STORTINGET

Innst. 247 S

(2022–2023)

Innstilling til Stortinget
fra justiskomiteen

Meld. St. 9 (2022–2023)

Innstilling fra justiskomiteen om Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet

Til Stortinget

1. Sammendrag

En av statens viktigste oppgaver er å ivareta nasjonal sikkerhet. Regjeringen tydeliggjør i denne meldingen strategisk retning, prioriteringer og tiltak for å ivareta nasjonal og digital sikkerhet på utvalgte områder. Tiltak omfatter blant annet regulering, nasjonalt eierskap og kontroll, bedre oversikt over verdier og økt kompetanse og kunnskap.

Meldingen er avgrenset mot det brede samfunnssikkerhets- og beredskapsperspektivet.

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.

Regjeringen beskriver i meldingen at vi står overfor et skjerpet risikobilde og utfordres av stater med sikkerhetspolitiske ambisjoner som ikke samsvarer med våre nasjonale sikkerhetsinteresser. Regjeringen vil derfor 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.

En grunnleggende forutsetning for å ivareta nasjonal sikkerhet er etter regjeringens mening 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 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.

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.

Økonomiske og administrative konsekvenser omtales i siste kapittel i meldingen.

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 at det 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.

2. Komiteens merknader

Komiteen, medlemmene fra Arbeiderpartiet, Kamzy Gunaratnam, Odd Harald Hovland og Maria Aasen-Svensrud, fra Høyre, Ingunn Foss og Sveinung Stensland, fra Senterpartiet, Ivar B. Prestbakmo og Else Marie Rødby, fra Fremskrittspartiet, lederen Per-Willy Amundsen og Tor André Johnsen, fra Sosialistisk Venstreparti, Andreas Sjalg Unneland, og fra Venstre, Ingvild Wetrhus Thorsvik, viser til Meld. St. 9 (2022–2023) Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet.

Innledning

Komiteen viser til at det ble avholdt åpen høring i saken 14. februar 2023, der åtte instanser deltok. I tillegg har komiteen mottatt ni skriftlige innspill.

Komiteen vil understreke at det å ivareta den nasjonale sikkerheten er en av statens viktigste oppgaver. Komiteen viser til at Russlands invasjon av Ukraina danner et svært alvorlig bakteppe for arbeidet med denne meldingen, der det norske samfunnet står i en langt mer uforutsigbar sikkerhetspolitisk situasjon enn vi har gjort på svært mange år. Et komplekst utfordringsbilde der trusselaktører tar i bruk stadig nye virkemidler for å ramme Norge, utfordrer den nasjonale sikkerheten innenfor alle samfunnsområder.

Komiteen deler regjeringens overordnede vurdering av behovet for kraftfulle tiltak for å ivareta nasjonal sikkerhet. Sammensatte trusler er komplekse og berører alle samfunnsområder. En slik uforutsigbarhet stiller store krav til samarbeid på tvers av virksomheter, sektorer og landegrenser.

Komiteen viser til at rask teknologisk utvikling og digitaliseringen av samfunnet i denne sammenhengen byr på både muligheter og utfordringer.

Komiteen mener at motstandskraft og robusthet bygges best i fredstid og gjennom et bredt spekter av virkemidler. Komiteen merker seg at innholdet i meldingen har til formål å styrke samfunnets kollektive motstandskraft gjennom forsterket nasjonal kontroll og digital sikkerhet. Komiteen er enig i at staten må innta en aktiv rolle i arbeidet for nasjonal kontroll over naturressurser, strategisk viktige virksomheter, kritisk infrastruktur og teknologi for å ivareta nasjonal sikkerhet.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet, Fremskrittspartiet og Venstre, ser positivt på at regjeringen ønsker å 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. I denne forbindelse vil flertallet særlig påpeke risikoen knyttet til store datamengder og kunstig intelligens. Det er ikke ønskelig at en fremmed stat skal få tilgang til store mengder informasjon om norske rettssubjekt, selv om hver enkelt informasjonsbit kan framstå tilforlatelig og ikke være verken gradert eller skjermingsverdig. Samlet sett kan store mengder data benyttes til blant annet å identifisere mønstre og trene kunstig intelligens på en måte som verken tar hensyn til personvern eller er ønskelig fra et nasjonalt sikkerhetsperspektiv.

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet viser til at regjeringen løftet fram behovet for et forsterket og mer koordinert arbeid med digital sikkerhet som et sentralt punkt i Hurdalsplattformen, herunder økt kapasitet til å kjempe mot cyberkriminalitet, nasjonal datalagringsevne og digital beredskap.

Disse medlemmer viser til at da krigen i Ukraina brøt ut vinteren 2022, var regjeringen raskt ute med å fremme forslag for Stortinget med helt nødvendig styrking av vesentlige sider ved norsk beredskap og den operative evnen for å kunne respondere på den aktuelle situasjonen. Blant annet foreslo regjeringen en rekke tiltak med formål om raskt å kunne øke innsatsen mot digitale angrep, både den sivile beredskapen og den nasjonale responsfunksjonen gjennom Nasjonal sikkerhetsmyndighet (NSM), for bedre å kunne forebygge, avdekke og koordinere håndteringen av alvorlige digitale angrep, jf. Prop. 78 S (2021–2022). Et sentralt tiltak i så måte er etableringen av et nasjonalt varslingssystem for digital infrastruktur og bevilgninger slik at flere virksomheter kan knytte seg til digitale innbruddsalarmer med varsling til NSM. Disse medlemmer vil også påpeke betydningen av at NSMs kapasitet til å yte bistand til virksomheter som har blitt utsatt for cyberangrep, er økt.

Disse medlemmer viser til at regjeringen samlet foreslo og fikk gjennomslag for 200 mill. kroner til styrking av vår digitale sikkerhet i 2022. Det vil bidra til økt digital sikkerhet på lokalt, regionalt og nasjonalt nivå. Bevilgningen skal bl.a. styrke NSMs evne til koordinering, hendelseshåndtering, analyse og bistand til virksomheter, samt bedre evnen til å oppdage, verifisere og varsle om koordinerte og alvorlige dataangrep. Disse medlemmer viser til at disse midlene er videreført i statsbudsjettet for 2023.

Disse medlemmer viser for øvrig til at det i statsbudsjettet for inneværende år ble øremerket 71 mill. kroner til videreføring av økt kapasitet i politiet til å avdekke sammensatte trusler og etterretning i de tre nordligste fylkene.

Disse medlemmer viser til at kommunene er attraktive mål for digitale angrep. Derfor har det vært av vesentlig betydning at regjeringen har styrket kommunenes evne til å oppdage, forebygge og håndtere digitale angrep. Dersom kritiske samfunnsfunksjoner som forsyningen av strøm, vann eller datasystemer settes ut av spill, vil dette ramme befolkningen hardt. Derfor var det helt sentralt at regjeringen i fjor foreslo å styrke den digitale sikkerheten i kommunene ved å legge til rette for at kommunene kan knytte seg til et cybersikkerhetssamarbeid (responsmiljø eller tilsvarende), samt etablering av en ordning for å styrke kommunenes kompetanse og kapasitet til å forebygge og håndtere digitale hendelser.

Komiteens medlemmer fra Høyre, Fremskrittspartiet og Venstre viser til at digital sikkerhet var et prioritert område for Solberg-regjeringen. I Meld. St. 5 (2020–2021) Samfunnssikkerhet i en usikker verden var digital sikkerhet et av syv områder som Solberg-regjeringen rettet oppmerksomhet mot. Videre viser disse medlemmer til at Stortinget den 10. april 2018 behandlet Meld. St. 38 (2016–2017) IKT-sikkerhet – Et felles ansvar. Dette var den første stortingsmeldingen om IKT-sikkerhet og la grunnlaget for Solberg-regjeringens arbeid med å gjøre Norge enda tryggere – også på det digitale området.

Disse medlemmer viser til at Nasjonalt cybersikkerhetssenter ble etablert i 2019. Formålet med senteret var blant annet å styrke samarbeidet mellom de ulike IKT-sikkerhetsmiljøene, slik at ulike aktører opererer i et felles risikobilde og med samme situasjonsforståelse, og å styrke samarbeidet mellom myndighetene og næringslivet. Videre viser disse medlemmer til at etableringen av Nasjonalt cyberkrimsenter (NC3) ved Kripos var et sentralt grep for politiets innsats for å bekjempe trusler og kriminalitet i det digitale rom. Sente-

ret utvikler metoder og gir bistand til politidistriktene i tillegg til at de etterforsker egne saker innen cyberkriminalitet.

Disse medlemmer viser også til at Solberg-regjeringen opprettet Felles cyberkoordineringssenter (FCKS), som består av NSM, Etterretningstjenesten, PST og Kripos. Senteret har som oppgave å fremskaffe tidsriktig informasjon og beslutningsgrunnlag til den operative og strategiske ledelsen om trusler og sårbarheter. Disse medlemmer mener FCKS har en koordineringsfunksjon mellom tjenestene.

Videre viser disse medlemmer til at Solberg-regjeringen lanserte Nasjonal strategi for digital sikkerhet og Nasjonal strategi for digital sikkerhetskompetanse i 2019. I strategien for digital sikkerhet var bekjempelse av IKT-kriminalitet et av fem prioriterte områder. Med strategiene ønsket Solberg-regjeringen å etablere et felles grunnlag for å håndtere digitale sikkerhetsutfordringer som følger av en rask og gjennomgående digitalisering av det norske samfunnet. Disse medlemmer mener det er helt sentralt å mobilisere alle relevante aktører i innsatsen mot IKT-kriminalitet. Strategien for digital sikkerhet vektlegger et styrket offentlig-privat, sivil-militært og internasjonalt samarbeid.

Disse medlemmer viser til at Solberg-regjeringen utarbeidet ny norsk kryptopolitikk, som blant annet innebar å arbeide for gode reguleringer som ivaretar rettssikkerheten og personvernet til norske innbyggere og bedrifter. Dette gjelder særlig når politiet tar i bruk sin lovlige tilgang til informasjon, som er nødvendig for kriminalitetsbekjempelse og opprettholdelse av lov og orden i det digitale rom.

Disse medlemmer peker på at Forum for nasjonal IKT-sikkerhet ble etablert i 2018, med deltakere fra myndigheter, næringsliv, akademia og interesse- og bransjeorganisasjoner. Disse medlemmer mener det offentlig–private samarbeidet på dette området er meget viktig for å møte et IKT-risikobilde i konstant endring, og samarbeidet har allerede fått effekt i det strategiske arbeidet. Disse medlemmer mener det er behov for å styrke det offentlig-private samarbeidet ytterligere i årene fremover. Næringslivet besitter betydelig kompetanse og ressurser som er sentralt for å forebygge, avdekke og håndtere trusler. Arenaer hvor private virksomheter og sikkerhetsaktører samarbeider med myndighetene, bør videreutvikles, slik at møteplassene blir arena for blant annet informasjonsutveksling og samarbeid om utvikling av regelverk, tiltak og prosedyrer. Disse medlemmer mener det må bli lettere å dele trusselvurderinger og etterretningsinformasjon for løpende å øke forståelsen for trusselbildet på tvers av samfunnssektorer.

Disse medlemmer peker også på at Solberg-regjeringen satte ned IKT-sikkerhetsutvalget for å se på regelverk og organisering innenfor IKT-sikkerhetsområdet, med mål om å oppnå økt IKT-sikkerhet. Utvalgets rapport ble levert høsten 2018. Disse medlemmer mener det er behov for en oppdatering og harmonisering av regelverket om digital sikkerhet. Det er også behov for å harmonisere det norske regelverket med regelverket som gjelder i EU, NATO-samarbeidet og særlig de andre nordiske landene. Ny lov om digital sikkerhet bør utformes slik at den gjennomfører NIS2-direktivet, slik at Norge holder samme nivå i det digitale sikkerhetsarbeidet som EU.

Disse medlemmer viser også til at Solberg-regjeringen fikk på plass en ny sikkerhetslov, som trådte i kraft 1. januar 2019. Den er sentral i det forebyggende arbeidet og har som formål å trygge Norges suverenitet, territorielle integritet og demokratiske styreform og andre nasjonale sikkerhetsinteresser gjennom å forebygge, avdekke og motvirke sikkerhetstruende virksomhet. Disse medlemmer vil tydeliggjøre sikkerhetsloven som et felles rammeverk for alle virksomheter som opprettholder de viktigste funksjonene i Norge, og gå raskere frem i arbeidet med å implementere loven i alle samfunnssektorer.

Komiteens medlemmer fra Høyre viser til at nasjonal sikkerhet, herunder digital sikkerhet, har vært og er et prioritert område for Høyre, noe vår historikk fra Solberg-regjeringen og videre satsinger i opposisjon viser. Disse medlemmer viser for øvrig til Høyres alternative statsbudsjett for 2023, hvor Høyre foreslår å styrke Nasjonal sikkerhetsmyndighet med 5 mill. kroner og øke antall IKT-studieplasser med 500. Disse medlemmer viser også til Representantforslag om styrking av rikets sikkerhet og kontraetterretning, Dokument 8:51 S (2022–2023), hvor Høyre fremmer flere forslag om å styrke den nasjonale sikkerheten.

Komiteens medlem fra Sosialistisk Venstreparti gir regjeringen honnør for å understreke viktigheten av statlig eierskap av eiendom og infrastruktur som er viktig for nasjonal sikkerhet. Dette medlem er også positiv til initiativet til å samordne digitaliseringspolitikken under mer demokratiske prosesser. Til nå har digitaliseringen i for stor grad vært overlatt til noen få aktører. Digitaliseringen har stor påvirkning på samfunnsutviklingen, da flere av de digitale verktøyene som har kommet på plass de siste tiårene, er blitt kritisk infrastruktur i samfunnet. Dette medlem mener at digital suverenitet og det å regulere datainnsamling, databruk og datalagring er viktig for å ivareta nasjonal sikkerhet. Dette medlem mener det må kartlegges hvilken type data og mengde som må innlemmes under statlig kontroll for å sikre nasjonal sikkerhet. Statlig eierskap over datasentre som inneholder samfunnskritisk informa-

sjon, som helse- og forsvarsdata, må ligge til grunn i den digitale sikkerhetspolitikken.

Komiteens medlem fra Venstre anerkjenner at stortingsmeldingen omtaler internasjonalt samarbeid som viktig, men er skuffet over at internasjonalt samarbeid ikke trekkes fram som et av de fire prioriterte grepene for å ivareta nasjonal og digital sikkerhet på utvalgte områder. Dette medlem er av den bestemte oppfatning at forpliktende internasjonalt samarbeid i demokratiske allianser av land som deler våre verdier, er helt sentralt for å ivareta norsk sikkerhet. Det er ikke en motsetning mellom å skape sikkerhet for Norge og å samarbeide internasjonalt. De mange EU-reguleringene som listes opp i stortingsmeldingen, er et godt eksempel på dette.

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet vil påpeke at det fremkommer av meldingen at Norge skal jobbe for et tett, forpliktende og forutsigbart internasjonalt samarbeid om nasjonal sikkerhet. For å motarbeide sammensatte trusler er det etablert et tett og godt samarbeid med allierte land, NATO, FN og EU for å nevne noen arenaer. Dette gjelder også i arbeidet med å sikre et åpent, stabilt og fredelig digitalt rom.

I lys av informasjon som er kommet fram i saken som omhandler Pride-skytingen i 2022, er komiteens medlem fra Venstre bekymret for om samarbeidet og rutinene for informasjonsdeling mellom etterretnings- og sikkerhetstjenestene er god nok. I den forbindelse stiller dette medlem spørsmål ved om det forenkler eller vanskeliggjør arbeidet med å hindre sikkerhetstruende aktivitet at det finnes tre ulike sentre for å koordinere samarbeidet mellom etterretnings- og sikkerhetstjenestene og politiet. Dette medlem mener at regjeringen burde vurdere å slå disse sammen av hensyn til budsjett, mindre byråkrati og for å redusere faren for overlappende ansvarsområder mellom de ulike sentrene. Det kan nevnes at fremmede staters cyberaktivitet, som formodentlig behandles i Felles cyberkoordineringssenter (FCKS), også er en del av fremmede staters sammensatte virkemiddelbruk – som etter sigende er et område som tilhører Nasjonalt etterretnings- og sikkerhetssenter (NESS).

Om kapittel 3: Virkemidler for å styrke nasjonal kontroll og bygge digital motstandskraft

Komiteen viser til meldingen, der regjeringen i kapittel 3 redegjør for det virkemiddelapparatet staten besitter for å sikre nasjonal kontroll og digital motstandskraft. Komiteen merker seg at meldingen omtaler videre utvikling av tiltak som omfatter både:

- regulatoriske virkemidler
- nasjonalt eierskap
- samarbeid nasjonalt og internasjonalt
- kompetanse og bevisstgjøring
- råd og veiledning
- nasjonal deteksjonsevne og hendelseshåndtering

Komiteen viser til at flere saker de siste årene har synliggjort hvor viktig det er å ha både regulatoriske virkemidler og evne til å tenke langsiktig for å sikre nasjonal kontroll og nasjonal sikkerhet. Flere virksomheter har blitt utsatt for alvorlige dataangrep de siste årene, hvilket er en påminnelse på behovet for digital motstandskraft. Komiteen er derfor enig i behovet for utvikling og tilpasning av tiltak for å kunne imøtekomme aktuelle situasjoner som kan oppstå. Det å forebygge uønskede hendelser blir stadig viktigere, spesielt i lys av de endrede økonomiske rammene. Selv om enkelte tiltak vil kunne påføre både offentlige og private virksomheter direkte kostnader og utløse økte krav til rapportering, må omkostningene veies opp mot hensynet til å kunne ivareta nasjonal sikkerhet.

Komiteens medlem fra Sosialistisk Venstreparti viser til regjeringens forslag om «strategisk viktig infrastruktur», hvor en vil identifisere allierte og nære partnere en er «avhengig av for å sikre nasjonal kontroll, og etablere et tett, forpliktende og forutsigbart samarbeid med disse». Dette medlem mener videreutviklingen av digital infrastruktur, som via nærsatellittbasert internett, ikke kan overlates til private utenlandske selskaper som SpaceX. Slik infrastruktur bør utløse muligheten gitt i Meld. St. 6 (2022–2023) «Et grønnere og mer aktivt statlig eierskap» om at staten kan kjøpe seg opp i viktige selskaper.

Dette medlem ønsker å vise til Attac Norge sitt innspill om å inkludere «strategiske digitale ressurser» i nasjonal sikkerhetslov i likhet med begreper som «strategiske naturressurser». Strategiske digitale verdier omfatter i deres innspill datasentre, skytjenester og andre lagringsløsninger, data og algoritmer, samt mer tradisjonell programvare som brukes i transport, helse, utdanning, forskning og arbeidslivet generelt. Dette medlem mener en slik definisjon er fornuftig og avgjørende for å gjennomføre landets grunnleggende nasjonale funksjoner (GNF).

Sikkerhetsloven

Komiteen viser til at det nå er fire år siden sikkerhetsloven, hvis formål er å forebygge, avdekke og motvirke sikkerhetstruende virksomhet, trådte i kraft.

Komiteen vil understreke nødvendigheten av at sikkerhetsloven, som er det viktigste regulatoriske verktøyet for å ivareta nasjonal sikkerhet, er tilpasset det til enhver tid gjeldende trussel- og risikobildet. Komite-

en merker seg at regjeringen varsler at den vil fremme nødvendige forslag til endringer av loven for å gi myndighetene bedre oversikt over endringer i eierskap i norske virksomheter og klargjøre reglene for å stanse uønskede salg til fremmede aktører.

Komiteen vil understreke at god sikkerhetsstyring fordrer kompetanse om trusler, sårbarheter og effektive tiltak og er en forutsetning for å kunne beskytte verdier mot uønskede hendelser. Det er derfor nødvendig å bygge en god sikkerhetskultur i hele samfunnet.

Komiteen merker seg at departementet har bedt de øvrige fagdepartementene om å kartlegge egen sikkerhetskompetanse, og imøteser oppfølgingen av dette arbeidet.

Kompetanse

Komiteen viser til at digitale angrep kan få store konsekvenser både for den enkelte virksomhet og for samfunnet for øvrig. Komiteen vil understreke at digital motstandskraft fordrer at de ulike virksomhetene, offentlige og private, har tilstrekkelig IKT-kompetanse for å kunne ivareta den digitale sikkerheten. Behovet for IKT-sikkerhetskompetanse har økt i takt med den digitale utviklingen. Komiteen er kjent med at behovsundersøkelser viser et stort udekket behov for IKT-sikkerhetskompetanse i alle sektorer. IKT-kompetanse er en kritisk faktor, både når det gjelder det forebyggende arbeidet i bedrifter, kommuner og for å beskytte virksomhetene fra digitale angrep, og ikke minst når det gjelder å forhindre at kritiske samfunnsfunksjoner kan settes ut av spill. Komiteen har merket seg innspillene fra enkelte høringsinstanser som påpeker at det er behov for å øke tilgangen på IKT-kompetanse, men også sørge for å sikre at selve innholdet i utdanningene er relevant for de oppgavene som kandidatene møter i arbeidslivet. Komiteen merker seg også innspill om behovet for å styrke det offentliges innkjøpskompetanse med hensyn til datasystemer.

Komiteen viser til at i Meld. St. 9 (2022–2023) ønsker regjeringen å styrke motstandskraften og robustheten gjennom økt kompetanse og kunnskap på det digitale. Det er positivt. Komiteen deler likevel bekymringen Tekna viser til i sitt høringsinnspill om mangel på kompetanse i kommunesektoren i dag, da det er mye flukt til privat næringsliv. Komiteen mener IKT er en kjerneaktivitet i det offentlige, og at myndighetene må ta initiativ som sikrer at god og stabil kompetanse er på plass for å levere den digitale infrastrukturen og sikkerheten som er nødvendig.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet, Fremskrittspartiet og Venstre, viser til at etterspørselen etter teknologisk kompetanse generelt, og IT-kompetanse spesielt, i arbeidslivet øker. Det stilles større krav til helhetlig og tverrfaglig kompetanse om digitalisering, blant annet for å ivareta den digitale sikkerheten. Flertallet viser til at til tross for at det har vært en sterk vekst i utdanningskapasiteten innen IT-utdanninger over flere år, er det fortsatt et stort behov for å øke rekrutteringen til realfag og kapasiteten i utdanningssystemet innen STEM-utdanninger.

For å imøtekomme etterspørselen etter IT-utviklere mener flertallet at vi i Norge i dag er avhengig av å rekruttere folk fra utlandet. Flertallet er kjent med at utenlandske statsborgere er i flertall blant doktorgradskandidatene innen teknologifag, og mange av disse kan ikke sikkerhetsklareres i Norge, hvilket begrenser muligheten for å benytte deres kompetanse i sentrale funksjoner. Flertallet vil understreke at den sikkerhetspolitiske situasjonen tilsier at Norge bør bli mer selvforsynt med nødvendig IT-sikkerhetskompetanse.

Flertallet merker seg med interesse at flere høringsinstanser har poengtert behovet for IT-kompetanse, både høyt spesialisert kompetanse på master og doktorgradsnivå og IT-kompetanse hos medarbeidere med annen høyere utdanning. Flertallet viser til at antall IT-studenter i fagskolene er tidoblet de siste ti årene, fra 300 til over 3 000 studenter. Flertallet merker seg innspillene i høringen om at etterspørselen etter kompetanse også bør kunne løses gjennom høyere yrkesfaglig utdanning. Flertallet mener det må være en prioritet å sikre arbeidslivet tilstrekkelig tilgang på IT-kompetanse, og at det er behov for kapasitetsvekst i høyere utdanning både innenfor grunn- og videreutdanninger, samt tilbudet innen etter- og videreutdanning. I denne sammenheng vil flertallet påpeke at en videre utvikling av utdanningstilbud og økt kapasitet i fagskolene vil være en viktig vei for å løse det akutte behovet for økt IT-kompetanse i arbeidslivet. Flertallet vil påpeke at et av fagskolenes fortrinn er at de raskt kan utvikle tilbud som svarer på arbeidslivets spesifikke behov.

Et annet flertall, medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet og Fremskrittspartiet, viser for øvrig til at regjeringen har varslet at Kunnskapsdepartementet våren 2023 vil legge fram en egen stortingsmelding om regjeringens politikk for å dekke fremtidens kompetansebehov. Formålet med meldingen er å sikre at dimensjoneringen av utdanningstilbudet framover bedre samsvarer med kompetansebehovene og utviklingen innen ulike disipliner.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet, Fremskrittspartiet og Venstre, viser til viktigheten av at Norsk senter for informasjonssikring (NorSIS) har en rolle i vår nasjonale cybersikkerhetskapasitet. NorSIS er en uavhengig organisasjon og medlemsforening som

arbeider med informasjonssikkerhet. Deres mest kjente råd- og veiledningstjeneste er slettmeg.no. Senteret er lokalisert på Gjøvik i tilknytning til NTNUs fakulteter. Flertallet mener det er viktig for vår nasjonale cybersikkerhetskapasitet at denne lille ekspertorganisasjonen på Gjøvik med et svært viktig samfunnsoppdrag finnes.

Flertallet viser videre til at NorSIS er en aktør som har befolkningens cybersikkerhet som enkeltindivider som fokusområde og samfunnsoppdrag. Flertallet mener det er viktig at vi har en cybersikkerhetsaktør som også ivaretar individperspektivet, og viser i forlengelsen av dette til at en aktør med befolkningen som sin primære kontaktflate er i en unik posisjon til å fange opp operasjoner rettet mot befolkningen, som eksempelvis forsøk på påvirkningsoperasjoner rettet mot befolkningen i cyberdomenet. Flertallet mener følgelig at NorSIS spiller en viktig rolle for den digitale motstandskraften i befolkningen.

Komiteens medlemmer fra Fremskrittspartiet vil fremheve at den viktigste forutsetningen for fortsatt drift og videreutvikling av ekspertmiljøet ved NorSIS er at senteret sikres en forutsigbar finansiering og tilstrekkelige midler til å bygge videre på dagens ekspertise. Disse medlemmer vil herunder påpeke at Fremskrittspartiet i sitt alternative statsbudsjett for 2023 foreslo å bevilge 2 mill. kroner mer enn regjeringen til styrking av NorSIS sitt arbeid med cybersikkerhet.

Disse medlemmer mener det er viktig at NorSIS sikres en langsiktig forutsigbarhet for driften ved senteret, slik at det er mulig å bygge organisasjonen og fagmiljøet i et lengre tidsperspektiv enn ett år av gangen.

Disse medlemmer fremmer på denne bakgrunn følgende forslag:

«Stortinget ber regjeringen utarbeide en forpliktende langtidsplan for driften ved Norsk senter for informasjonssikring.»

Samordning og koordinering mellom departementene

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, ønsker å vise til Riksrevisjonens rapport «Myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor» hvor det understrekes at det er svakheter i det digitale sikkerhetsarbeidet i flere sektorer. Flertallet anerkjenner at denne rapporten kom etter Meld. St. 9 (2022–2023), og forventer at Riksrevisjonens kritikk og anbefalinger følges opp på egnet måte.

Et annet flertall medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet, Fremskrittspartiet og Venstre, viser til at arbeidet med digital sikkerhet og nasjonal kontroll berører hele samfunnet, og derfor krever samordning av aktører og virkemidler på tvers av sektorene. Dette flertallet vil understreke at grunnlaget for å kunne møte komplekse utfordringer på tvers av sektorer er en felles og samstemt trussel- og risikoforståelse. Tverrsektoriell koordinering både mellom departementer, mellom departementer og underliggende etater, mellom det private og det offentlige, samt mellom det sivile og militære vil derfor være en nøkkelfaktor for å heve den samlede sikkerheten.

Et tredje flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Venstre, mener en bevisstgjøring om trusselbildet og avdekking av sårbarhet krever koordinering mellom myndigheter på ulike forvaltningsnivå, og mellom myndighetene og virksomheter i privat næringsliv. Dette flertallet viser til at Justis- og beredskapsdepartementet har hatt ansvaret for samordningen av samfunnssikkerhetsarbeidet og digital sikkerhet i sivil sektor siden 2013. Dette flertallet merker seg at Riksrevisjonen har foretatt undersøkelse av myndighetenes samordning av arbeidet med digital sikkerhet i sivil sektor. Rapporten som ble offentliggjort i februar 2023, jf. Dokument 3:7 (2022–2023), konkluderer med at ansvaret for digital sikkerhet i sivil sektor ikke har vært godt nok ivaretatt.

Når det gjelder oversikt over verdier som er strategisk viktige, merker dette flertallet seg innspill fra høringsinstanser som opplever til dels svært stor forskjell mellom departementene når det gjelder status og fremdrift i dette arbeidet.

Dette flertallet viser til meldingen, der regjeringen signaliserer at den vil vurdere ytterligere tiltak for å forsterke samordningen på myndighetsnivå og gjøre det enklere for sluttbrukeren.

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet viser til meldingen og regjeringens arbeid for at NSM og Norges forskningsråd skal etablere Norges nasjonale koordineringssenter for digital sikkerhet, og merker seg at senteret skal samarbeide med øvrige miljøer i Norge innenfor digital sikkerhet for nettopp å styrke koordineringsarbeidet.

Skyplattformer og datasenter

Komiteens flertall, medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet, Fremskrittspartiet og Venstre, viser til at datasenter er en sentral del av den digitale infrastrukturen som leverandør av viktige tjenester til både privatpersoner og offentlige og private virksomheter. Samfunnets avhengig-

het av digitale tjenester blir stadig større, og stadig flere kritiske tjenester bæres av den digitale infrastrukturen. Det fordrer et bevisst forhold til sikkerhet og robuste lagringsløsninger. Omfanget av til dels sensitiv og skjermingsverdig informasjon tilsier behov for særlig robuste lagringsløsninger som ivaretar og beskytter norske interesser. Flertallet er kjent med at det per i dag verken finnes offentlige eller kommersielle datasentre eller skyplattformer tilrettelagt for virksomheter underlagt sikkerhetsloven.

Flertallet deler oppfatningen om behovet for innenlands datalagringskapasitet og at myndighetene gjennom regulering bør legge til rette for at flere norskeide datasentre kan levere skytjenester i Norge for å redusere sårbarheten som er knyttet til avhengighet av internasjonale skytjenester. Datasentrene legger også til rette for innovasjon og effektivisering både i næringslivet og i det offentlige.

Et annet flertall, medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet og Fremskrittspartiet, viser til at regjeringen allerede har tatt tak i dette, og at regjeringen i 2022 sendte på høring forslag til datasenterregulering, blant annet innføring av krav om registreringsplikt for datasenteraktører, som vil gi myndighetene en bedre oversikt over næringen i Norge. I tillegg foreslo regjeringen å sette spesifikke krav om forsvarlig sikkerhet i datasentre.

Dette flertallet viser til at Nasjonal sikkerhetsmyndighet (NSM) på oppdrag fra Justis- og beredskapsdepartementet har gjennomført en konseptvalgutredning for å vurdere behovet for og etablering av en nasjonal skytjeneste for statsforvaltningen. Utredningen ble overlevert departementet 26. januar 2023 og er nå over i en ny fase – ekstern kvalitetssikring.

Komiteens medlem fra Sosialistisk Venstreparti viser til regjeringen sin utredning av innføring av en nasjonal skytjeneste. Dette medlem mener en nasjonal skytjeneste vil være et essensielt verktøy for å ivareta nasjonal sikkerhet gjennom lagring av samfunnskritiske, offentlige data. Dette medlem mener også at en nasjonal skytjeneste må inneholde plattform- og programvareløsninger for bruk av det offentlige, for å frigjøre infrastruktur som daglig brukes av det offentlige, fra private, internasjonale selskapers kontroll.

Sikkerhetsklarering

Komiteens flertall, medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet, Fremskrittspartiet og Venstre, vil understreke at i lys av den sikkerhetspolitiske situasjonen vi opplever nå, er det helt avgjørende å ha kontroll på gradert informasjon, og hvem som har tilgang til denne, for å ivareta nasjonens sikkerhet. Flertallet er kjent med at flere virksomheter erfarer utfordringer med å få tilgang på personell med riktig sikkerhetsklarering. Flertallet registrerer at det er påpekt behov for å harmonisere sikkerhetslovgivningen og styrke samarbeidet om sikkerhetsklarering mellom de nordiske landene, slik at virksomheter lettere kan benytte knappe personellressurser på tvers av grensene mellom de nordiske nabolandene. Flertallet viser til at regjeringen i meldingen skriver at det vil være særlig relevant å søke fellesnordiske løsninger der det er mulig, gitt våre liknende styresett, verdisyn og trussel- og risikobilde.

Et annet flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Venstre, viser til at etter kritikk fra EOS-utvalget varslet justis- og beredskapsministeren i 2021 at regjeringen ville foreta en gjennomgang av praksisen i klareringssaker, med sikte på å gjøre eventuelle justeringer for å sikre at sikkerhetsklarering av personell skjer basert på individuelle og ikke skjematiske vurderinger, slik loven krever. Dette flertallet viser til at tilsynet har avdekket at det er uklarheter om hvordan regelverket skal fortolkes og praktiseres i enkelte typer saker. Dette flertallet mener det er viktig å påse at feil lovanvendelse ikke bidrar til mangel på kompetente arbeidstakere.

Lov om digital sikkerhet

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet viser til at regjeringen arbeider med et forslag til lov om digital sikkerhet. Lovens formål vil være å forplikte virksomheter som har en særlig viktig rolle for å opprettholde kritisk samfunnsmessig og økonomisk aktivitet, og sikre gjennomføring av nasjonale råd og anbefalinger. Disse medlemmer merker seg at lovforslaget skal gjelde for tilbydere av samfunnsviktige tjenester innenfor samfunnsområdene energi, transport, helse, vannforsyning, banktjenester, finansmarkedsinfrastruktur og digital infrastruktur. Disse medlemmer imøteser lovforslaget og behandlingen av dette.

Komiteens medlemmer fra Fremskrittspartiet mener saken om justis- og beredskapsministerens bruk av en kinesisk applikasjon på sin tjenestetelefon, og hennes mangelfulle besvarelser av Stortingets spørsmål i den anledning, har avdekket det disse medlemmer oppfatter som flere kritiske hull i regelverket for den norske regjeringens IKT-sikkerhet. Disse medlemmer viser til at det i medieomtalen av den nevnte saken har blitt referert til kinesisk sikkerhetslovgivning, som alle kinesiske selskaper er bundet av. Etter sikkerhetslovgivningen er kinesiske selskaper forpliktet til på forespørsel å utlevere informasjon til kinesiske myndigheter, herunder brukerinformasjon

som er innhentet gjennom applikasjoner. Den brukerinformasjonen en norsk bruker deler med en kinesisk teknologiprodusent, er følgelig bare en forespørsel unna å bli delt med kinesiske myndigheter.

Disse medlemmer mener dette konkrete eksempelet på hvordan kinesiske applikasjoner kan operere som den kinesiske etterretningstjenestens forlengede arm, illustrerer viktigheten av at teknologi fra land vi ikke har sikkerhetspolitisk samarbeid med, ikke gis tilgang til å innhente informasjon fra norske regjeringsmedlemmers kommunikasjonsenheter. Disse medlemmer mener det burde være åpenbart at land som figurerer som et risikoelement for Norge i Politiets sikkerhetstjenestes risikovurdering, ikke skal gis innpass på norske regjeringsmedlemmers kommunikasjonsenheter. Det pekes i forlengelsen av dette på at et datainnbrudd på Stortinget i 2021 ble identifisert til å ha blitt gjennomført fra kinesisk territorium, og norske myndigheter gikk langt i å ansvarliggjøre den kinesiske stat for dette.

Disse medlemmer er videre av den oppfatning at det etter en naturlig språklig forståelse av ordlyden i Nasjonal sikkerhetsmyndighets 13 råd om sikkerhet på mobile enheter, er åpenbart at en kinesiskprodusert applikasjon ikke skal installeres på en statsråds tjenestetelefon. Det samme har eksperter på IKT-sikkerhet uttalt i mediene. Justis- og beredskapsministeren fastholder imidlertid at installasjon av en kinesisk applikasjon på tjenestetelefonen er i henhold til Nasjonal sikkerhetsmyndighets retningslinjer, og at hun ikke har gitt feilaktige opplysninger når hun har hevdet at hennes mobilbruk er i henhold til gjeldende råd og retningslinjer. Dette er statsråden med det konstitusjonelle ansvaret for IKT-sikkerhet, så hun uttaler seg med autoritet når hun adresserer hvordan disse rådene skal forstås. Statsministeren har i besvarelsen av Stortingets skriftlige spørsmål nr. 1231 sluttet seg til justis- og beredskapsministerens forståelse av rådene om sikkerhet på mobile enheter. Slik disse medlemmer ser det, har denne fortolkningen i praksis gjort Nasjonal sikkerhetsmyndighets 13 råd om sikkerhet på mobile enheter innholds- og verdiløse.

Disse medlemmer viser til at blant annet USA, Canada, Danmark og EU har vedtatt forbud mot å laste ned TikTok på tjenestetelefonene til enten alle føderalt ansatte eller alle folkevalgte og politisk ansatte. Slik disse medlemmer ser det, er det at flere av våre allierte vedtar slike forbud, en klar indikasjon på hvilken potensiell sikkerhetstrussel applikasjoner fra land vi ikke har sikkerhetspolitisk samarbeid med, representerer. Disse medlemmer viser videre til at justis- og beredskapsministeren i sin besvarelse av Stortingets skriftlige spørsmål nr. 1206 opplyser om at hun ikke vil gi føringer som forbyr TikTok eller andre apper. Som tidligere nevnt er disse medlemmer ikke i tvil om at installasjon av TikTok på en statsråds mobiltelefon ikke er i henhold til Nasjonal sikkerhetsmyndighets gjeldende råd om sikkerhet på mobile enheter.

Slik disse medlemmer ser de,t har regjeringen og ansvarlig statsråds oppfatning om hvordan Nasjonal sikkerhetsmyndighets råd for mobilbruk skal tolkes og anvendes, resultert i en situasjon hvor det er påkrevd med umiddelbare grep for å tydeliggjøre at teknologi fra land vi ikke har sikkerhetspolitisk samarbeid med, ikke skal gis mulighet til å infiltrere regjeringsmedlemmenes mobile kommunikasjonsenheter. Disse medlemmer fremmer på denne bakgrunn forslag om innføring av forbud mot bruk av applikasjoner fra land vi ikke har sikkerhetspolitisk samarbeid med, på regjeringen og departementenes kommunikasjonsenheter. Disse medlemmer fremmer videre forslag om at regjeringen må få utarbeidet nye råd for mobilbruk, som erstatter Nasjonal sikkerhetsmyndighets 13 råd om sikkerhet på mobile enheter.

«Stortinget ber regjeringen sikre at regjeringen, regjeringsapparatet og departementene ikke har adgang til å bruke applikasjoner på offisielle kommunikasjonsenheter som har eierskap i eller driftes fra land vi ikke har et sikkerhetspolitisk samarbeid med.»

«Stortinget ber regjeringen sørge for at Nasjonal sikkerhetsmyndighet utarbeider nye råd for mobilbruk, som erstatter Nasjonal sikkerhetsmyndighets 13 råd om sikkerhet på mobile enheter.»

Komiteens medlemmer fra Høyre og Venstre støtter intensjonen i forslagene fra Fremskrittspartiet. I lys av både tjenestenes vurdering om at Kina utgjør en stadig større trussel mot Norge, og kunnskap om hvilken sikkerhetsrisiko den kinesiske appen TikTok utgjør, mener disse medlemmer det er påfallende at regjeringen ikke vil vurdere å gi offisielle føringer som forbyr bruk at TikTok og andre lignende apper på tjenestetelefoner i regjeringsapparatet, jf. Dokument nr. 15:1206 (2022–2023). Disse medlemmer viser blant annet til at både Regeringskansliet i Sverige og EU-kommisjonen har sendt ut beskjed til alle ansatte om at appen TikTok bør slettes fra tjenestetelefoner. I tillegg har den amerikanske regjeringen uttalt at den støtter et lovforslag som åpner for å forby appen TikTok. Disse medlemmer peker også på at det under Solberg-regjeringen ble gitt føringer fra politisk ledelse ved Statsministerens kontor om at ingen i regjeringen skulle laste ned TikTok. Disse medlemmer mener det er et lederansvar å sørge for en god digital sikkerhetskultur. Det er derfor naturlig at regjeringen vurderer å gi føringer om å forby appen TikTok i regjeringsapparatet.

Disse medlemmer mener det kan være grunn til å be Nasjonal sikkerhetsmyndighet revidere rådene

for mobilbruk, herunder vurdere å være tydeligere på hvilke råd som gjelder for apper med kjente sikkerhetsrisikoer. Samtidig understreker disse medlemmer at sikkerhetsråd fra NSM ikke fratar den enkelte ansvar for å vurdere sikkerheten ved applikasjoner man velger å laste ned på digitale enheter. En oppdatert liste over apper som utgjør en sikkerhetsrisiko, kan gi en falsk trygghet, ettersom det stadig lages nye apper og det ikke er noen garantier mot at i utgangspunktet «sikre» apper kan være hacket eller inneholde skadelig programvare.

Kvantedatateknologi

Komiteens flertall, medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet, Fremskrittspartiet og Venstre, viser at bruk av nye fremvoksende og banebrytende teknologier er økende og utfordrer balansen mellom angrepskapasiteter og forsvarskapasiteter. Kvantedatamaskiner vil kunne knekke noen av de mest vanlige krypteringsmekanismene og slik utfordre den digitale motstandskraften. Muligheten til å manipulere og kontrollere kvanteeffekter på et stadig mer nøyaktig nivå ved å bruke kvanteteknologi gir nye muligheter og dertil nye utfordringer. Utviklingen av kvantedatamaskiner er forventet å revolusjonere den digitale verden og vil kunne påvirke globale kommunikasjonsnettverk og sikkerheten på internett.

Et annet flertall, medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet og Fremskrittspartiet, viser til at regjeringen har tatt initiativ til å få en oversikt over norske fagmiljøer som driver med forskning og høyere utdanning i kvanteteknologi, og at Kunnskapsdepartementet og Justis- og beredskapsdepartementet på denne bakgrunn har sendt en forespørsel til Forskningsrådet om å framskaffe dette.

Om kapittel 4: Nasjonal kontroll over verdier av betydning for nasjonal sikkerhet

Komiteen viser til at oppkjøp av eiendom med strategisk beliggenhet og viktige bedrifter kan brukes i et langsiktig påvirkningsarbeid mot Norge. Komiteen har merket seg at E-tjenesten, PST og NSM har påpekt i sine trussel- og risikovurderinger at dette kan utgjøre en trussel. Skjerming av verdier som kan ha betydning for nasjonal sikkerhet, og forhindre at uønskede aktører får kontroll, innsikt eller innflytelse over verdier som kan skade vår stabilitet eller suverenitet, er derfor helt nødvendig.

Komiteen merker seg videre at regjeringen har påbegynt et arbeid for å fange opp sikkerhetstruende virksomhet knyttet til eierskap, og bruk av, eiendom. Komiteen merker seg at regjeringen vurderer å innføre søknadsplikt for å kjøpe visse strategiske eiendommer, tinglysningsplikt for å forhindre at skjult eierskap kan brukes for å få uønsket innflytelse i Norge, samt tydeliggjøring at virksomhetseiers plikt til å foreta en risikovurdering for å identifisere konkrete eiendommer som kan legge til rette for sikkerhetstruende virksomhet mot skjermingsverdige objekter og skjermingsverdig infrastruktur.

Komiteen mener det også er viktig å sikre oversikt over uønsket økonomisk aktivitet for bedrifter som ikke er underlagt sikkerhetsloven, og har merket seg at regjeringen har satt ned et offentlig utvalg for å utrede behovet for et regelverk eller en ordning, for å kunne screene økonomisk aktivitet rettet mot slike virksomheter.

Norske virksomheters kjøp av skytjenester fra store kommersielle, multinasjonale selskaper gir noen positive sikkerhetsgevinster ved at utdaterte IT-løsninger erstattes av løsninger med bedre sikkerhet, samtidig som det skaper avhengighet til utenlandske leverandører som fører til digital sårbarhet. Komiteen merker seg at regjeringen er i gang med å utrede en nasjonal skytjeneste for å øke nasjonal kontroll over kritisk datainfrastruktur og viktig informasjon, samt stille nye krav til datasentre og innføre registreringsplikt for datasenteraktører i Norge, for å forhindre at uønsket og ulovlig aktivitet kan foregå i det skjulte. Komiteen imøteser dette arbeidet.

Nasjonal kontroll over verdier

Komiteens flertall, medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet, Fremskrittspartiet og Venstre, mener den sikkerhetspolitiske situasjonen krever større nasjonal kontroll med verdier som kan benyttes av fremmede makter til å handle i strid med Norges interesser. I trusselvurderingen for 2023 peker Etterretningstjenesten på at utenlandske makter, særlig Kina, bruker utenlandsinvesteringer som et virkemiddel for å understøtte egne strategiske mål. Summen av investeringer og oppkjøp kan medføre at stater Norge ikke har sikkerhetspolitisk samarbeid med, får innflytelse og kontroll over verdier som er i strid med norske sikkerhetsinteresser.

Et annet flertall, medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet og Fremskrittspartiet, viser til at omsetningen av norske eiendommer og bedrifter kan påvirke nasjonale sikkerhetsinteresser. Gjennom tilgang på og kontroll over teknologi, informasjon og naturressurser kan salg av eiendom og virksomheter i Norge gi utenlandske aktører strategisk tilgang til ressurser som på sikt kan svekke norske interesser.

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet viser i den forbindelse til at oppkjøp og investering i norske virksomheter og eiendom i regi av fremmede aktører er et av tre forhold som NSM framhever i sin risikorapport for 2023.

Som redegjort for i meldingen, viser disse medlemmer til at flere saker de senere årene har aktualisert behovet for at myndighetene tar aktivt grep for å ivareta nasjonal kontroll gjennom å forhindre utenlandsk eierskap i Norge som kan utgjøre en trussel mot Norges sikkerhet og beredskap. Ikke minst viste Solberg-regjeringens forsøk i 2014 på nedsalg i Kongsberg Gruppen en svak forståelse av behovet for nasjonal kontroll over utvikling og produksjon av forsvarsteknologi. Saken vakte stor politisk debatt, og salget ble ikke gjennomført. Tilsvarende viser disse medlemmer til at Solberg-regjeringen utviste svak håndtering i Bergen Engines-saken, der russiske interesser var en av de potensielle interessentene. Igjen var det takket være stor oppmerksomhet i media og politisk årvåkenhet fra partier på Stortinget at det ble foretatt en vurdering av salget opp mot sikkerhetsloven, og transaksjonen ble til slutt stoppet. Disse medlemmer mener disse sakene synliggjør hvor viktig det er at staten har virkemidler både til å avdekke og for å kunne gripe inn der det er nødvendig.

Disse medlemmer viser til at regjeringen høsten 2022 sikret fortsatt norsk eierskap over Meraker Brug og dermed forhindret at 1,2 millioner mål norsk jord, inkludert vannkraftverk, havnet på utenlandske hender. Det er videre en kjensgjerning at Kina over flere år har vært aktiv i å kjøpe opp utenlandske naturressurser. I Norge har kinesiske selskaper vist interesse for jord- og skogbrukseiendommer. Disse medlemmer merker seg at både Høyre og Fremskrittspartiet har uttalt seg negativt til regjeringens oppkjøp av Meraker Brug.

Disse medlemmer mener tvert imot at det å sikre norsk eiendomsrett over store norske landområder er en klok investering for å ivareta nasjonal kontroll, og viser til at regjeringen varsler en lovendring som vil kunne forhindre salg av slike store eiendommer til utenlandske eiere. Disse medlemmer vil understreke at statlig eierskap ikke er et mål i seg selv, men et virkemiddel i det forebyggende arbeidet med å ivareta nasjonal kontroll over nasjonale interesser.

Disse medlemmer viser for øvrig til at regjeringen også har opprettet en screeningmekanisme, hvis formål er å sikre enhetlig behandling av sikkerhetstruende økonomisk aktivitet innenfor ulike sektorer – som for eksempel Bergen Engines-saken.

Komiteens medlemmer fra Høyre og Venstre viser til at Solberg-regjeringen satte i gang et arbeid med å revidere sikkerhetsloven for å sikre økt kontroll med oppkjøp som kan påvirke nasjonal sikkerhet. Disse medlemmer mener arbeidet må ses i sammenheng og harmoniseres med EU-regler om screening av utenlandske direkteinvesteringer.

Disse medlemmer registrerer at Arbeiderpartiet og Senterpartiet kritiserer håndteringen av Bergen Engines-saken. Disse medlemmer viser til at Solberg-regjeringen den 18. mars 2021 konkluderte med at den hadde tilstrekkelig informasjon til å beslutte at salget av Bergen Engines til Transmashholding Group (TMH) måtte stanses for å unngå at nasjonale sikkerhetsinteresser blir truet. Disse medlemmer viser til at Solberg-regjeringen gjennom kongelig resolusjon av 26. mars 2021 påla RollsRoyce å stanse salget av det norske selskapet Bergen Engines AS til selskaper i TMH. Disse medlemmer viser videre til at Solberg-regjeringen samme dag påla stans i enhver overføring av aksjer, eiendeler, eiendom, industriell eller teknologisk informasjon eller andre rettigheter i Bergen Engines eller selskapets datterselskaper til TMH, med hjemmel i lov 1. juni 2018 nr. 24 om nasjonal sikkerhet § 2-5 første ledd. Disse medlemmer viser til at Rolls-Royce, Bergen Engines og TMH den 8. mars 2021 ble varslet om at norske myndigheter vurderte å stanse salget av Bergen Engines med hjemmel i sikkerhetsloven. Disse medlemmer viser til at NSM samtidig bad partene om å stoppe den påbegynte «due diligence»-prosessen, og fikk bekreftelse 12. mars 2021 om at prosessen var stanset. For øvrig viser disse medlemmer til Høyre, Venstre og Kristelig Folkepartis merknader i Innst. 503 S (2020–2021).

Når det gjelder Meraker Brug, viser komiteens medlemmer fra Høyre til Høyres merknader i Innst. 47 S (2022–2023). Disse medlemmer legger til at selv om det er gode grunner for å skjerpe kontrollen med utenlandske oppkjøp, betyr ikke det at staten skal forebygge slike oppkjøp ved ukritisk å kjøpe opp eiendommer til langt over markedspris.

Videre mener disse medlemmer det er påfallende at Arbeiderpartiet og Senterpartiet kritiserer Høyre og Solberg-regjeringens sikkerhetsarbeid. Solberg-regjeringen fikk på plass en ny og oppdatert sikkerhetslov, det digitale sikkerhetsarbeidet ble kraftig styrket, og det ble satt i gang et arbeid med å revidere sikkerhetsloven i 2021.

Disse medlemmer viser til at Solberg-regjeringen blant annet la frem forslag om endringer i sikkerhetslovens regler om eierskapskontroll i oktober 2021, hvor høringsfristen gikk ut 10. januar 2022. I svar på spørsmål 110 fra finanskomiteen/Høyres fraksjon av 18. mai 2022 svarte Justis- og beredskapsdepartementet at

«[r]evisjonen av sikkerhetsloven gjennomføres i to trinn. Det første trinnet omfatter forslag til endringer av sikkerhetsloven §10 om eierskapskontroll. Forslaget

har vært på høring. Det tas sikte på å oversende denne lovproposisjon til Stortinget over sommeren.

Trinn to omfatter forslag til øvrige endringer i sikkerhetsloven. Det tas sikte på å sende forslaget på alminnelig høring i løpet av sommeren. Det tas videre sikte på å oversende Stortinget en lovproposisjon med forslag til disse endringene før årsskiftet 2022/2023».

Disse medlemmer konstaterer at Arbeiderparti–Senterparti-regjeringen verken har lagt frem lovproposisjon om endringer av eierskapskontrollreglene eller sendt øvrige forslag til endringer i sikkerhetsloven på høring per 9. mars 2023. Disse medlemmer peker for øvrig på at Arbeiderparti–Senterparti-regjeringen heller ikke har klart å legge frem forslag om kriminalisering av samarbeid med fremmed etterretningstjeneste om å utøve påvirkningsvirksomhet, selv om høringsfristen gikk ut 15. august 2021. Disse medlemmer mener Arbeiderpartiet og Senterpartiets retorikk står i skarp kontrast til evnen til å faktisk gjøre grep for å styrke den nasjonale sikkerheten gjennom nødvendige lovendringer.

Nordområdene og Svalbard

Komiteens flertall, medlemmene fra Arbeiderpartiet, Høyre, Senterpartiet, Fremskrittspartiet og Venstre, viser til nordområdenes økte strategiske betydning i dagens sikkerhetspolitiske situasjon. Den strategiske plasseringen, samt nærheten til skjermingsverdige objekter og naturressurser, er av stor betydning for forsyningssikkerhet for energi, vann og mat. Flertallet merker seg for regjeringen i meldingen understreker behovet for å sikre bedre kontroll i nordområdene og innvarsler en ny giv i nordområdepolitikken. Flertallet er enig i at det å sikre norsk eierskap til viktig infrastruktur og eiendom og nasjonal kontroll over naturressurser i nordområdene er helt sentralt i arbeidet for å ivareta nasjonal kontroll og sikkerhet. I denne forbindelse er levende og livskraftige sivile samfunn i Nord-Norge av helt sentral betydning for å opprettholde norsk sikkerhet. Flertallet vil i den forbindelse understreke betydningen av å sikre norsk bosetning i nærområdene mot Russlands grense for å kunne understøtte norsk suverenitet og norske interesser i regionen.

Et annet flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Fremskrittspartiet, viser til at Svalbard har stor strategisk betydning for Norges muligheter i nordområdene og Arktis. Dette flertallet merker seg at det har vært en stor økning i utenlandsk tilflytting til Svalbard de siste årene. Det er viktig at lokale myndighetspersoner har god kjennskap til svalbardpolitikken og tilknytning til Norge. Dette flertallet mener derfor det er et riktig tiltak at regjeringen har innført krav om tre års botid på fastlandet for utenlandske statsborgere som vil stemme ved lokalvalg på Svalbard fra lokalvalget i 2023. Dette flertallet viser for øvrig til at regjeringen gjennom Prop. 78 S (2021–2022) har styrket etterretnings- og sikkerhetstjenestene og politiets evne til å forebygge sikkerhetstruende virksomhet, særlig i de tre nordligste fylkene.

3. Forslag fra mindretall

Forslag fra Fremskrittspartiet:

Forslag 1

Stortinget ber regjeringen utarbeide en forpliktende langtidsplan for driften ved Norsk senter for informasjonssikring.

Forslag 2

Stortinget ber regjeringen sikre at regjeringen, regjeringsapparatet og departementene ikke har adgang til å bruke applikasjoner på offisielle kommunikasjonsenheter som har eierskap i eller driftes fra land vi ikke har et sikkerhetspolitisk samarbeid med.

Forslag 3

Stortinget ber regjeringen sørge for at Nasjonal sikkerhetsmyndighet utarbeider nye råd for mobilbruk, som erstatter Nasjonal sikkerhetsmyndighets 13 råd om sikkerhet på mobile enheter.

4. Komiteens tilråding

Komiteens tilråding fremmes av en samlet komité.

Komiteen har for øvrig ingen merknader, viser til meldingen og rår Stortinget til å gjøre følgende

vedtak:

Meld. St. 9 (2022–2023) – Nasjonal kontroll og digital motstandskraft for å ivareta nasjonal sikkerhet – vedlegges protokollen.

Oslo, i justiskomiteen, den 21. mars 2023

Per-Willy Amundsen
leder

Ivar B. Prestbakmo
ordfører

Svanemerketrykksak, 2041 0654 Trykk og layout: Stortingets administrasjon