salget:

> «Eiendommen ligger strategisk plassert mot den nordlige innseilingen til Bergen og forsvarsinstallasjoner av sikkerhetsmessig betydning for Norge og allierte nasjoner. Russisk etterretningsaktivitet mot norske mål og interesser kan medføre at eiendommen fremstår som en interessant plattform for russiske tjenester».

Boks 4.5 Ny lovgivning i Finland strammer inn på hvem som kan eie eiendom

FFI-rapport 22/00426 om «Russisk økonomisk statshåndverk – implikasjoner for norsk sikkerhet» omtaler ny finsk lovgivning: «I Finland slo myndighetene i 2018 til mot flere russiskeide eiendommer med omfattende overvåkingsutstyr installert på eiendommen. Eiendommene befant seg i nærheten av strategisk viktige havner og gjennomfartsårer i Østersjøen, og eieren i siste instans var skjult gjennom selskaper registrert i skatteparadiser. Mens eiendommene kan være knyttet til ikke-statlig, kriminell aktivitet, peker finske sikkerhets- og etterretningstjenester generelt på at eiendommer i Finland kjøpt av russiske aktører kan brukes til militære formål. Det er konsentrasjonen av eiendommene i nærheten av strategisk viktige lokasjoner som vekker sikkerhets- og etterretningstjenestenes mistanke».

Finske myndigheter innførte i 2019 en lov om plikt til å søke tillatelse til kjøp av visse eiendommer. Loven forvaltes av det finske forsvarsdepartementet.

[3] Se nærmere om eksportkontrollarbeidet under 3.1.3.

[4] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union.

Figur 4.3 Utenlandsk eierskap i eiendommer kan innebære en trussel mot nasjonale sikkerhetsinteresser.
Foto: Robert Bye/Unsplash

Utenlandske eierinteresser i eiendom kan være representert i Norge via utenlandske privatpersoner som bor her, via foretak de kontrollerer eller har eierandeler i, eller som investeringer i eiendom uten annen form for registrert aktivitet i Norge. Informasjon om hvem som eier eiendom er i svært liten grad systematisert på måter som gir oversikt over utenlandske eierinteresser til tross for at det samles inn mye relevant data. Ofte blir opplysninger om eiere registrert på måter som ikke skiller mellom norske og utenlandske aktører.

Ved vurdering av eierskap til eiendom og bruk av eiendom er det viktig å vurdere mulighetsrommet i allerede eksisterende regelverk, til å for eksempel systematisere allerede eksisterende data, og gi relevante myndigheter tilgang til informasjon om eierskap til eiendommer.

Det tas sikte på å legge frem forslag til endringer i sikkerhetslovens eierskapsbestemmelser mv. tidlig 2023. Det vurderes forslag om endringer i sikkerhetsloven § 7-3 for å presisere at virksomheters risikovurdering skal identifisere konkrete eiendommer som har en beliggenhet som kan legge til rette for sikkerhetstruende virksomhet mot skjermingsverdige objekter og skjermingsverdig infrastruktur. Dette vil kunne øke årvåkenheten og bevisstheten hos virksomheten og senke terskelen for å varsle sikkerhetsmyndigheten når virksomheten får informasjon om aktiviteter knyttet til eiendommer som kan utgjøre en risiko. Forslaget innebærer også at sikkerhetsmyndigheten skal føre oversikt over eiendommer av sikkerhetsmessig betydning, hvor risikoen ikke kan reduseres med sikkerhetstiltak.

For å styrke myndighetenes evne til å fange opp sikkerhetstruende virksomhet knyttet til eierskap til og bruk av eiendom, ønsker regjeringen å gi Kartverket og NSM i oppgave å tilrettelegge for et system slik at sikkerhetsmyndigheten får den nødvendige oversikten over eiendom av sikkerhetsmessig betydning. Slik tilgang kan gis med hjemmel i § 4 tredje ledd bokstav h) i forskrift om

utlevering, viderebruk og annen behandling av opplysninger fra grunnboken og matrikkelen.

Skjult eierskap til fast eiendom kan ha konsekvenser for nasjonale sikkerhetsinteresser hvis eiendommene benyttes til sikkerhetstruende virksomhet. Som et ledd i å styrke den nasjonale kontrollen med skjult eierskap har regjeringen påbegynt et arbeid for å kartlegge utfordringer knyttet til skjult eierskap i fast eiendom.

Regjeringen vil styrke kontrollen med eiendom av betydning for nasjonal sikkerhet og vurderer blant annet å

- *foreslå endringer i sikkerhetsloven som tydeliggjør at virksomhetseier har en plikt til å foreta en risikovurdering som skal identifisere konkrete eiendommer som har en beliggenhet som kan legge til rette for sikkerhetstruende virksomhet mot skjermingsverdige objekter og skjermingsverdig infrastruktur.*
- *gi sikkerhetsmyndigheten elektronisk tilgang til grunnbok og matrikkel for å holde oversikt over eiendom av betydning for nasjonal sikkerhet.*
- *kartlegge utfordringer knyttet til skjult eierskap i fast eiendom, herunder en eventuell tinglysningsplikt.*
- *se nærmere på hvordan en plikt til å søke tillatelse til kjøp av visse eiendommer eventuelt kan reguleres.*

4.2.4 Vektlegge nasjonal sikkerhet i arealplanleggingen

Kommuneplanens arealdel skal i nødvendig utstrekning vise hensyn og restriksjoner som har betydning for bruken av areal. Blant disse hensynene er ikke nasjonal sikkerhet et forhold som vektlegges i dagens bestemmelser. Dette vil regjeringen vurdere å endre.

Berørt statlig og regionalt organ kan fremme innsigelse til forslag til kommuneplanens arealdel og reguleringsplan i spørsmål som er av nasjonal eller vesentlig regional betydning, eller som av andre grunner er av vesentlig betydning for vedkommende organs saksområde. Gjennom innsigelsesinstituttet er det altså etablert et system for kontroll med bestemmelsene i dag. Videre er det delegert til statsforvalterne å veilede kommunene i arealplanleggingen, blant annet knyttet til bestemmelsene om samfunnssikkerhet. Veiledningsrollen er viktig fordi den bidrar til å øke kommunenes kompetanse i arealplanleggingen.

Regjeringen vil se nærmere på bestemmelsene i plan- og bygningsloven for å sikre at nasjonal sikkerhet blir vektlagt i arealplanleggingen. Videre vil regjeringen vurdere å utvide innsigelsesinstituttet slik at staten har innsigelsesrett på områder knyttet til nasjonal sikkerhet. Regjeringen vil også vurdere å utvide statsforvalterens veiledningsplikt overfor kommunen knyttet til nasjonal sikkerhet.

4.2.5 Ivareta hensynet til nasjonal sikkerhet i konsesjonslovgivningen

Konsesjonsloven har som formål å regulere og kontrollere omsetningen av fast eiendom for å oppnå et effektivt vern om landbrukets produksjonsarealer og slike eier- og bruksforhold som er mest gagnlige for samfunnet.[5] Loven gjelder erverv av fast eiendom, men ikke indirekte overdragelser som for eksempel erverv av aksjer eller upersonlige selskaper som eier fast eiendom. I tillegg til erverv, gir loven blant annet hjemmel for kontroll hvis det stiftes langvarige bruksretter mv. på en eiendom som ville utløst konsesjon ved eventuell overdragelse. Slike rettigheter er konsesjonspliktige uavhengig av størrelsen på det arealet rettigheten legger beslag på. Loven fastsetter at den gjelder alle erverv, men det er gjort unntak fra dette i lov og forskrift. Unntakene har i praksis ført til at kontrollen vanligvis bare er aktuell når noen erverver eiendom som skal nyttes til landbruksformål, eller ved erverv av eiendom som ligger i kommuner med nedsatt konsesjonsgrense og hvor formålet med ervervet er å bruke eiendommen til andre formål enn helårsbolig.

Kommunen kan gi konsesjon uten videre, sette vilkår for konsesjon, eller avslå søknaden. Hva som i det konkrete tilfellet anses som slike eier- og bruksforhold som er mest gagnlig for samfunnet tolkes vidt. Det innebærer at ulike samfunnshensyn og -interesser kan trekkes inn i vurderingen av konsesjonssøknaden. Blant annet kan konsesjonsloven kobles til nasjonal sikkerhet siden det gir kontroll over hvem som erverver eiendom. Det kan være ønskelig å regulere ervervet på enkelte eiendommer, for eksempel basert på en verdikartlegging, som omtalt i 4.1.1.

Regjeringen vil se nærmere på praktiseringen av konsesjonsloven slik at hensynet til nasjonal sikkerhet vurderes før konsesjon gis, der det er relevant.

Hensikten er å forebygge at uønskede aktører får innsikt, kontroll og innflytelse over eiendom som er av betydning for nasjonal sikkerhet.

---

[5] Lov om konsesjon ved erverv av fast eiendom (28. november 2003).

Boks 4.6 Critical Entities Resilience (CER) – nytt direktiv fra EU

EU arbeider med et nytt direktiv (CER-direktivet) for å øke sikkerheten for medlemslandenes evne til å levere kritiske varer og tjenester og sørge for at befolkningen har tilgang til disse også i en krisesituasjon. Direktivet omfatter tjenester som drikkevann, energi, helse, transport, digital infrastruktur, offentlige myndigheter, ytre rom og finanssektoren. Direktivet er ment å styrke EU-landenes motstandsdyktighet i samfunnet generelt.

4.3 Strategisk viktig infrastruktur

En infrastruktur kan bestå av fysiske elementer, som vannforsyning, undervannsinfrastruktur, installasjoner til havs, havner, flyplasser, eller for det ytre rom (bakkebasert og satellittbasert). Infrastruktur kan også bestå av digitale og mer høyteknologiske elementer som algoritmer og sensorer. Kartlegging, oppkjøp og investering i viktig infrastruktur kan skape muligheter for infiltrasjon, overvåking og sabotasje. Dette kan muliggjøre angrep eller forstyrrelser i den samfunnsfunksjonen som infrastrukturen understøtter. I tillegg kan import av teknologi fra utenlandske selskaper gjøre kritisk infrastruktur sårbar for fremtidige digitale angrep. Med bakgrunn i utfordringsbildet, er det viktig å vurdere ulike virkemidler for å sikre strategisk viktig infrastruktur som er av betydning for nasjonal sikkerhet.

Å sikre nasjonal kontroll over kritisk infrastruktur som går utover Norges landegrenser er utfordrende, men viktig. Dagens sikkerhetspolitiske situasjon understreker dette. For denne typen infrastruktur er Norge avhengig av internasjonalt samarbeid for å oppnå nasjonal kontroll.

Regjeringen vil kartlegge strategisk viktig infrastruktur for å identifisere hvilke allierte og nære partnere vi er mest avhengig av for å sikre nasjonal kontroll, og etablere et tett, forpliktende og forutsigbart samarbeid med disse.

4.3.1 Nasjonal skytjeneste

Mange norske virksomheter velger å kjøpe skytjenester fra store kommersielle, multinasjonale selskaper. Dette bidrar som oftest til å øke sikkerheten for virksomhetene siden de kan utfase utdaterte IT-løsninger, og få tilgang til sikker infrastruktur og profesjonelle sikkerhetsmiljøer. Samtidig er regjeringen opptatt av den samlede nasjonale avhengigheten til utenlandske skyleverandører, og hva konsekvensene av avhengigheten kan være ved potensielle kriser og konflikter. For noen virksomheter bør derfor bruk av skytjenester vurderes opp mot behovet for nasjonal kontroll og nasjonal beredskap.

Stadig flere virksomheter velger allmenne skytjenester for å imøtekomme behovet for nye og forbedrede IT-løsninger. For flere statlige virksomheter er det imidlertid en utfordring at det ikke finnes tilgang på funksjonelle og kostnadseffektive skytjenester med tilstrekkelig grad av nasjonal kontroll. Det kan føre til økt risiko dersom man likevel velger slike løsninger. Alternativet er at virksomhetene må velge lokale løsninger, noe som kan føre til høyere kostnader og begrenset tilgang til nye teknologiske verktøy. Problemet forventes å øke i tiden som kommer.

Regjeringen vil vurdere etablering av en nasjonal skytjeneste for å sikre økt nasjonal kontroll over kritisk IKT-infrastruktur og å beskytte viktig informasjon.

NSM fikk i november 2021 i oppdrag å utrede behovet for en slik skytjeneste. Flere sentrale aktører er involvert i arbeidet. Utredningsarbeidet er omfattende, komplekst og tar opp flere prinsipielle og tverrsektorielle problemstillinger, blant annet teknologiske, sikkerhetsrelaterte, organisatoriske, juridiske og økonomiske. Alternativene som

Boks 4.7 Andre lands nasjonale skytjenester

Flere av våre nærmeste naboland har aktiviteter knyttet til nasjonale skytjenester. Sverige har foreløpig ikke etablert en statlig tjeneste, men utført flere utredninger og avklaringer. Danmark har etablert en «GovCloud» som driftes av Statens It og som gir mulighet for å plassere applikasjoner i en offentlig eid og driftet skytjeneste. Tyskland har etablert «Die Bundescloud» som er en lukket skytjeneste som utvikles, eies og driftes av staten. Storbritannia har sin «G-cloud» som bidrar til å gjøre anskaffelser enklere med standardiserte rammeavtaler og godkjenning av leverandører.

vurderes skal ta utgangspunkt i nasjonal behandling og lagring av data. Sikkerhetsutfordringer som kan oppstå om en leverandør er underlagt utenlandske staters jurisdiksjon inngår i vurderingen. Det samme gjelder eiermodell, eksempelvis om den nasjonale skytjenesten skal eies og driftes av staten selv, men der kompetanse og innovasjonskraft fra det private benyttes. Utredningen skal leveres innen utgangen av 2022, slik at kvalitetssikring kan gjennomføres innen sommeren 2023.

4.3.2 Datasentre

Datasenter er en infrastruktur som lagrer og bærer digitale tjenester og data, og inngår som en viktig del av den digitale grunnmuren, på linje med infrastruktur for elektronisk kommunikasjon (ekom). Meld. St. 28 (2020–2021) *Vår felles digitale grunnmur* omtaler den økende sammensmeltingen av tradisjonell elektronisk kommunikasjon og IT-, sky- og datasentertjenester, hvor tredjepartsleverandører blir tettere integrert i ekomtilbydernes løsninger.

Mange kritiske digitale tjenester leveres i dag fra datasentre, og virksomheters avhengigheter til disse øker. Noen eksempler på tjenester som datasentre bærer er mobiltjenester, som tale og data, betalingstjenester, helse- og velferdstjenester, kritiske kommunikasjonstjenester, TV- og radiodistribusjon (DAB), Forsvarets kommunikasjonstjenester og fremtidens nød- og beredskapskommunikasjon.

Regjeringen vil spesifisere krav til sikkerhet og beredskap for datasentre, og har sendt på høring et lovforslag. Forslaget innebærer at det stilles krav om forsvarlig sikkerhet for datasentertjenester og at det innføres en registreringsplikt for datasenteraktører som medfører at myndighetene vil få en bedre oversikt over datasenternæringen i Norge. Forsvarssektoren unntas fra reguleringen av datasenteroperatører.

Datasentre og anonymt utleie kan misbrukes av kriminelle og statlige aktører. I ytterste konsekvens utfordrer slik utleie nasjonal sikkerhet ved at digitale angrep kan utføres fra Norge uten at norske myndigheter har mulighet for å lokalisere eiere eller utstyr.

Regjeringen vil utrede aktuelle tiltak for å avdekke og bekjempe utleie og bruk av datasentre til kriminelle og sikkerhetstruende formål. Konsekvensene av aktuelle tiltak for datasenternæringen og nasjonal datalagringsevne skal vurderes. Utredningen starter når ny ekomlov er fremmet for Stortinget.

Regjeringen ønsker også å gjennomføre en kartlegging av hvilke datasentre som leverer tjenester av betydning for kritiske samfunnsfunksjoner. En slik kartlegging vil avdekke om sektorer og deres redundans er konsentrert i et fåtall

Figur 4.4 Lefdal Mine Datacenter er bygd i en nedlagt gruve mellom Måløy og Nordfjordeid.

Foto: ABB

Boks 4.8 Drift og forvaltning av IT-løsninger i statlige virksomheter

På oppdrag fra Kommunal- og distriktsdepartementet er det gjennomført en ekstern kartlegging av i hvilken grad dagens organisering av drift og forvaltning av statlige IT-løsninger er egnet til å løse fremtidens krav og utfordringer når det gjelder kostnadseffektiv og sikker utvikling, drift og forvaltning av statens IT-løsninger. Kartleggingen viser blant annet at en betydelig andel av statlige virksomheter ikke har utarbeidet en sourcing- eller skystrategi. Samlet sett kan dette medføre sårbarheter på nasjonalt nivå ved at man mister oversikt over hvilke verdikjeder Norge er avhengig av og hvilke data som lagres hvor. Kartleggingen viser imidlertid at 65 prosent av virksomhetene etterlever i stor grad (54 prosent) eller i svært stor grad (11 prosent) grunnprinsippene for sikkerhetsstyring, utarbeidet av NSM.

datasentre, og om dette innebærer en konsentrasjonsrisiko. Kartleggingen skal omfatte datasentre i og utenfor Norge. For datasentre i Norge skal kartleggingen inkludere avhengigheter til ekom-nett og kraftleveranser som forsyner datasentrene. Det vil også være relevant å kjenne årsaken til at enkelte virksomheter benytter utenlandske datasentre, og hva som skal til for at de skal gå over til å benytte datasentre i Norge. Justis- og beredskapsdepartementet, i samarbeid med relevante departementer, vil vurdere tiltak på området med bakgrunn i kartleggingen. I samsvar med etablert ansvarsdeling mellom sivile sektorer og forsvarssektoren, ivaretas en tilsvarende kartlegging og oppfølging for forsvarssektoren av Forsvarsdepartementet.

Av hensyn til nasjonal sikkerhet er det på en del områder svært viktig at vi har kontroll på data som er lagret og at de er tilgjengelig i ulike deler av krisespennet. Regjeringen ønsker at de funksjonene som samfunnet er mest avhengig av skal leveres fra datasentre i Norge eller hos nære allierte og partnere. Dette fordrer forsvarlig sikkerhet på disse datasentrene. Drift av og lagring knyttet til informasjon av betydning for nasjonale sikkerhetsinteresser var blant annet en problemstilling som ble belyst i forbindelse med diskusjoner omkring IKT-infrastruktur i helseforetakene etter hendelsene i Helse Sør-Øst i 2018.[6] Samtidig har krigen i Ukraina tydeliggjort at det kan være sårbart å ha all slik infrastruktur plassert i eget land. Dette tilsier også for Norges del at vi må tilstrekkelig redundans, blant annet gjennom internasjonalt samarbeid og avtaler. Politiet åpnet et nytt datasenter i 2021, der også andre aktører i justissektoren er tilstede. Politiet jobber i tillegg med en konseptvalgutredning for et tilsvarende datasenter for å sikre redundans.

4.3.3 Graderte løsninger

I dag har vi en rekke systemer for gradert kommunikasjon. Mange av systemene utvikles, driftes og forvaltes av forsvarssektoren. Det er i dag ikke en felles aktør som har et tydelig ansvar for å ivareta sivile sektorers behov i dette arbeidet i et totalforsvarsperspektiv. Flere systemer er i dag under utvikling, innfasing eller utfasing. Det er videre en utfordring at mange av løsningene har ulike drifts- og forvaltningsmodeller på sivil side.

Regjeringen vil vurdere hvilket miljø eller aktør som er mest egnet til å ivareta sivile sektorers behov vedrørende graderte løsninger. Dette for å sikre en mer enhetlig leveranse av graderte systemer i sivile sektorer og effektiv samhandling mellom sivile sektorer og forsvarssektoren.

4.3.4 Digital kommunikasjonsinfrastruktur

Den digitale infrastrukturen bærer stadig større verdier og mer kritiske tjenester for det norske samfunnet. Det er et klart budskap i Hurdalsplattformen at regjeringen skal vurdere i hvilke tilfeller staten bør ta eierskap til digital infrastruktur, for å sikre disse verdiene. Regjeringen setter derfor ned et ekspertutvalg for å vurdere hvordan staten kan ivareta nasjonal kontroll over kritisk digital kommunikasjonsinfrastruktur. Kommunal- og distriktsdepartementet koordinerer dette arbeidet.

Sjøfiberkabler utgjør en viktig del av den digitale infrastrukturen på sokkelen. Ny teknologi kan påvise mulige trusler mot sjøfiberkabler, for eksempel ved å analysere akustiske signaler. Regjeringen styrker telekomberedskapen på norsk sokkel. Tiltak omfatter blant annet en støtteordning for innkjøp av ny teknologi som gjør at trusler mot sjøfiberkabler kan identifiseres, midler til å gjennomføre undersøkelser av viktige

[6] Innst. 386 S (2017–2018) Innstilling til Stortinget fra helse- og omsorgskomiteen.

sjøfiberstrekk og innkjøp av utstyr som kan avdekke forstyrrelser av satellittbaserte tjenester, for eksempel for GPS på norsk sokkel.

4.3.5 Romvirksomhet av betydning for nasjonal sikkerhet

Etterretnings- og sikkerhetstjenestene har i økende grad løftet frem betydning av romvirksomhet for nasjonal sikkerhet og nasjonale sikkerhetsinteresser de seneste årene. Dette har blitt forsterket av endringene i den sikkerhetspolitiske situasjonen i Europa og verden, spesielt det siste året. Det vil derfor være stadig viktigere med forebyggende sikkerhet på dette området, både i det ytre rom og for bakkebaserte installasjoner. Norge er en viktig romnasjon, og vår geografiske plassering er attraktivt for romaktiviteter, blant annet for oppskytning av satelitter og utplassering av bakkebaserte sensorer.

Regjeringen vurderer at romaktiviteter i det ytre rom og på bakken er av strategisk betydning for Norges utenriks-, sikkerhets- og forsvarspolitiske forhold. I arbeidet med ny romlov legger regjeringen vekt på hensynet til ivaretakelse av nasjonale sikkerhetsinteresser. I tillegg søker regjeringen å identifisere ytterligere hvilke områder innenfor romvirksomhet hvor hensynet til nasjonal sikkerhet spesielt gjør seg gjeldende. For å ivareta de tverrsektorielle hensynene innenfor romvirksomhet drøftes konkrete saker i det tverrdepartementale romsikkerhetsutvalget.

4.4 Strategisk viktige naturressurser

Naturressurser kan være av betydning for nasjonal sikkerhet. I forbindelse med implementering av sikkerhetsloven er det identifisert grunnleggende nasjonale funksjoner innenfor blant annet vannforsyning, kraftforsyning, matvareforsyning og petroleumsvirksomhet. Andre naturressurser er per i dag ikke definert som avgjørende for nasjonal sikkerhet. Imidlertid bør naturressurser som mineralforekomster og jord- og skogressurser vurderes med utgangspunkt i deres betydning for nasjonal sikkerhet. Utenlandsk eierskap over strategisk viktige naturressurser kan på sikt utfordre vår egen råderett over disse ressursene.

Figur 4.5 Naturressurser kan være av betydning for nasjonal sikkerhet.

Foto: Shutterstock

Boks 4.9 Betydningen av energi-, mineral- og vann- og skogressurser

Energiressurser

Energiressursene har vært og er en viktig del av grunnlaget for bosetting, industri og næringsliv i hele Norge. Regjeringen vil at våre fornybare energiressurser skal tas i bruk og foredles i Norge. Regjeringens klimapolitikk skal også bidra til et sterkt nasjonalt eierskap til naturressurser.

Flere land søker informasjon om norske beslutningsprosesser om energiproduksjon. Virksomheter i petroleumssektoren må være forberedt på at uvedkommende vil forsøke å få tilgang til informasjon. Gitt energidimensjonen av Russlands krigføring i Ukraina, er dette ytterligere aktualisert. Regjeringen har i 2022 iverksatt en rekke tiltak for å sikre petroleumssektoren.

Det er i dag stor grad av nasjonalt eierskap innen petroleumssektoren. Konsesjonssystemet sikrer nasjonal kontroll over hvilke selskaper som får rettigheter til utvinningstillatelser på norsk sokkel og viktige beslutninger krever myndighetssamtykke. Olje- og energidepartementet kan av hensyn til nasjonal sikkerhet nekte adgang til og utøvelse av petroleumsvirksomhet hvis søkeren eller rettighetshaveren faktisk kontrolleres av en stat utenfor EØS eller av statsborgere fra slik stat.

Energilovgivningen stiller krav til både fysisk og digital sikkerhet m.m., og har et bredere virkeområde enn sikkerhetsloven. Dette regelverkets formål er imidlertid ikke å ivareta nasjonal sikkerhet, men kraftforsyningen som sådan. Regelverket skal ivareta forsyningssikkerhet for kraft, og stiller krav til forebyggende sikkerhet og beredskap for både villede og ikke-villede hendelser.

Mineralressurser

Samfunnsutviklingen har vist at det er et økende behov for mineraler, blant annet som følge av det grønne skiftet. Mineraler kan være kritiske for viktige samfunnsformål og for teknologiutvikling på strategisk viktige områder. Internasjonalt har det vist seg at kontroll over råvareproduksjonen kan benyttes for å monopolisere verdikjedene. Mineralressurser kan ha betydning for nasjonal sikkerhet. Det kan derfor være ønskelig å forebygge at uønskede utenlandske aktører får tilgang til mineralressurser i Norge, på land eller på havbunnen. Dette kan både være av hensyn til deres nasjonale teknologiutvikling, potensiell militær bruk av sivil teknologi og eventuelt gjennom eiendommens plassering i nærheten av skjermingsverdige objekter eller infrastruktur.

Vannforsyning

Utvikling i trusselbildet de senere årene har vist at det er behov for økt oppmerksomhet om sikkerheten ved vannforsyning. Kommunale vannverk har vært utsatt for digitale angrep på infrastruktur for vann og avløp i løpet av 2021. Norsk vannforsyning må være rustet for å stå imot både tilsiktede handlinger og ikke-tilsiktede hendelser. Forebygging og god beredskap i vannforvaltningen er viktig for samfunnssikkerheten. Trygg vannforsyning er en grunnleggende nasjonal funksjon definert i henhold til sikkerhetsloven.

Skog- og landbruksressurser

Eierskap til skog- og landbrukseiendommer kan være av betydning for nasjonal sikkerhet når eiendommen har en strategisk beliggenhet, eller ligger i nærheten av skjermingsverdige objekter eller infrastruktur. I tillegg kan totaliteten av utenlandsk eierskap av skog- og landbrukseiendom utgjøre en sårbarhet for nasjonal sikkerhet ved at store landområder ikke eies nasjonalt. Nasjonalt eierskap og kontroll over skogeiendommer vil være viktig. Regjeringen vil arbeide videre for å sikre norsk eierskap på skogeiendommer gjennom konsesjonslovgivningen. I tillegg kan konsesjonslovgivning for landbrukseiendom bidra til nasjonal kontroll og langsiktig og god forvaltning av landbruksressursene.

4.4.1 Hvordan sikre kontroll over strategisk viktige naturressurser

Regulatoriske virkemidler er det viktigste virkemiddelet for å sikre nasjonal kontroll over strategisk viktige naturressurser og kan brukes for å forebygge at enkelte aktører får tilgang til å kjøpe noen typer eiendom eller ressurser. Statlig eierskap er et av flere virkemidler som har vært benyttet for å sikre råderetten over, og i noen grad inntekter fra, landets store naturressurser. Samtidig er naturressurser stedbundet. Staten vil derfor uavhengig av eierskap ha en viss kontroll over ressursene, og kan på ulike måter regulere forvaltningen av dem. Nasjonal kontroll over naturressurser dreier seg ikke kun om eiendom, men også om vår nasjonale evne til å utvinne og utnytte ressursene.

Et viktig element for å vurdere behovet for nasjonal kontroll over naturressurser, er hvor de ligger geografisk, for eksempel i områder av særlig betydning for nasjonal sikkerhet eller suverenitetshevdelse. Geografisk er Svalbard og nordområdene særlig relevant på grunn av sin strategiske plassering, men også beliggenhet i nærheten av skjermingsverdige objekter vil være av

Boks 4.10 Meraker Brug

Meraker Brug var en av de største private skog- og utmarkseiendommene i Norge, og har historie tilbake til tidlig på 1700-tallet. Eiendommene har et samlet areal på om lag 1,2 millioner mål, hvorav mer enn 200 tusen mål er produktiv skog. Eiendommene ligger i Meråker, Stjørdal, Malvik og Steinkjer kommune. Statskog SF har inngått avtale om kjøp av 94 prosent av aksjene i AS Meraker Brug og er i prosess for å kjøpe de resterende. Kjøpet ble godkjent av Stortinget i november 2022. Regjeringen har gjennom statlig eierskap sikret eiendommen på norske hender. Med dette kjøpet går Norges største privateide eiendom over i offentlig eie og felles naturressurser kommer fellesskapet til gode.

Figur 4.6 Store områder sør i Meråker med Fonnfjellet og Skarvene i bakgrunnen.

Foto: AS Meraker Brug

stor betydning. I tillegg kan naturressurser være viktige for nasjonal sikkerhet basert på hvilke behov de dekker, for eksempel forsyningssikkerhet, energi, vann eller mat.

Det er ikke nødvendigvis et mål å ha nasjonalt eierskap over naturressurser som er avgjørende for nasjonal sikkerhet. Det kan snarere være viktig å ha nasjonal kontroll gjennom andre virkemidler, for å forebygge at andre aktører får eierskap eller kontroll over slike naturressurser. Dette gjelder også der en naturressurs i dag ikke vurderes å være av betydning for nasjonal sikkerhet, men som på lengre sikt kan få betydning for vår nasjonale sikkerhet dersom en annen aktør får innflytelse eller kontroll over den.

Norge må ha relevant teknologisk kompetanse om eksempelvis mineralforekomster, utvinning av vannressurser, olje og gass, og vindkraft. Dette kan bidra til å redusere vår egen avhengighet og sårbarheter.

4.5 Strategisk viktig teknologi

Den teknologiske utviklingen går stadig raskere. Skillet mellom sivil og militær teknologi blir mindre, samtidig som stadig flere aktører får tilgang til den samme teknologien. Teknologiutviklingen påvirker blant annet internasjonale relasjoner og hvilke virkemidler stater og ikkestatlige aktører benytter seg av i fred, krise og væpnet konflikt. Dersom Norge skal kunne utnytte teknologiutviklingen til å styrke nasjonal sikkerhet, er det avgjørende med nasjonal kompetanse, forskning og utvikling, i tillegg til å skape næringsutvikling. Som en liten nasjon, har ikke Norge ressurser til å ha gode fagmiljøer innenfor alle nye og banebrytende teknologier. Det er derfor viktig å vurdere hvilke teknologier som er av betydning for nasjonal sikkerhet og på hvilke områder vi har et særlig behov for nasjonal kompetanse. Eksempler kan være kvanteteknologi, kunstig intelligens, datavitenskap eller romteknologi.

Innenfor definerte strategisk viktige teknologiområder kan nasjonalt eierskap og kontroll handle om å ha tilstrekkelig nasjonal spesialistkompetanse, å hindre utenlandsinvesteringer som truer nasjonal sikkerhet eller å ha et klart eksportkontrollregelverk for kunnskapsoverføring i og fra Norge. Det vises her også til Meld. St. 17 (2020–2021) *Samarbeid for sikkerhet – Nasjonal forsvarsindustriell strategi for et høyteknologisk og fremtidsrettet forsvar* og Forsvarsdepartementets strategi for å beskytte norskutviklet forsvarsteknologi. Strategien er innrettet mot nasjonale teknologiske kompetanseområder og omfatter også andre teknologiområder som defineres som beskyttelsesverdig, spesielt nye og banebrytende teknologier som romteknologi.

4.5.1 Nasjonalt senter for anvendt kryptologi

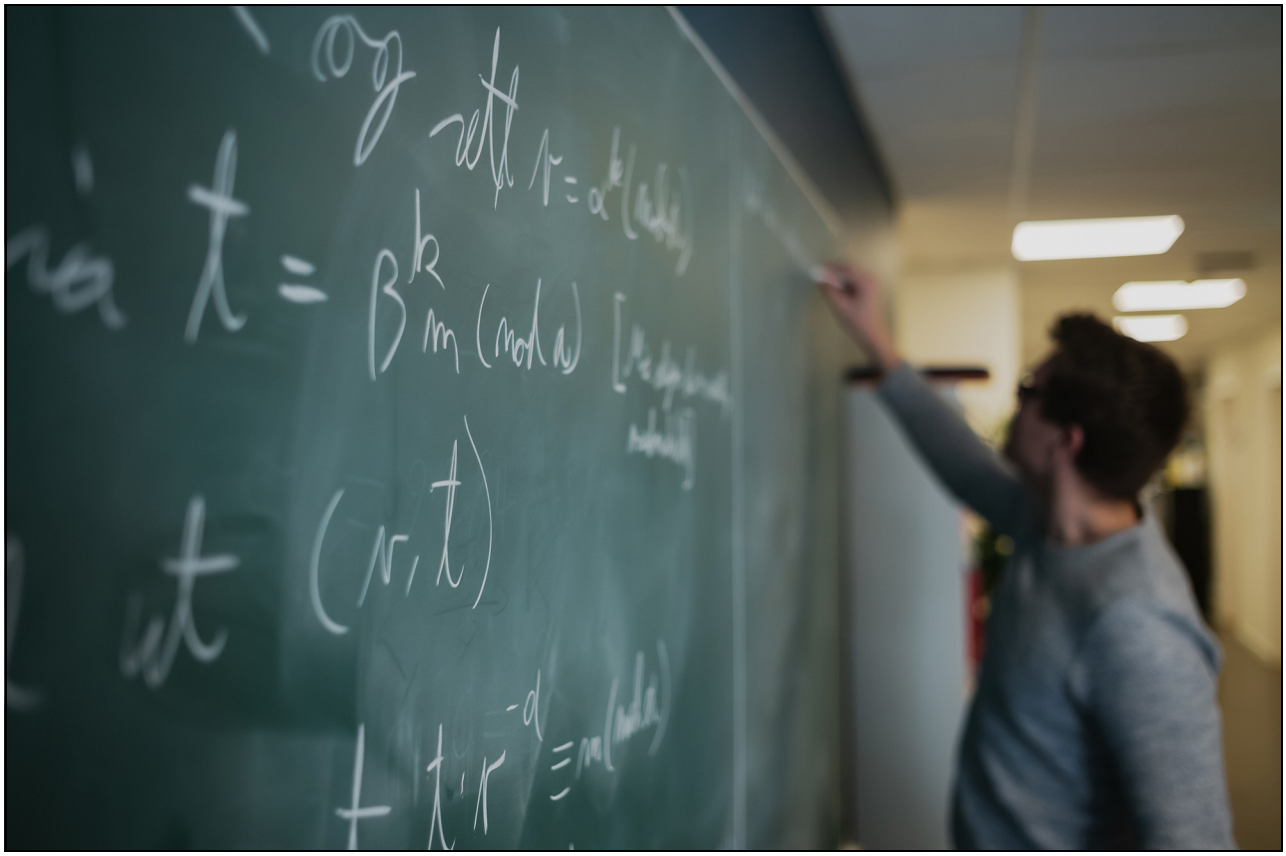
Kryptologi er en viktig del av nasjonalt forebyggende sikkerhetsarbeid og avgjørende for å beskytte sikkerhetsgradert informasjon. Teknologiutviklingen, med raskt økende regnekraft, reduserer sikkerhetsnivået i dagens kryptoalgoritmer. I noen tilfeller må vi ta høyde for at kryptert informasjon vi anser som sikret i dag, vil kunne bli lagret av uvedkommende og dekryptert en gang i fremtiden. Problemstillingen aktualiseres ytterligere av utviklingen innen kvantedatamaskiner. Det er dermed helt nødvendig å sikre at vi har kompetansen som kreves for å møte utfordringene innen kryptologi. Det er behov for kryptologikompetanse innen akademia, kryptoindustrien og hos myndighetene.

Norge er en betydelig leverandør av høygradert kryptografi til andre NATO-land. Disse leveransene danner et viktig grunnlag for samarbeid som er av betydning for nasjonal sikkerhet. Det er helt nødvendig å sikre den nasjonale evnen og kompetansen som kreves for å møte kryptoutviklingen og å opprettholde posisjonen som en troverdig leverandør av kryptoløsninger til NATO.

NSM er styrket med 6,2 mill. kroner i 2022 for å etablere et nasjonalt senter for anvendt kryptologi. Senteret skal bidra til at Norge opprettholder og videreutvikler nasjonal kryptokompetanse og gjøre Norge rustet til å møte fremtidens utfordringer innenfor kryptologi. NSMs oppgraderte høyteknologiske kryptolaboratorium er en sentral del av senteret.

4.5.2 Kraftsamle kompetanse og kapabilitetsbygging innen ulike teknologiområder

Ulike teknologier forsterker og interagerer med hverandre. Kunstig intelligens ved bruk av maskinlæring og stordata, tingenes internett, 5G/6G, utviklingen av kvanteteknologi og andre banebrytende teknologier er eksempler på dette. Bruken av nye teknologier på sikkerhetsområdet vil øke, og balansen mellom angrepskapasiteter og forsvarskapasiteter vil utfordres og finne stadig nye former.



Figur 4.7 NSM har forsket på kryptoanalyse og sikker kryptografi for nasjonal sikkerhet siden 1940-tallet.
Foto: NSM

Et eksempel på dette er at kompleks infrastruktur for telekommunikasjon i økende grad vil styres av automatisk analyse basert på kunstig intelligens. Denne teknologien muliggjør selvreparerende nettverk med svært kort tid for rekonfigurasjon etter en hendelse, men åpner samtidig en arena for nye og avanserte angrep. Teleselskapene har kontroll over hvordan og i hvilken grad dette skal introduseres, og ekomloven stiller krav til forsvarlig sikkerhet.

Et annet eksempel er kvanteteknologi. Kvantedatamaskiner vil kunne løse enkelte typer kompliserte oppgaver som er uløselige med dagens klassiske datamaskiner. Det er antakelig bare et spørsmål om tid før kvantedatamaskiner vil kunne knekke noen av de mest vanlige krypteringsmekanismene som nå er i bruk.

I tillegg viser den teknologiske utviklingen, som tingenes internett, at det vil bli mulig å inkludere sensorer og nettilkobling til svært mange, kanskje de fleste, gjenstander vi omgir oss med. Tett internasjonalt samarbeid er en viktig arena for standardisering og nødvendig regulering.

Selv om det er vanskelig å vite resultatet av den teknologiske utviklingen, er konsekvensene trolig betydelige. Regjeringen vil følge med på utviklingen og bidra til at det finnes gode og robuste norske kunnskapsmiljøer innenfor de ulike teknologiområdene.

4.6 Nordområdene

Nordområdene er Norges viktigste strategiske satsingsområde, og regjeringen vil gi ny giv til nordområdepolitikken. Regjeringen vil vektlegge samarbeid med andre land og økt aktivitet på land i Norge. Regjeringen er opptatt av å sikre norsk eierskap til viktig infrastruktur, eiendom og nasjonal kontroll over naturressurser i nordområdene.

Samtidig kan utenlandsk etterretningsvirksomhet i nordområdene svekke norske myndigheters handlingsrom. Trusselen vil fortsatt være størst fra russiske og kinesiske etterretningstjenester. Det forventes at russiske etterretningstjenester vil fortsette sin kartlegging av sivil og militær infrastruktur i regionen, mens Kina og kinesiske aktører vil fortsette å prioritere sin langsiktige posisjonering i nordområdene, blant annet

for fremtidig ressursutvinning. Statlige virkemidler for å bidra til nasjonal sikkerhet i nordområdene bør vurderes i lys av regionens strategiske betydning. Eiendommer, infrastruktur, naturressurser og bedrifter av betydning for nasjonal sikkerhet bør derfor vurderes særskilt med tanke på deres geografiske plassering langs kysten, i grenseområdene og i nærheten av viktig infrastruktur.

Større byer og mange kyststrøk i Nord-Norge har en god demografisk utvikling. Det er imidlertid områder med spredt bosetning og store avstander hvor det er nedgang i folketallet og store endringer i den demografiske befolkningssammensetningen.[7] De mindre sentrale kommunene og de befolkningsmessig minste kommunene har de største utfordringene, og det er også her det er vanskeligst å rekruttere arbeidskraft og tjenestene er under størst press. Det er særlig i Nord-Troms og i Finnmark at disse utfordringene er størst.

Gitt nordområdenes strategiske beliggenhet og betydning, kan disse utviklingstrekkene få konsekvenser for kommunene og statens håndtering av uønskede hendelser som kan true nasjonal sikkerhet. Dette representerer i seg selv en sårbarhet ved at kommunene er mer avhengig av private investeringer for å utføre lovpålagte oppgaver og sørge for innbyggernes velferd. Kommuner kan mangle tilstrekkelig kompetanse og erfaring for å kunne håndtere saker av betydning for nasjonal sikkerhet, slik som å gjøre vurderinger som bør ligge til grunn for å sette opp russiske krigsminnesmerker, vurdere utenlandske eiendomsoppkjøp eller enkelte former for turisme.

Levende og livskraftige sivile samfunn i Nord-Norge, og spesielt øst i Finnmark, er en viktig del av norsk sikkerhet. Det å sikre norsk bosetning i nærområdene mot Russlands grense bidrar til å underbygge norsk suverenitet og norske interesser i regionen.

Regjeringen har gjennom Prop. 78 S (2021–2022) styrket etterretnings- og sikkerhetstjenestene og politiets evne til å forebygge sikkerhetstruende virksomhet, særlig i våre tre nordligste fylker.

Svalbard

Svalbard har stor strategisk betydning for Norges muligheter i nordområdene og Arktis, og svalbardpolitikken er derfor en viktig del av regjeringens nordområdepolitikk. Nasjonal kontroll bidrar blant annet til å nå de stortingsforankrede målene for svalbardpolitikken. Det er lang tradisjon for bred politisk enighet om hovedlinjene i svalbardpolitikken, og målene har ligget fast over lengre tid:

- Konsekvent og fast håndhevelse av suvereniteten
- Korrekt overholdelse av Svalbardtraktaten og kontroll med at traktaten blir etterlevet
- Bevaring av ro og stabilitet i området
- Bevaring av områdets særegne villmarksnatur
- Opprettholdelse av norske samfunn på øygruppen

Statens viktigste virkemidler i samfunnsutviklingen på Svalbard er de helhetlige meldingene til Stortinget om Svalbard, lovgivning, økonomiske virkemidler, ulike former for eierskap, blant annet for eiendom, grunn og infrastruktur, samt strategier. Målene for svalbardpolitikken forutsetter at regelverk og rammer for Svalbard blir vurdert og tilpasset etter samfunnsutviklingen, samt etter øvrige relevante utviklingstrekk.

Stemmerett og statlig eierskap

På Svalbard tas virkemidler i bruk som ikke benyttes på fastlandet. Dette har sammenheng med at det er særlige rammer for Svalbard, herunder at utlendingsloven ikke gjelder. De seneste årene har man hatt en økt tilflytning til Longyearbyen direkte fra utlandet. Longyearbyen lokalstyre, som er det lokale folkevalgte organet for Longyearbyen, forvalter verdier og funksjoner av nasjonal betydning. De som sitter i lokalstyret må ha god kjennskap til målene i svalbardpolitikken og de særlige rammebetingelsene for Svalbard. Som følge av dette er det nå innført et krav om at utenlandske statsborgere har tre års botid i en kommune på fastlandet for å kunne stemme og stille til valg i Longyearbyen.

Statlig eierskap er videre et tiltak som er benyttet på Svalbard. Staten eier direkte eller indirekte flere selskaper på Svalbard. Det direkte eierskapet består per i dag av Store Norske Spitsbergen Kulkompani AS (SNSK), Kings Bay AS, Bjørnøen AS og Universitetssenteret på Svalbard AS, som alle er statsaksjeselskaper. Begrunnelsen for statens eierskap i disse selskapene er blant annet å bidra til å understøtte de overordnede målene i svalbardpolitikken.

Staten er også en stor grunneier på Svalbard. Statens grunneiendom omfatter all grunn i og rundt Longyearbyen. I 2016 kjøpte også staten grunneiendommen Austre Adventfjord ved Long-

[7] «Regionale utviklingstrekk 2021», Rapport, Kommunal- og moderniseringsdepartementet.

Figur 4.8 Svalbard har stor strategisk betydning for Norges muligheter i nordområdene og Arktis.

Foto: Shutterstock

yearbyen. Totalt utgjør statens direkte eierskap 98,75 prosent av grunnen på Svalbard.

Statlig direkte eierskap i selskaper, statlig eierskap til grunn og norsk lovgivning gir oss et godt utgangspunkt for å forvalte Svalbard til fellesskapets beste.

5 Økonomiske og administrative konsekvenser

Det prinsipielle utgangspunktet er at forebyggende nasjonalt sikkerhetsarbeid har som formål å øke sikkerheten i samfunnet. Sikkerhet og sikringstiltak kan være kostnadskrevende, og de foreslåtte tiltakene i meldingen vil kunne medføre politiske og økonomiske kostnader for det norske samfunnet. Imidlertid kan manglende sikkerhet få svært store samfunnsmessige og økonomiske konsekvenser. Tiltakene må derfor være forståelige og forholdsmessige og brukes på en slik måte at det bidrar til forutsigbarhet og tillit, avveier ulike hensyn og samtidig bidrar til å ivareta nasjonal sikkerhet.

Vesentlige deler av det nasjonale sikkerhetsarbeidet og arbeidet med digital sikkerhet skjer i hver enkelt sektor, basert på sikkerhetsloven og relevant sektorlovgivning, samt spesifikke krav og anbefalinger i arbeidet med digital sikkerhet. Arbeidet skal være en integrert del av den ordinære styringen. Hvis risiko- og sårbarhetsbildet endrer seg, er det viktig at tiltakene og virkemiddelapparatet justeres deretter. Av sikkerhetsloven følger det at skal gjøres kost-nytte-vurderinger før sikringstiltak besluttes. Regjeringen har en ambisjon om å styrke nasjonal sikkerhet på flere sentrale områder. I meldingen vises det til en rekke tiltak. Eventuelle utgifter som går ut over gjeldende budsjettrammer, vil regjeringen komme tilbake til i forbindelse med de årlige budsjettforslagene.

Justis- og beredskapsdepartementet

t i l r å r :

Tilråding fra Justis- og beredskapsdepartementet 9. desember 2022 om Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet blir sendt Stortinget.

Bestilling av publikasjoner

Departementenes sikkerhets- og serviceorganisasjon
publikasjoner.dep.no
Telefon: 22 24 00 00

Publikasjonene er også tilgjengelige på
www.regjeringen.no

Omslagsillustrasjon: Konsis

Trykk: Departementenes sikkerhets- og serviceorganisasjon – 12/2022