STORTINGET

Innst. 187 S

(2017–2018)

Innstilling til Stortinget
fra justiskomiteen

Meld. St. 38 (2016–2017)

Innstilling fra justiskomiteen om IKT-sikkerhet. Et felles ansvar

Til Stortinget

1. Sammendrag

1.1 Innledning

Dette er den første stortingsmeldingen om IKT-sikkerhet. Meldingen redegjør for regjeringens politikk for arbeidet med IKT-sikkerhet.

Meldingen er delt i fire hoveddeler: 1) Innledning, 2) Sentrale områder i arbeidet med IKT-sikkerhet, 3) Oppfølging av Lysneutvalgets anbefalinger og 4) Økonomiske og administrative konsekvenser.

Det er flere grunner til at IKT-sikkerhet vies mye oppmerksomhet. Den digitale utviklingen er en avgjørende del av vår verdiskapning og vekst. Digitaliseringen har bidratt til et tryggere og mer sikkert samfunn. Folk kan lettere komme i kontakt med hverandre og få rask tilgang til informasjon. Digitaliseringen har også medført at samfunnets risikobilde har endret seg. Ingen sektorer, og få nasjoner, kan i dag kontrollere sin digitale sårbarhet alene. Digitalt sårbarhetsutvalg (Lysneutvalget) (NOU 2015:13 Digital sårbarhet – sikkert samfunn) viser til at Norge ligger langt fremme når det gjelder digitalisering, noe som gjør at vi som samfunn tidlig møter sårbarhetsutfordringene.

Trusselvurderinger viser at fremmede stater er villige til å bruke ulike virkemidler for å få tilgang til sensitiv og skjermingsverdig informasjon og påvirke politiske, økonomiske og forvaltningsmessige beslutninger. Det er store økonomiske tap knyttet til IKT-kriminalitet. I tillegg skjer det en rekke ganger at IKT-systemer svikter på grunn av menneskelige feil, programvarefeil, utstyrsfeil, naturhendelser eller en kombinasjon av disse.

For å sikre effektivisering gjennom økt digitalisering av det norske samfunnet må IKT-løsninger og digitale tjenester være tilstrekkelig sikre og pålitelige. Virksomheter og privatpersoner må ha tillit til at systemer og nettverk både fungerer slik de skal, og ivaretar personvernet til den enkelte. God IKT-sikkerhet og evne til å håndtere uønskede digitale hendelser er en forutsetning for å oppnå denne tilliten.

Utfordringene i det digitale rommet er grenseoverskridende – på tvers av land, sektorer og virksomheter, og utviklingen går svært fort. Hybride trusler visker ut det tradisjonelle skillet mellom fred og krig og utfordrer tradisjonell ansvarsplassering mellom sivil og militær sektor. Regjeringen ønsker derfor å styrke samarbeidet mellom private og offentlige virksomheter, mellom sivile og militære virksomheter og på tvers av landegrenser. På nasjonalt nivå vil Justis- og beredskapsdepartementet, Forsvarsdepartementet og Utenriksdepartementet ytterligere styrke sitt samarbeid på området.

1.2 Et felles ansvar

Alle virksomheter har ansvar for å ivareta egen IKT-sikkerhet. Hver enkelt statsråd har et overordnet ansvar for å ivareta IKT-sikkerheten i egen sektor. Justis- og beredskapsdepartementet har samordningsansvaret for IKT-sikkerhet i sivil sektor. Departementet skal utforme regjeringens politikk for IKT-sikkerhet, herunder etablere nasjonale krav og anbefalinger på IKT-sikkerhetsområdet for både offentlige og private virksomheter. Berørte fagdepartement, myndigheter og næringslivet skal involveres i dette arbeidet. Krav skal i nødvendig grad være hjemlet i lov og forskrift.

1.3 Forebyggende IKT-sikkerhet – virksomheters egenevne

Regjeringen er opptatt av å legge til rette for at virksomheter kan øke egenevnen til å forebygge uønskede digitale hendelser. Svaret på utfordringene innebærer ikke bare økte ressurser eller styrking av kapasitet. Hensiktsmessige regelverk og hensiktsmessig organisering står også sentralt for å sikre våre verdier.

Virksomheter er avhengige av komplekse digitale verdikjeder, og andres sårbarhet blir til egen sårbarhet. Det er nødvendig at virksomheter har tilstrekkelig oversikt over egen sårbarhet. En god oversikt setter virksomheten i stand til å vurdere hensiktsmessige tiltak.

Sentrale tiltak:

- nedsette et utvalg som skal utrede rettslig regulering på IKT-sikkerhetsområdet og organisering av tverrsektorielt ansvar
- legge bedre til rette for at virksomheter kan vurdere og prioritere tiltak innenfor IKT-sikkerhet gjennom systematisering og utvikling av anbefalinger og krav
- utvikle og vedlikeholde et godt og tilgjengelig kunnskapsgrunnlag som gjør enkeltindivider, virksomheter og myndigheter i stand til å treffe riktige tiltak for å opprettholde tilstrekkelig sikkerhet i sine IKT-systemer

1.4 Avdekke og håndtere digitale angrep

Regjeringen er opptatt av å styrke vår nasjonale evne til å avdekke og håndtere digitale angrep. Digitale angrep kan være krevende å oppdage og kan i ytterste konsekvens utgjøre en trussel mot nasjonale interesser og krenkelse av norsk suverenitet. Aktørene kan være andre stater, organiserte ikke-statlige grupperinger og private rettssubjekter. Målet til angriperne kan være å begå vinningskriminalitet, drive utpressing eller ødelegge eller endre informasjon eller funksjonalitet. Det kan også være å skaffe seg informasjon om stats- og forretningshemmeligheter, forskningsresultater eller teknologiske nyvinninger fra kommersielle bedrifter. Problemstillingene er ofte globale, og risikoen for straff og konsekvenser er lav.

Sett fra et stats- og samfunnssikkerhetsperspektiv er den største trusselen de aktørene som har ressurser til å gjennomføre handlinger som vi ikke oppdager, som oppdages for sent, som kan forårsake skader på kritisk infrastruktur, eller som kan påvirke demokratiske prosesser. I denne kategorien finner vi ofte statlige aktører, særlig andre lands sikkerhets- og etterretningstjenester.

En utfordring kan være at det oppstår usikkerhet og utilstrekkelig koordinering mellom myndighetsaktører som har ansvar for å bekjempe alvorlige digitale angrep. Regjeringen er derfor opptatt av å legge til rette for samarbeid og deling av informasjon.

Sentrale tiltak:

- videreutvikle det nasjonale varslingssystemet for digital infrastruktur (VDI) for å øke evnen til å avdekke digitale angrep
- etablere og videreutvikle et nasjonalt rammeverk for digital hendelseshåndtering som fører til mer effektiv håndtering og bedre samvirke mellom aktører
- etablere et informasjonsdelingsarbeid for å bedre samarbeidet mellom offentlige og private virksomheter ved digitale hendelser og etablere en teknisk plattform for deling av informasjon
- utrede og konkretisere hvordan en form for digitalt grenseforsvar kan etableres og lovreguleres
- gjøre politiet bedre i stand til å bekjempe kriminalitet i det digitale landskapet
- øke den nasjonale evnen til å motstå alvorlige digitale angrep gjennom videreutvikling av samarbeidet mellom Etterretningstjenesten, NSM, PST og politiet for øvrig
- forbedre NSMs evne til å analysere alvorlige digitale angrep mot samfunnskritisk infrastruktur og informasjon

1.5 IKT-sikkerhetskompetanse

Regjeringen ønsker å legge til rette for å styrke IKT-sikkerhetskompetansen i Norge og arbeide for at kompetansebehovene for IKT-sikkerhet i samfunnet og næringslivet blir ivaretatt.

IKT-sikkerhetskompetanse er en knapp ressurs nasjonalt og internasjonalt. Behovet for mer og bedre utdannet IKT-sikkerhetspersonell er understreket både i Lysneutvalgets utredning, i Meld. St. 10 (2016–2017) Risiko i et trygt samfunn og i Meld. St. 27 (2015–2016) Digital agenda for Norge. Regjeringen har de siste årene lagt til rette for bedre utdanningskapasitet og økt forskning på IKT-sikkerhet.

Sentrale tiltak:

- etablere en nasjonal kompetansestrategi for IKT-sikkerhet, der blant annet behovet for studieplasser og forskningssatsing vurderes
- gjennom den påbegynte fagfornyelsen i grunnopplæringen vurdere hvorvidt IKT-sikkerhet er tilstrekkelig inkludert i den grunnleggende digitale kompetansen elevene skal tilegne seg
- styrke IKT-sikkerhetskompetansen i tilsyn
- legge vekt på systematisk oppfølging og læring etter både øvelser og hendelser, også ved digitale hendelser

1.6 Kritisk IKT-infrastruktur

Vårt samfunn består av en rekke kritiske samfunnsfunksjoner, som energiforsyning, finansielle tjenester og satellittbaserte tjenester. Dette er funksjoner som må opprettholdes til enhver tid av hensyn til samfunnets og

befolkningens grunnleggende behov. En rekke av disse samfunnsfunksjonene forutsetter at man har en IKT-infrastruktur som virker nær sagt overalt og hele tiden.

IKT-infrastrukturer består av både informasjons- og kommunikasjonsinfrastrukturer (internettjenester, elektroniske kommunikasjonsnett etc.) og informasjons- og kommunikasjonssystemer som er en del av den kritiske samfunnsfunksjonen. Det kan eksempelvis være sentrale styrings- og kontrollsystemer, administrative systemer og logistikksystemer.

Beskyttelse av kritisk IKT-infrastruktur er et av hovedsatsingsområdene til EUs byrå ENISA. Alle medlemsland i EU oppfordres til å prioritere dette i sine nasjonale IKT-sikkerhetsstrategier. NATO setter også i større grad enn tidligere sivilt beredskapsarbeid og sivilt–militært samarbeid på dagsordenen. Sivil beredskap, krisehåndtering og robuste samfunnskritiske funksjoner er en forutsetning for det enkelte lands og dermed alliansens samlede beredskap og forsvar.

Regjeringen er opptatt av at kritisk IKT-infrastruktur må være robust og pålitelig, slik at uønskede hendelser i størst mulig grad unngås, samtidig som man raskt må kunne gjenopprette normalsituasjonen ved en uønsket hendelse. Vi må også være i stand til å sikre at uvedkommende ikke får tilgang til informasjonen som formidles gjennom slik infrastruktur. Beskyttelse av kritisk IKT-infrastruktur er sentralt i det arbeidet regjeringen gjør innenfor IKT-sikkerhet. En del av dette arbeidet er å delta på internasjonale arenaer.

Lysneutvalget trekker frem den nasjonale infrastrukturen for elektronisk kommunikasjon (ekom) som en sentral komponent som inngår i nær sagt alle digitale verdikjeder. I tråd med anbefalingene fra Lysneutvalget og Samferdselsdepartementets oppfølging av ekomplanen ble Nkom gitt i oppdrag å vurdere sårbarhetsreduserende tiltak knyttet til samfunnets og samfunnskritiske funksjoners avhengighet av Telenors kjerneinfrastruktur, og hvordan ulike transportnett og utlandsforbindelser kan kombineres for å øke den samlede nasjonale kapasiteten og sikkerheten i ekomnettene. I rapporten «Robuste og sikre nasjonale transportnett – Målbilder og sårbarhetsreduserende tiltak» fra april 2017 følger Nkom opp oppdraget og redegjør for dagens situasjon, forventet utvikling i markedet og hva som må til av eventuelle regulatoriske og budsjettmessige tiltak for å heve sikkerheten i de norske ekomnettene. Rapporten er et viktig kunnskapsgrunnlag for regjeringens videre arbeid på området.

I tillegg må virksomheter med ansvar for kritiske samfunnsfunksjoner som er sterkt avhengige av elektronisk kommunikasjon, selv vurdere tiltak som kan redusere risikoen for utfall i kommunikasjonen.

Sentrale tiltak:

- prioritere midler til etablering av en pilot for alternativt kjernenett, jf. Meld. St. 33 (2016–2017) Nasjonal transportplan 2018–2029
- arbeide videre med konkretisering av mulige statlige tiltak som kan bidra til å legge til rette for flere fiberkabler til utlandet
- arbeide for et sterkt kommunikasjonsvern i Norge

1.7 Oppfølging av Lysneutvalgets anbefalinger

Del III i meldingen gir som nevnt en oversikt over status på myndighetenes vurdering og oppfølging av Lysneutvalgets anbefalinger og en oversikt over prioriteringer i det videre oppfølgingsarbeidet. Justis- og beredskapsdepartementet vil benytte statusoversikten til å følge opp departementene i sivil sektor i det videre arbeidet med nasjonal IKT-sikkerhet.

Statusoversikten viser at det behov for en bred tilnærming til arbeidet med IKT-sikkerhet fremover. Flere sektorer arbeider med samme type utfordringer, for eksempel når det gjelder å utvikle kompetanse innenfor IKT-sikkerhet eller å håndtere en alvorlig digital hendelse. På grunnlag av vurderingene i del III, sammen med eksisterende kunnskapsgrunnlag, utviklingstrekk og utfordringsbilde på området, vil regjeringen vektlegge utvalgte tverrsektorielle områder. Regjeringen mener at disse områdene er av særlig betydning for nasjonal IKT-sikkerhet:

- Forebyggende IKT-sikkerhet – virksomheters egenevne
- Avdekke og håndtere digitale angrep
- IKT-sikkerhetskompetanse
- Kritisk IKT-infrastruktur

Det vises til meldingens del III for en nærmere gjennomgang av problembeskrivelsene i NOU 2015:13 og status på de ulike tiltakene.

1.8 Økonomiske og administrative konsekvenser

IKT-sikkerhet er et bredt fagområde som berører de fleste sektorer og mange ulike samfunnsområder. Meldingen tar ikke sikte på å gi en uttømmende redegjørelse for alt som gjøres av betydning for IKT-sikkerhet, men fremhever noen viktige prioriterte områder.

Vesentlige deler av IKT-sikkerhetsarbeidet skjer i hver enkelt sektor, basert på relevant sektorlovgivning samt spesifikke krav til departementenes samfunnssikkerhetsarbeid og arbeid med IKT-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. Endring i virkemiddelbruk, og eventuelle tiltak som iverksettes som et resultat av endringer i risiko- og sårbarhetsbildet, skal dekkes innenfor gjeldende budsjett-

rammer. Hvis tiltak medfører utgiftsøkninger over statsbudsjettet, vil regjeringen komme tilbake til dette i forbindelse med de årlige budsjettforslagene.

2. Komiteens merknader

Komiteen, medlemmene fra Arbeiderpartiet, Jan Bøhler, lederen Lene Vågslid og Maria Aasen-Svensrud, fra Høyre, Guro Angell Gimse, Sigurd Hille og Frida Melvær, fra Fremskrittspartiet, Liv Gustavsen og Solveig Horne, fra Senterpartiet, Geir Ingen Lien og Emilie Enger Mehl, og fra Sosialistisk Venstreparti, Petter Eide, vil vise til Meld. St. 38 (2016–2017) om IKT-sikkerhet, som er den første stortingsmeldingen om IKT-sikkerhet. Komiteen mener arbeidet med IKT-sikkerhet er svært viktig og hilser denne meldingen velkommen.

Komiteen vil vise til at det er utarbeidet flere analyser om digitale sårbarheter. Komiteen mener disse bidrar godt til bedre folkeopplysning og økt bevisstgjøring, samtidig som de bidrar til å gi myndigheter og virksomhetsledere et beslutningsgrunnlag for å utforme politikk og tiltak for å redusere sårbarhet.

Ettersom Norge er et av de mest digitaliserte landene i verden, er det etter komiteens mening avgjørende at alle nivå i samfunnet får tilgang til kunnskap og en større bevisstgjøring om sårbarheter i det digitale rommet. Komiteen støtter regjeringen sitt arbeid med å legge til rette for et styrket samarbeid på tvers av private og offentlige virksomheter, mellom sivile og militære virksomheter og på tvers av landegrenser for å avdekke og redusere digital sårbarhet i samfunnet.

Fleirtalet i komiteen, medlemene frå Arbeidarpartiet, Høgre og Framstegspartiet, registrerer at mange høyringsinnspel framhevar behovet for eit styrkt offentleg-privat samarbeid for å løyse utfordringar knytte til IKT-sikkerheit. Fleirtalet er samde i at offentleg og privat sektor har ulike kapasitetar, kunnskapar og kompetansar som kan utfylle kvarandre på ein god måte, og meiner vidare at regjeringa sitt forslag om å opprette eit felles forum for offentleg-privat samarbeid vil kunne støtte opp under og styrke det nasjonale arbeidet med IKT-sikkerheit.

Medlemene i komiteen frå Høgre og Framstegspartiet er positive til meldinga si heilskaplege og systematiske tilnærming til utfordringsbiletet.

Desse medlemene vil vise til at det i den kommande handlingsplanen til Nasjonal plan for IKT-sikkerheit vil bli lagt til rette for at verksemder på ein enkel måte kan vurdere og prioritere tiltak innanfor IKT-sikkerheit ut frå verksemda sin storleik og modningsnivå. Desse medlemene er vidare samde med Abelia sitt innspel om behov for folkeopplysning, og meiner at dette langt på veg blir tatt i vare og kan vidareutviklast gjennom «Nasjonal sikkerhetsmåned», som rettar seg direkte mot verksemder og enkeltindivid.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, mener det er positivt at det legges fram en melding som samler kunnskapen som foreligger. Meldingen inneholder gode beskrivelser av utfordringene på området, og når kunnskapen finnes, gjenstår det å omsette den til handling. Dette vil kreve felles innsats med flere aktører.

Flertallet vil påpeke at IKT-sikkerhet på et overordnet plan handler om å kunne beskytte den enkelte borger og nasjonen som helhet mot digitale sårbarheter og angrep. I tillegg er god datasikkerhet og godt personvern essensielt for at befolkningen skal ha tillit til IKT-systemer.

Flertallet merker seg at flere høringsinstanser mener meldingen ikke er konkret nok og ikke i tilstrekkelig grad viderefører analysene gjort av Lysne 1-utvalget.

Flertallet vil vise til at Norge ligger langt framme når det gjelder digitalisering, samtidig, som vi står i fare for ikke å klare å utvikle gode nok nasjonale kompetansemiljøer innenfor IKT, og mener dette er alvorlig all den tid IKT-kompetanse er nødvendig for å utvikle og drifte vital, kritisk digital infrastruktur. God rekruttering av dyktige og motiverte studenter innen IT og teknologi vil derfor være viktig.

Flertallet mener dette også er avgjørende for at teknologiutviklingen skal bidra til innovasjon og næringsutvikling. Med en høy digital kompetanse og en moderne og oppdatert maskinpark er vi i Norge særlig godt rustet til å ivareta og utvikle gode sikkerhetssystemer og en sikkerhetskultur i arbeids- og samfunnsliv.

Flertallet mener det er en svakhet ved meldingen at den ikke anerkjenner at både enkeltindivider og små virksomheter kan ha begrenset kapasitet til å sikre seg mot trusler på det digitale feltet, og er kritisk til at det ikke er foreslått tiltak for å redusere sårbarheten til denne gruppa, noe som også ble pekt på under høringen om meldingen i Stortinget 16. januar 2018.

Flertallet mener kunnskap om IKT-sikkerhet er avgjørende for bevisstgjøring og forebygging, og at denne type kunnskap er av stor betydning for å fremme en kultur for sikker adferd.

Flertallet mener at staten årlig bør ta ansvar for at viktig styringsinformasjon innhentes, og støtter Abelia sitt innspill om at Stortinget bør drøfte behovet for

en folkeopplysningskampanje som har som målsetting å bedre IKT-sikkerhetskulturen i Norge.

Komiteens medlemmer fra Arbeiderpartiet og Sosialistisk Venstreparti fremmer derfor følgende forslag:

«Stortinget ber regjeringen sørge for at staten årlig kartlegger den digitale sikkerhetskulturen i befolkningen. Kunnskapen må danne grunnlag for myndighetenes beslutningsgrunnlag og for råd og anbefalinger som gis til befolkningen og små virksomheter for å redusere digital sårbarhet.»

Selv om meldingen handler om IKT-sikkerhet og ikke informasjonssikkerhet, mener komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, at personvern i større grad burde vært drøftet. Flertallet mener at det bør fremskaffes en bedre oversikt over status, utfordringer og eventuelle farer for personvernet.

Komiteens medlemmer fra Arbeiderpartiet og Sosialistisk Venstreparti fremmer derfor følgende forslag:

«Stortinget ber regjeringen fremskaffe en oversikt over status, utfordringer og eventuelle farer for personvernet og komme tilbake til Stortinget på egnet måte.»

Komiteens medlemmer fra Senterpartiet og Sosialistisk Venstreparti viser til at meldingen ikke tar stilling til eller gir føringer knyttet til hva som er kritisk infrastruktur, og hvordan dette skal reguleres. Det er på det rene at deler av kritisk digital infrastruktur ikke vil falle inn under sikkerhetsloven. Det er derfor uklart hvilke rammer som gjelder for sikkerhets- og sårbarhetsanalyser for virksomheter som forvalter kritisk digital infrastruktur, men som faller utenfor sikkerhetslovens virkeområde. Dette er verken besvart i Prop. 153 L (2016–2017), som er forslag til ny lov om nasjonal sikkerhet (sikkerhetsloven), eller i denne meldingen. Disse medlemmer mener derfor at meldingen ikke i tilstrekkelig grad avklarer spørsmål som er viktig for IKT-sikkerheten.

Lysneutvalget

Komiteen vil vise til at et sentralt kunnskapsgrunnlag for arbeidet med IKT sikkerhet er NOU 2015:13 Digital sårbarhet – sikkert samfunn (Lysneutvalget). Komiteen vil videre vise til at dette utvalget vurderte digitale sårbarheter på flere nivåer – både på et overordnet samfunnsnivå og i tekniske infrastrukturer og systemer. Komiteen vil vise til at utvalget har gitt en rekke anbefalinger for å redusere digitale sårbarheter i samfunnet og i kritiske samfunnsinstitusjoner. Komiteen merker seg at Lysneutvalget viser til at Norge ligger langt fremme når det gjelder digitalisering, noe som gjør at vi som samfunn tidlig møter sårbarhetsutfordringer.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, mener Norges fremskutte posisjon innen den digitale utviklingen også burde medført en mer aktiv politikk for å møte spørsmål knyttet til digital sårbarhet. Det burde blant annet vært satset langt sterkere på utdanning og forskning innen IKT på et tidligere tidspunkt, samt lagt til rette for god og digital kompetanse gjennom hele opplærings- og utdanningsløpet. Flertallet mener særlig at Høyre- og Fremskrittspartiregjeringen i for liten grad har tatt digitale sårbarheter inn over seg. Flertallet merker seg at flere høringsinstanser peker på at regjeringen i stortingsmeldingen ikke viderefører analysene fra Lysne 1-utvalget i tilstrekkelig grad, og vil vise til Simula, som påpekte til justiskomiteen under høringen om meldingen 16. januar 2018 at sektoransvaret ikke tas nok på alvor av Justis- og beredskapsdepartementet. Simula etterlyser også et vesentlig høyere engasjement fra departementet når det gjelder oppbygging av kapasitet og påpeker at det ikke er tilstrekkelig med generelle bevilgninger for å oppnå tilstrekkelig oppbygging av kompetansemiljøer for IKT-sikkerhet.

Flertallet vil vise til at Lysne 1-utvalget fremhevet både øremerking av flere rekrutteringsstillinger og målrettede satsinger på IKT-sikkerhet på masternivå, og økte krav til IKT-sikkerhetsfag i de ulike IKT-bachelorutdanningene.

Komiteens medlemmer fra Arbeiderpartiet og Sosialistisk Venstreparti fremmer følgende forslag:

«Stortinget ber regjeringen sørge for at IKT-sikkerhet integreres som en obligatorisk del i alle IKT-studieprogrammer på bachelornivå.»

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, fremmer følgende forslag:

«Stortinget ber regjeringen sørge for at relevante ingeniør- og teknologiutdanninger har kurs i IKT-sikkerhet.»

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, viser til sine merknader i Innst. 364 S (2016–2017) og fremmer følgende forslag:

«Stortinget ber regjeringen utrede og foreslå konkrete tiltak som sikrer nødvendig kompetanse om IKT-sikkerhet hos alle kandidater med IKT-utdanning.»

IKT-sikkerhetskompetanse

Komiteen mener den åpne høringen 16. januar 2018 om IKT sikkerhetsmeldingen var viktig, og den gav komiteen mange viktige innspill. Komiteen registrerer at samtlige aktører på komiteens høring mente det var svært viktig med en melding om IKT-sikkerhet, og alle gav sin tilslutning til hovedtrekkene. Komiteen merker seg at et stort flertall av aktørene som deltok på høringen, særlig pekte på behov for økt kompetanse om IKT-sikkerhet. Komiteen merker seg behovet for økt IKT sikkerhetskompetanse innen både fagutdanningene og høyere utdanning. Komiteen er bekymret for mangelen på folk med IKT sikkerhetskompetanse. Komiteen registrerer særlig de klare tilbakemeldingene om det kritiske behovet for kryptologer.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, vil framheve høringsinstansenes bekymring for mangelen på IKT-kompetanse i samfunns- og arbeidslivet og viser her til mange forslag som er kommet fra blant annet Abelia, IKT Norge, NITO og Tekna. Gjennomgående er forslagene bredt anlagt, for eksempel om et økt omfang av studieplasser og rekrutteringsstillinger på alle nivåer, og hvor deler er øremerket IKT-sikkerhet spesielt. Men det fremheves også betydningen av mer praksis i studiene, av bedre muligheter for kompetanseheving og etter- og videreutdanning og større satsing på tverrfaglig teknologiforskning.

Medlemene i komiteen frå Høgre og Framstegspartiet registrerer at mange av høyringsinnspela framhevar behovet for auka kompetanse innan IKT-sikkerheit. Desse medlemene vil vise til den kommande nasjonale kompetansestrategien for IKT-sikkerheit som er under arbeid. Der vil regjeringa vurdere behovet for studieplassar og forskingssatsingar, og med bakgrunn i denne legge til rette for ei langsiktig oppbygging av IKT-sikkerheitskompetanse. Desse medlemene er samde i at det er behov for å styrke kompetansen innan IKT generelt og IKT-sikkerheit spesielt. Desse medlemene vil framheve regjeringa si offensive satsing med å legge til rette for betre utdanningskapasitet og auka forsking på IKT-sikkerheit dei seinare åra.

Desse medlemene vil framheve at om vi skal lykkast med det digitale skiftet, må vi også lykkast med den digitale sikkerheita, slik at vi tryggar viktig og kritisk informasjon. Regjeringa har tatt på alvor tilbakemeldingane frå IT-miljøa og sett i gang ei offensiv satsing med å legge til rette for betre utdanningskapasitet og auka forsking innan IKT og IKT-sikkerheit. Digital kompetanse har blitt og vil bli ein viktig del av opplæringa i grunnskulen og vidaregåande skule. I tillegg til mogelegheitene som ligg i teknologien, må det også vere fokus på trygg bruk. Regjeringa vil følgje opp dette i Meld. St 28 (2015–2016) Fag–Fordyping–Forståelse – En fornyelse av Kunnskapsløftet.

Desse medlemene viser til at det i fleire av høyringsinnspela vert vist til NIFU sin rapport «IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud», som syner at det vil bli betydeleg mangel på IKT-sikkerheitskompetanse i framtida. Rapporten baserer seg på historiske tal over studentar og uteksaminerte i perioden mellom 2012 og 2016. Desse medlemene vil understreke at det er sett i verk fleire strategiske tiltak for å møte desse utfordringane. Berre i 2016, 2017 og 2018 er det komme 1 500 nye IKT-studieplassar over heile landet. Når alle studieplassane er ferdig utbygde, vil det vere over 5 900 totalt. Regjeringa har også vedtatt 65 øyremerkte rekrutteringsstillingar i 2016 og 22 i 2018 med vekt på IKT-sikkerheit og kryptologi. Kunnskapsdepartementet har bedt utdanningsinstitusjonane om å prioritere IKT-sikkerheit, og har gjennom det gått lengre enn det som er vanleg nettopp for å trygge rekrutteringa.

Desse medlemene vil legge vekt på at Noreg er avhengig av å byggje framståande og varige forskingsmiljø innan IKT-sikkerheit. Gjennom Forskingsrådet sitt program IKTPluss «et trygt informasjonssamfunn» vart det i 2015 løyvd 150 mill. kroner til IKT-sikkerheitsprosjekt. Desse prosjekta er no i full gang. I 2018 vil det bli gitt høve til nye søknadar med ei totalramme på 200 mill. kroner. Regjeringa har i tillegg auka opp antal rekrutteringsstillingar (postdoktor- og stipendiatstillingar) til realfag, teknologi og IKT-sikkerheit, for å styrke kunnskap og forsking på området. Desse medlemene er glade for at det i FoU-strategien for samfunnssikkerhet (2015–2019) er lagt vekt på partnarskap, utvida kontakt og dialog mellom forsking, utdanning, myndigheiter og sluttbrukarar for å få etablert meir treffsikre og anvendelege prosjekt.

Desse medlemene vil understreke at det i nært samarbeid mellom tilbydarar og oppdragsgjevarar bør utviklast og leggast til rette for fleksible tilbod om kurs og etter- og vidareutdanningar til personar som har behov for IKT-sikkerheitskompetanse på arbeidsplassen, og at både offentleg og privat sektor vert oppmoda om å prioritere dette i sine verksemder.

Komiteens medlemmer fra Arbeiderpartiet og Sosialistisk Venstreparti mener det vil være fornuftig med en gjennomgang av IKT-studiene i fagskolene og høyskole- og universitetssektoren for å legge til rette for å utdanne og utvikle IKT-kompetanse.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, fremmer derfor følgende forslag:

«Stortinget ber regjeringen komme tilbake til Stortinget med forslag til klarere regler og rammer for sikkerhets- og sårbarhetsvurderinger i virksomheter som forvalter kritisk infrastruktur, men som faller utenfor sikkerhetslovens virkeområde.»

«Stortinget ber regjeringen innføre felles nasjonale krav til risiko- og sårbarhetsvurderinger av IKT-sikkerhet i virksomheter med kritisk infrastruktur.»

Flertallet viser til at Norge går mot kritisk kompetansemangel innenfor IKT. Vi lever i en tid med store teknologiske endringer. Jobber som vi kjenner, vil forsvinne, og nye jobber vil komme til. Norge har gode forutsetninger for å lykkes med endringene vi skal gjennom, men manglende spisskompetanse, for eksempel innenfor teknologi, kan bli en barriere for å skape vekst og nye arbeidsplasser i Norge. Flertallet mener at Høyre- og Fremskrittspartiregjeringen har styrt Norge mot kritisk kompetansemangel innenfor IKT. Dersom vi ikke gjennomfører et taktskifte, vil en av fire IKT-stillinger kunne stå ubesatte i 2030, ifølge rapport regjeringen selv har bestilt.

Flertallet vil trekke frem at til tross for at 30,7 pst. flere søkte seg til IKT-fagene for studieåret 2018–2019, var det i budsjettforslaget fra Høyre- og Fremskrittspartiregjeringen bare lagt opp til en minimal økning i antall studieplasser.

Komiteens medlemmer fra Arbeiderpartiet viser til at i Arbeiderpartiets alternative statsbudsjett ble det foreslått 3 000 nye studieplasser i 2018, hvorav minst 1 000 skulle gå til IKT og teknologi. Det er også i tråd med budsjettkravet fra bransjen, ved IKT Norge, Abelia, NITO og Tekna.

Komiteens medlemmer fra Senterpartiet viser til sitt alternative budsjett, der det er foreslått å opprette1 000 nye studieplasser innen IKT-fag.

Komiteens medlem fra Sosialistisk Venstreparti vil vise til sine merknader til statsbudsjettet 2018 i Innst. 12 S (2017–2018), og til Sosialistisk Venstrepartis alternative budsjett, hvor det ble prioritert midler til 500 studieplasser innenfor IKT ut over regjeringens forslag.

Komiteens medlemmer fra Arbeiderpartiet og Sosialistisk Venstreparti vil ha en solid satsing på digitalisering i hele utdanningsløpet. Digital kompetanse er for viktig til å overlates til et valgfag i ungdomsskolen, slik regjeringen til nå har gjort. Valgfag er kun for elever som er så heldige å gå på en skole med råd til å opprette et nytt fag som det – for det store flertallet av skoler – ikke følger penger med til.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, viser til at den viktigste grunnen til en storsatsing på digitale læremidler i skole og utdanning også er at elever kan lære mer, få bedre oppfølging og oppleve mer variasjon og motivasjon på skolen. Det forutsetter en bred satsing på gode digitale læremidler, en satsing på lærernes pedagogiske kompetanse i god bruk av dem og tilgang til datamaskiner/nettbrett og andre digitale verktøy.

For at befolkningen skal få påfyll av kunnskap og kompetanse som setter oss i stand til å ta i bruk ny teknologi og de mulighetene digitalisering kan gi, vil komiteens medlemmer fra Arbeiderpartiet satse på koding/programmering for alle elever – allerede i barneskolen – moderne og oppdatert utstyr på yrkesfagene, 1 000 flere IKT-studieplasser og gjennomføre en bred kompetansereform for arbeidslivet, i samarbeid med partene.

Disse medlemmer viser til at Arbeiderpartiet hadde rundt 275 mill. kroner mer enn Høyre- og Fremskrittspartiregjeringen til IKT-satsing i budsjettforslaget for 2018.

Disse medlemmer vil opprette et nytt forskningsprogram i IKT og datasikkerhet. For å øke forskningen på IKT og datasikkerhet foreslo Arbeiderpartiet i sitt alternative statsbudsjett et nytt forskningsprogram under Norges forskningsråd, på minimum 50 mill. kroner allerede i 2018.

Disse medlemmer er skuffet over at regjeringspartiene stemte ned Arbeiderpartiets forslag. I budsjettet for 2018 var det også realnedgang i bevilgningene til forskning, og disse medlemmer etterlyser særlig en større satsing på forskning knyttet til IKT og datasikkerhet.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, viser til at det er stor variasjon mellom de ulike kommunene når det gjelder bruk av digitale læringsmidler og fokus på digital kompetanse. Flertallet er opptatt av at det ikke skapes et digitalt klasseskille mellom dem som bruker slike verktøy, og de som ikke gjør det. For at kommunene skal kunne anskaffe nødvendig utstyr og sørge for god kvalitet i undervisningen, kreves det først og fremst en solid kommuneøkonomi.

Komiteens medlemmer fra Senterpartiet viser til at Senterpartiet i sitt alternative budsjett har lagt opp til en kraftfull satsing på kommuner og fylkeskommuner. Overføringene til kommunesektoren ble

samlet sett foreslått økt med 3,9 mrd. kroner sammenlignet med regjeringens forslag. Disse medlemmer viser videre til Senterpartiet sine merknader i Innst. 12 S (2017–2018):

«Disse medlemmer er bekymret for at manglende dekning av høyhastighets bredbånd fører til et digitalt klasseskille i Norge, og at regjeringens manglende oppfølging og kutt i tilskuddsmidler forsterker den skjeve utviklingen mellom ulike deler av landet. Disse medlemmer viser til at dette også påvirker skolens oppdrag og vilkår. I Senterpartiets alternative statsbudsjett ble det derfor foreslått å øke satsingen på høyhastighets bredbånd med 500 mill. kroner, samt en forsterket satsing på koding i grunnopplæringen og økning i antall studieplasser innen IKT-studier, inkludert økt kapasitet på masternivå for å utdanne flere IT-eksperter.»

Komiteens medlem fra Sosialistisk Venstreparti vil vise til at Sosialistisk Venstreparti i sitt alternative budsjett foreslo en økning i overføringer til kommunene direkte på 4,6 mrd. kroner mer enn regjeringen og en økning på 100 mill. kroner til satsing på bredbånd.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, er enige med Tekna sitt høringsinnspill, som peker på at sikkerhet må integreres i utviklingen av alle nye systemer, ikke minst i den første fasen man designer et system. Flertallet mener derfor det er viktig at sikkerhet integreres i alle IKT-utdanninger. Et godt personvern og god datasikkerhet er essensielt for nasjonens sikkerhet, men også for at befolkningen skal ha tillit til systemene.

Flertallet fremmer derfor følgende forslag:

«Stortinget ber regjeringen sørge for at det stimuleres til bedre etter- og videreutdanningstilbud på fagskoler, universiteter og høyskoler innen IKT- og datasikkerhet.»

Flertallet vil vise til Innst. 19 S (2016–2017), der flertallet hadde følgende merknad om betydningen av koding i skolen. Flertallet mener at dette viser til utfordringer som regjeringen fremdeles ikke har tatt på alvor.

«Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet, Venstre og Sosialistisk Venstreparti, mener det teknologirike samfunnet utfordrer måten vi lærer på, og hvilke fremtidskompetanser som blir viktige. Flertallet merker seg at det i NOU 2013:2 Hindre for digital verdiskaping, ble påpekt en manglende kompetanse i koding/programmering i befolkningen og et behov for å legge til rette for at barn og unge ikke bare er i stand til å bruke, men også skape digitalt innhold og digitale tjenester. Flertallet viser til at EU har satt koding på sin «Digital Agenda for Europe» og at de oppfordrer utdanningsministre i medlemslandene til å fremme koding i skolen. Flertallet har registrert de positive erfaringene flere skoler i Norge har gjort med koding/programmering som valgfag og gjennom ulike prosjekter under paraplyen «Lær kidsa koding». Flertallet merker seg at det er gjort positive erfaringer fra disse prosjektene både når det gjelder elevenes digitale og teknologiske kompetanse og knyttet opp mot realfag, som for eksempel matematikk.

Flertallet mener derfor at koding/programmering bør inngå som en del av opplæringen for alle elever i skolen.»

Flertallet fremmer følgende forslag:

«Stortinget ber regjeringen sørge for at digitalisering og IKT-sikkerhet prioriteres i neste Langtidsplan for forsking og høyere utdanning.»

«Stortinget ber regjeringen sørge for at alle elever gjennom grunnskolen får erfaring med programmering, og at dette starter allerede på barneskolen.»

Flertallet vil peke på at mange høringsinstanser har etterlyst satsing på kompetanseheving av IKT, og IKT-sikkerhet spesielt. Flertallet vil også vise til Rapport fra NIFU: «IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud», som viser at det vil være manglende samsvar mellom tilbud og etterspørsel på rundt 4 100 personer i år 2030 innenfor IKT-sikkerhet. Flere har lansert forslag som satsing på nærings-PhD-er, og oppbygging av en etter- og videreutdanning.

Kryptologer

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, er bekymret over tilbakemeldinger fra organisasjoner og fagmiljøer om at det er kritisk mangel på kandidater som kan sikkerhetsklareres og utdannes til kryptologer. Flertallet understreker at det er en krise under oppseiling innenfor kryptografi, slik flere høringsinstanser påpekte under justiskomiteens høring om stortingsmeldingen.

Flertallet mener det har vært for svak satsing direkte for å utdanne og rekruttere flere kandidater til kryptologiutdanningen.

Flertallet merker seg at det i stortingsmeldingen vises til at den nasjonale kryptopolitikken skal revideres (kapittel 22.11) av Forsvarsdepartementet og Justis- og beredskapsdepartementet. Flertallet støtter dette, men vil, slik Simula etterlyser i sitt innspill til justiskomiteen, påpeke at det er viktig at dette arbeidet gjøres i åpenhet. Flertallet mener som Simula at det sivile kompetansemiljøet må brukes aktivt for å sikre at kryptopolitikken blir revidert på en best mulig måte.

Flertallet fremmer følgende forslag:

«Stortinget ber regjeringen igangsette konkrete tiltak for å øke rekrutteringen av PhD-kandidater som kan sikkerhetsklareres.»

Tjenesteutsetting

Komiteen registrerer noen ulike syn når det gjelder spørsmålet om tjenesteutsetting. Flere av aktørene som møtte til komiteens høring 16. januar 2018, mener at drift av systemer som håndterer sensitive personopplysninger, skal skje i Norge, mens andre aktører som Abelia mener at det viktigste er å sørge for sikrere prosjekter, sterkere bestillerkompetanse og utførelse av nødvendige risikoanalyser som vil kreve kompetanse ut over dagens nivå.

Medlemene i komiteen frå Høgre og Framstegspartiet støttar opp om regjeringa sitt synspunkt om at tenesteutsetjing til profesjonelle aktørar vil kunne gi betre tryggleik og meir stabile og tilgjengelege tenester til ein lågare og meir føreseieleg kostnad. Vidare er desse medlemene samde i at dette fordrar god forståing av – og bevisstheit om – ansvar, risiko, bestillarkompetanse og oppfølging av leverandørar. Desse medlemene meiner at det er viktig å legge til rette for eit tydeleg regelverk, relevant og oppdatert rettleiing og god informasjon, for å styrke verksemder si eigenevne til førebyggjande IKT-sikkerheit. Desse medlemene meiner at nasjonale satsingar på utdanning, forsking og utvikling knytte til IKT-tryggleik òg vil kunne fremje og forsterke konkurransedyktige nærings- og kompetansemiljø i Noreg.

Fleirtalet i komiteen, medlemene frå Arbeidarpartiet, Høgre og Framstegspartiet, er samde i at IKT-sikkerheitsmeldinga må sjåast i samanheng med den nyleg vedtekne Prop. 153 L (2017–2018), Lov om nasjonal sikkerhet (sikkerhetsloven). I forarbeidet er det gjort grundige vurderingar av kva krav som skal leggast til grunn ved mellom anna sikkerheitsgraderte anskaffingar. Den vedtekne lova stiller krav til sikkerheitsavtaler, leverandørklarering og at verksemder vert pålagt ei varslingsplikt ved sikkerheitsgraderte anskaffingar. For at utanlandske leverandørar skal kunne leverandørklarerast, må det mellom anna ligge føre ei bi- eller multilateral avtale om utveksling og plikt til gjensidig vern av sikkerheitsgradert informasjon mellom norske myndigheiter og heimstaten til leverandøren. Fleirtalet vil i tillegg framheve at regelverk om eigarskapskontroll er tatt inn i sikkerheitslova for å hindre at nasjonal sikkerheit vert skadelidande ved at verksemder blir kjøpte opp av utanlandske aktørar. Kongen i statsråd vil gjennom dette få heimel til å stoppe oppkjøp av verksemder som ligg under sikkerheitslova.

Fleirtalet meiner at innovasjon og teknologiutvikling ofte skjer i møte mellom selskap – også på tvers av landegrenser. Fleirtalet viser til at vi er avhengige av eit tillitsbasert, nasjonalt og internasjonalt samarbeid både for å utvikle system, og ikkje minst for å løyse mange av dei utfordringane vi ser utviklar seg i det digitale rommet. Ingen land løyser desse utfordringane åleine. Som for andre delar av IKT-området føreset tenesteutsetjing at verksemdene har tilstrekkeleg kompetanse og oversikt over risikobiletet, og det er grunn til å understreke verksemdene sitt ansvar for dette. Fleirtalet vil vere tydelege på at grundige risiko- og sårbarheitsanalyser skal leggast til grunn ved sikkerheitsgraderte anskaffingar, og på dei premissane som er nedfelte i sikkerheitslova og anna styringsverktøy.

Et annet flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, mener økt bestillerkompetanse og et tydelig og klart regelverk er av stor betydning og helt nødvendig for å ivareta sikkerheten for personsensitive opplysninger så vel som opplysninger om vital infrastruktur. Det er etter dette flertallets oppfatning likevel ikke nok. Det viser flere konkrete tilfeller i senere tid, og dette flertallet er bekymret for konsekvensene av tjenesteutsetting av IKT-drift. En konsekvens etter tjenesteutsetting av IKT i Helse Sør-Øst var at helseforetaket måtte bruke flere hundre millioner kroner på å komme seg ut av avtalen Helse Sør-Øst hadde inngått, slik NITO beskriver i sitt høringsinnspill til justiskomiteen. Dette flertallet vil videre vise til Nødnett eller Broadnet-saken, som tydelig har vist behovet for mer presis lovgivning.

Dette flertallet vil vise til at NRK i fjor vinter avdekket at IT-arbeidere i India hadde tilgang til deler av det norske nødnettsystemet. Motorola og underleverandøren Broadnet driftet nettet for det tidligere Direktoratet for nødkommunikasjon, som ble underlagt Direktoratet for samfunnssikkerhet og beredskap 1. mars 2017. NRK-avsløringen viste at Broadnet ga tilgang til nødnettet til IT-arbeidere hos en indisk underleverandør uten at disse hadde nødvendig tillatelse eller sikkerhetsklarering. Dette flertallet viser til at dette er et alvorlig eksempel på en sikkerhetsglipp mot kritisk infrastruktur omfattet av sikkerhetsloven.

Dette flertallet mener at behandlingen av sikkerhetsloven må ses i sammenheng med behandlingen av IKT-sikkerhetsmeldingen. Dette flertallet vil vise til Arbeiderpartiets, Senterpartiets og Sosialistisk Venstrepartis merknader i Innst. 103 L (2017–2018), Lov om nasjonal sikkerhet:

«Disse medlemmer mener at informasjon knyttet til nasjonale sikkerhetsinteresser må pålegges å bli driftet og lagret i Norge. Disse medlemmer vil understreke at outsourcing av utvikling og drift av kritiske nasjonale IKT-tjenester og system ikke må aksepteres, og at det må innføres klare nasjonale krav til vurdering av sikkerhet og sårbarhet.

Disse medlemmer viser til IKT-skandalen i Helse Sør-Øst som angår IKT-drift i Sykehuspartner. Konsekvensen av denne avtalen var at uvedkommende kunne

få tilgang til pasientdata om 2,8 millioner nordmenn. Derved kunne sensitiv personinformasjon komme på avveie, og dessuten kunne uvedkommende kartlegge en infrastruktur som kunne brukes til sabotasje som kunne lamme Norge. Denne saken viser at lovverk og departementets praksis i dag ikke er betryggende.»

Komiteens medlemmer fra Arbeiderpartiet og Sosialistisk Venstreparti fremmer følgende forslag:

«Stortinget ber regjeringen sørge for at systemer som håndterer data knyttet til nasjonale sikkerhetsinteresser, driftes fra Norge.»

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, fremmer følgende forslag:

«Stortinget ber regjeringen sørge for at ved en eventuell lagring av data i annet land må risiko- og sårbarhetsvurderingen også omfatte lovverk og sikkerhetssituasjon i landet der dataene lagres.»

Komiteens medlemmer fra Senterpartiet og Sosialistisk Venstreparti fremmer følgende forslag:

«Stortinget ber regjeringen sørge for at svært sensitive personopplysninger blir lagret og driftet i Norge.»

«Stortinget ber regjeringen sørge for at informasjon knyttet til nasjonale sikkerhetsinteresser blir lagret og driftet i Norge.»

Disse medlemmer viser til at utsetting av statlige IKT-tjenester øker risikoen for sårbarhet og at flere som ikke skulle hatt tilgang til sensitiv informasjon, får det. Disse medlemmer viser til nylig sak i Helse Sør-Øst om hvordan personer i utenlandske selskaper som ikke skulle hatt tilgang til helseinformasjon om norske pasienter, har hatt det uten at foretaket har vært informert om dette. Det viser også hvordan det har vært mulig for utenforstående å få oversikt over systemet slik at det senere kan saboteres. Dette forholdet blir nå etterforsket av PST.

Komiteens medlem fra Sosialistisk Venstreparti mener at sensitive personopplysninger om norske borgere og den norske stat i hovedsak skal forvaltes innenfor Norges grenser, og skal være underlagt nasjonal kontroll. Det er vesentlig at denne type informasjon ivaretas innenfor norsk jurisdiksjon.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, vil for øvrig vise til sine merknader i Innst. 103 L (2017–2018), og spesielt til merknadene om kontroll over infrastruktur, hvor det fremgår:

«Disse medlemmer vil understreke at outsourcing av utvikling og drift av kritiske nasjonale IKT-tjenester og system ikke må aksepteres, og at det må innføres klare nasjonale krav til vurdering av sikkerhet og sårbarhet.»

På den bakgrunn fremmer flertallet følgende forslag:

«Stortinget ber regjeringen fremme en sak hvor det foreslås tiltak for hvordan man kan redusere nasjonal sårbarhet og sikre nasjonal kontroll over kritisk IKT-infrastruktur. Regjeringen bes videre se på ulike kontrollrutiner som må iverksettes ved utsetting av informasjonshåndtering til utenlandske selskaper eller tredjeparter.»

Utrede et digitalt grenseforsvar

Komiteen vil vise til at meldingen tar opp utfordringene med å avdekke digitale angrep og berører spørsmålet om et digitalt grenseforsvar i Norge. Komiteen er kjent med Lysne II-utvalget, som har utredet de prinsipielle sidene ved en eventuell tilgang for E-tjenesten til digital kommunikasjon ut og inn av Norge. Komiteen registrerer at regjeringen vil utrede og konkretisere hvordan et digitalt grenseforsvar kan etableres og lovreguleres. Komiteen registrerer videre at det i en slik utredning vil være avgjørende å finne en balanse mellom den sikkerhets- og etteretningsmessige effekten av dette og de personvernrelaterte spørsmålene en slik tilgang reiser. Komiteen mener denne balansen er viktig i en slik utredning. Komiteen merker seg også innspillene fra blant andre Advokatforeningen som kom frem under justiskomiteens høring om meldingen.

Fleirtalet i komiteen, medlemene frå Arbeidarpartiet, Høgre og Framstegspartiet, viser til regjeringa sitt pågåande arbeid med å utgreie og konkretisere korleis eit digitalt grenseforsvar kan etablerast og lovregulerast. Omsynet til personvernet utgjer ein viktig del av dette utgreiingsarbeidet. Fleirtalet vil vidare minne om at ansvaret for utgreiinga er lagt til Forsvarsdepartementet, og at den politiske handsaminga av saka om eit digitalt grenseforsvar vil bli lagt til utanriks- og forsvarskomiteen når utgreiinga er klar og venta til Stortinget i løpet av 2018.

Komiteens medlemmer fra Senterpartiet og Sosialistisk Venstreparti mener at overvåking og kontroll må hvile på en etisk og prinsipiell tilnærming og være minst mulig inngripende overfor innbyggerne. Stortinget har ansvar for å legge til rette for et trygt samfunn, men samtidig må det gjøres fornuf-

tige avveininger mellom sikkerhetshensyn og hensynet til personvernet. Disse medlemmer mener det må settes klare grenser for hvor langt offentlige styresmakter og andre kan gå i retning av innsyn eller kontroll med den enkeltes gjøremål. Dette er bakgrunnen for at Senterpartiet og Sosialistisk Venstreparti var sterkt imot datalagringsdirektivet og kjempet for betydelige endringer i regjeringens forslag om å utvide politiets og PSTs overvåkingsfullmakter. Disse medlemmer imøteser forslag som kan styrke Norges digitale forsvarsevne, men samtidig er det viktig at det ikke åpnes opp for masseovervåking av lovlydige borgere.

Komiteens medlem fra Sosialistisk Venstreparti viser til at regjeringen vil utrede og konkretisere lovendringer for å opprette et digitalt grenseforsvar. Dette medlem vil understreke at det ikke er et forsvar i den forstand at det vil kunne stanse pågående cyberangrep på den norske stat eller virksomheter, men er et etterretningsvirkemiddel for å oppdage slike angrep. Ifølge utvalget er formålet å sette e-tjenesten i stand til å «kartlegge og motvirke ytre trusler mot rikets selvstendighet og sikkerhet og andre viktige nasjonale interesser». Opprettelse av et digitalt grenseforsvar i tråd med Lysne II-utvalgets forslag vil innebære at all datatrafikk som krysser grensen, vil bli lagret. Det betyr det aller meste av datatrafikk, e-poster, facebook-meldinger, google-søk, snapchat-meldinger osv. Dataene vil bli lagret også hvis det kun er kommunikasjon mellom norske borgere, fordi trafikken ofte går via servere i utlandet. Dette understreker i hvor stor grad personvernet til enkeltmennesker kan bli kompromittert, og hvor utsatt denne informasjonen er for eksempel ved en formålsutglidning eller ved svake kontrollmekanismer.

Dette medlem mener at kontrollmekanismene utvalget la til grunn, var for svake. Spesielt forslaget om å opprette en spesialdomstol knyttet til e-tjenesten viser at kontrollen vil bli for lite uavhengig. Dette må vurderes nøye ved et eventuelt forslag om digitalt grenseforsvar. Det er store problemstillinger knyttet til om et slikt tiltak er i tråd med menneskerettighetene og utviklingen av rettspraksis fra EU-domstolen. Dette må vurderes nøye og konkret ved et eventuelt forslag.

Dette medlem vil også peke på at det i alle tilfeller vil være krevende for offentligheten å ta stilling til et digitalt grenseforsvar all den tid det er usikkert og umulig å diskutere offentlig hvor effektivt det vil være, i hvor stor grad e-tjenesten kan lese kryptert innhold, og hvor enkelt det vil være å omgå dette. Det vil derfor være vanskelig å vurdere om inngripen i personvernet kan forsvares gjennom effekten av tiltaket.

Dette medlem mener derfor at regjeringen ikke kun kan begrense den nasjonale cybersikkerheten til å fokusere på et digitalt grenseforsvar. Det bør være ønskelig at det i tillegg til Lysne II-utvalget også settes ned et utvalg som skal utrede tiltak for å styrke vår digitale forsvarsevne uten å åpne for det som reelt sett er masseovervåkning av norske borgere. Et alternativ kan være å se på en utvidelse av VDI-systemet som vi i dag har for å beskytte kritisk infrastruktur i Norge. Dette medlem mener at det er viktig å se på dette samlet og ikke kun satse på et digitalt grenseforsvar.

På den bakgrunn fremmer dette medlem følgende forslag:

«Stortinget ber regjeringen sette ned et utvalg som skal utrede tiltak for å styrke vår digitale forsvarsevne uten å åpne for masseovervåkning av norske borgere.»

Komiteens medlemmer fra Arbeiderpartiet og Sosialistisk Venstreparti mener også at det er behov for et løft for cyberforsvaret og Nasjonal sikkerhetsmyndighet, slik at de kan sikres flere ressurser og økt kompetanse. Det er derfor nødvendig med en forpliktende opptrappingsplan. Disse medlemmer vil derfor fremme følgende forslag:

«Stortinget ber regjeringen komme tilbake med forslag om en opptrappingsplan for Nasjonal sikkerhetsmyndighet og e-tjenesten for å sikre mer ressurser, økt kompetanse og bedre samordning mellom aktørene i cyberforsvaret.»

Disse medlemmer viser til NRKs sak 2. mars 2018 om at persondata om norske borgere er samlet inn gjennom E-tjenestens lyttestasjoner på Ringerike. Disse medlemmer viser til lov om Etterretningstjenesten § 4, hvor det heter:

«Etterretningstjenesten skal ikke på norsk territorium overvåke eller på annen fordekt måte innhente informasjon om fysiske eller juridiske personer.»

Disse medlemmer henviser også til uttalelser fra leder av EOS-utvalget Eldbjørg Løwer, hvor hun sier til NRK 2. mars 2018:

«Vi har vært usikre på om den måten E-tjenesten har utført disse oppgavene har vært tilstrekkelig hjemlet i dagens lov.»

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, vil videre vise til at sjefen for Etterretningstjenesten, generalløytnant Morten Haga Lunde, uttalte til NRK den 5. mars 2018 at § 3 i Lov om Etterretningstjenesten gir hjemmel til å samle inn metadata og til å operere innenfor kommunikasjonsetterretning i luftsnittet. Fagdirektør i Norges nasjonale institusjon for menneskerettigheter, Anine Kierulf, uttalte på samme sted at denne bestemmelsen er for generell og ikke gir tilstrekkelig hjemmel. § 3 i Lov om Etterret-

ningstjenesten angir ingen vilkår for overvåkning, hvor lenge dataene kan lagres, og hva dataene kan brukes til. Flertallet mener dette viser at det er et behov for en avklaring av hvorvidt E-tjenesten har hjemmel i Lov om Etterretningstjenesten til å lagre metadata som blant annet inneholder informasjon om norske borgere.

Komiteens medlem fra Sosialistisk Venstreparti mener det er sentrale elementer som må reguleres om metadata skal lagres på den måten det gjøres i dag, og at dette må skje på bakgrunn av en offentlig debatt. Det er ikke tvilsomt at etterretningstjenesten skal kunne drive etterretning i en digitalisert tidsalder hvor datastrømmene går via andre land, men da må dette skje etter en klar lovhjemmel og på strenge vilkår.

Dette medlem viser til Lysne II-utvalget, som drøfter en løsning med såkalt positiv filtrering dersom det er nødvendig å lagre store deler datamateriale slik det gjøres ved denne lytteposten. Dette er en løsning hvor man på forhånd vil spesifisere hva som skal tillates benyttet til etterretningsformål. Alle datastrømmer som ikke maskinelt gjenkjennes som noe som skal tas vare på, blir da filtrert vekk. Utvalgets vurdering er at:

«Forskjellen i positiv og negativ filtrering kommer til syne når det er en del av datatilfanget som verken kan defineres som klart relevant eller klart irrelevant.»

Dette medlem mener at ved innføring av et krav om positiv filtrering må myndighetenes overvåkingsorganer hente inn en kjennelse fra domstolene på forhånd for å kunne søke i de lagrede dataene. Dette medlem mener det også bør vurderes en godkjenning fra domstolene av formål og objekter ved overvåkingen.

Dette medlem mener regjeringen først og fremst må redegjøre for hvorvidt denne type overvåkning er innenfor dagens lov. I tillegg bør regjeringen utrede og komme tilbake til Stortinget med forslag til en klargjøring av hjemmelen, og vilkårene, for denne type innhenting av datainformasjon som uunngåelig vil involvere norske borgere.

På denne bakgrunn fremmer komiteens medlemmer fra Senterpartiet og Sosialistisk Venstreparti følgende forslag:

«Stortinget ber regjeringen klargjøre hvorvidt lov om etterretningstjenesten § 3 gir hjemmel til å samle inn metadata og til å operere innenfor kommunikasjonsetterretning i luftsnittet.»

«Stortinget ber regjeringen utrede og komme tilbake til Stortinget med forslag om vilkår for metadatainnsamling, lagringslengde og hvordan dataene skal brukes etter lov om etterretningstjenesten, herunder en ordning med godkjenning av domstol for innsamling og lagring av slike metadata, og godkjennelse for bruk.»

Digital infrastruktur

Fleirtalet i komiteen, medlemene frå Arbeidarpartiet, Høgre, Framstegspartiet og Senterpartiet, er samde i behovet for å bli mindre avhengige av Telenor sitt kjernenett. Fleirtalet viser til at det er sett av totalt 80 mill. kroner til eit pilotprosjekt for eit alternativt kjernenett.

IKT-kriminalitet

Komiteen mener et sentralt område i arbeidet med å forebygge, avdekke og etterforske kriminalitet nå handler om IKT-kriminalitet. Komiteen registrerer at IKT-kriminalitet øker i omfang både hva gjelder kriminalitet rettet mot selve IKT-systemet, men også kriminelle handlinger begått ved hjelp av IKT. Komiteen registrerer at meldingen viser til at flere rapporter og utredninger viser behov for å styrke politiets kompetanse og kapasitet på området. Komiteen mener etableringen av et cybersikkerhetssenter er viktig i denne sammenhengen.

Komiteen stiller seg positiv til å opprette et nasjonalt senter for å forebygge og bekjempe IKT-kriminalitet (Cyber Crime Center) og viser til Politidirektoratets (POD) pågående prosess med en slik etablering.

Medlemene i komiteen frå Høgre og Framstegspartiet ser at IKT-kriminalitet raskt aukar i omfang, og at det er behov for fokus på politiet sin kompetanse og kapasitet på området. Desse medlemene viser til at regjeringa har sett i verk fleire tiltak for å styrke politiet si evne til å førebyggje og bekjempe IKT-kriminalitet gjennom t.d. lovendringar knytte til skjulte tvangsmiddel og ein eigen strategi for digital kompetanseheving i politiet. Desse medlemene er samde i at det må leggast til rette for å gi politiet naudsynte verkemiddel for å kunne beskytte borgarane og samfunnet effektivt i samsvar med politilova § 2, og understrekar at det i tilstrekkeleg grad må takast omsyn til borgarane sitt behov for vern mot inngrep.

Desse medlemene er opptatte av å styrke politiet sine føresetnadar for å nedkjempe IKT-kriminalitet gjennom auka fokus på kompetanse. Politiutdanninga skal styrkast, og ein må vurdere å opne opp for at personar utan politifagleg utdanning, t.d. spesialistar med høg teknologisk spisskompetanse, får tilbod om politifagleg tilleggsutdanning. Desse medlemene vil vise til Justis- og beredskapsdepartementet sitt pågåande arbeid med å revidere POD sin strategi for digital kompetanseheving og at det i denne samanhengen vert vurdert å legge fram ei eiga stortingsmelding.

Komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, ser at omfanget av IKT-kriminalitet vokser raskt, med seksuallovbrudd, ID-tyveri, bedragerisaker m.m. Kriminelle nettverk blir stadig mer sofistikerte i sin kommunikasjon, og cyberangrep utgjør en stadig større trussel mot staten, bedrifter og enkeltpersoner. Endringene som skjer ved at det tas i bruk ny teknologi, gjør at alt blir mer effektivt og komplekst, også kriminaliteten og hvordan den begås. I tillegg skapes det stadig nye sårbarheter og svakheter som de kriminelle kan utnytte og angripe. Det kreves en styrking totalt sett av politiet for å være rustet til å møte og håndtere disse endringene.

Flertallet er bekymret for at politiet ikke er satt i god nok stand til å henge med på denne utviklingen. Ikke fordi det mangler engasjement, vilje eller erkjennelse, men fordi det mangler kompetanse, utstyr og kapasitet.

Komiteens medlemmer fra Arbeiderpartiet og Senterpartiet mener at regjeringen og forlikspartiene ikke har tatt dette godt nok inn over seg i sine forslag til statsbudsjett. Disse medlemmer mener særlig den stramme driftssituasjonen politidistriktene er satt i for 2018, vanskeliggjør arbeidet med å ruste opp innsatsen på dette feltet.

Slik komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, ser det, er det en viktig kobling mellom vinningskriminalitet på nett og samfunnssikkerhet. Bedrageri, svindel og utpressingssaker som i det store bildet kan karakteriseres som «småsaker», er ofte utført av godt organiserte aktører som gjennom sin virksomhet tilføres store summer. Dette utgjør en trussel mot sårbare individer, men også mot samfunnet.

Flertallet har registrert at det er en rekke tiltak som nå er under etablering eller burde etableres i politiet for å bekjempe alle former for IKT-kriminalitet. Nettpatruljene som skal etableres i alle politidistrikt, vil kreve mannskap, monitoreringsplattformer og investeringer i både maskinvare og programvare, samt en plattform for innhenting av materiale fra publikum og vil sannsynligvis ha store utviklings- og investeringskostnader framover. Lagring av innhentet og beslaglagt informasjon er en annen utfordring politiet står overfor, ettersom datamengdene øker, og lagringskapasiteten er for liten. Mannskap med IKT-kompetanse, både politi og sivile, er en mangelvare over hele landet, og det må påregnes betydelige kostnader forbundet med fagutvikling, kursing og etterutdanning. Flertallet mener derfor det er nødvendig med en reell økonomisk satsing på politiet for å bekjempe alle former for IKT-kriminalitet, samtidig som det må bygges et fremtidig kompetent rekrutteringsgrunnlag.

På denne bakgrunn fremmer komiteens flertall, medlemmene fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti, følgende forslag:

«Stortinget ber regjeringen legge fram en plan som synliggjør politiets arbeid med IKT-kriminalitet og hvordan dette skal finansieres.»

Flertallet viser til at det er bra med en satsing på et eget nasjonalt senter for å forebygge og bekjempe IKT-kriminalitet. Flertallet vil understreke at bevilgningene til et slikt senter ikke skal tas fra bevilgningene til politidistriktene. Da vil verken kriminaliteten eller beredskapen høynes.

3. Forslag fra mindretall

Forslag fra Arbeiderpartiet og Sosialistisk Venstreparti:

Forslag 1

Stortinget ber regjeringen sørge for at staten årlig kartlegger den digitale sikkerhetskulturen i befolkningen. Kunnskapen må danne grunnlag for myndighetenes beslutningsgrunnlag og for råd og anbefalinger som gis til befolkningen og små virksomheter for å redusere digital sårbarhet.

Forslag 2

Stortinget ber regjeringen fremskaffe en oversikt over status, utfordringer og eventuelle farer for personvernet og komme tilbake til Stortinget på egnet måte.

Forslag 3

Stortinget ber regjeringen sørge for at IKT-sikkerhet integreres som en obligatorisk del i alle IKT-studieprogrammer på bachelornivå.

Forslag 4

Stortinget ber regjeringen sørge for at systemer som håndterer data knyttet til nasjonale sikkerhetsinteresser, driftes fra Norge.

Forslag 5

Stortinget ber regjeringen komme tilbake med forslag om en opptrappingsplan for Nasjonal sikkerhetsmyndighet og e-tjenesten for å sikre mer ressurser, økt kompetanse og bedre samordning mellom aktørene i cyberforsvaret.

Forslag fra Senterpartiet og Sosialistisk Venstreparti:

Forslag 6

Stortinget ber regjeringen sørge for at svært sensitive personopplysninger blir lagret og driftet i Norge.

Forslag 7

Stortinget ber regjeringen sørge for at informasjon knyttet til nasjonale sikkerhetsinteresser blir lagret og driftet i Norge.

Forslag 8

Stortinget ber regjeringen klargjøre hvorvidt lov om etterretningstjenesten § 3 gir hjemmel til å samle inn metadata og til å operere innenfor kommunikasjonsetterretning i luftsnittet.

Forslag 9

Stortinget ber regjeringen utrede og komme tilbake til Stortinget med forslag om vilkår for metadatainnsamling, lagringslengde og hvordan dataene skal brukes etter lov om etterretningstjenesten, herunder en ordning med godkjenning av domstol for innsamling og lagring av slike metadata, og godkjennelse for bruk.

Forslag fra Sosialistisk Venstreparti:

Forslag 10

Stortinget ber regjeringen sette ned et utvalg som skal utrede tiltak for å styrke vår digitale forsvarsevne uten å åpne for masseovervåkning av norske borgere.

4. Komiteens tilråding

Komiteens tilråding I–XI fremmes av komiteens medlemmer fra Arbeiderpartiet, Senterpartiet og Sosialistisk Venstreparti.

Komiteens tilråding XII fremmes av en samlet komité.

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

vedtak:

I

Stortinget ber regjeringen sørge for at relevante ingeniør- og teknologiutdanninger har kurs i IKT-sikkerhet.

II

Stortinget ber regjeringen utrede og foreslå konkrete tiltak som sikrer nødvendig kompetanse om IKT-sikkerhet hos alle kandidater med IKT-utdanning.

III

Stortinget ber regjeringen komme tilbake til Stortinget med forslag til klarere regler og rammer for sikkerhets- og sårbarhetsvurderinger i virksomheter som forvalter kritisk infrastruktur, men som faller utenfor sikkerhetslovens virkeområde.

IV

Stortinget ber regjeringen innføre felles nasjonale krav til risiko- og sårbarhetsvurderinger av IKT-sikkerhet i virksomheter med kritisk infrastruktur.

V

Stortinget ber regjeringen sørge for at det stimuleres til bedre etter- og videreutdanningstilbud på fagskoler, universiteter og høyskoler innen IKT- og datasikkerhet.

VI

Stortinget ber regjeringen sørge for at digitalisering og IKT-sikkerhet prioriteres i neste Langtidsplan for forsking og høyere utdanning.

VII

Stortinget ber regjeringen sørge for at alle elever gjennom grunnskolen får erfaring med programmering, og at dette starter allerede på barneskolen.

VIII

Stortinget ber regjeringen igangsette konkrete tiltak for å øke rekrutteringen av PhD-kandidater som kan sikkerhetsklareres.

IX

Stortinget ber regjeringen sørge for at ved en eventuell lagring av data i annet land må risiko- og sårbarhetsvurderingen også omfatte lovverk og sikkerhetssituasjon i landet der dataene lagres.

X

Stortinget ber regjeringen fremme en sak hvor det foreslås tiltak for hvordan man kan redusere nasjonal sårbarhet og sikre nasjonal kontroll over kritisk IKT-infrastruktur. Regjeringen bes videre se på ulike kontrollrutiner som må iverksettes ved utsetting av informasjonshåndtering til utenlandske selskaper eller tredjeparter.

XI

Stortinget ber regjeringen legge fram en plan som synliggjør politiets arbeid med IKT-kriminalitet og hvordan dette skal finansieres.

XII

Meld. St. 38 (2016–2017) – IKT-sikkerhet. Et felles ansvar – vedlegges protokollen.

Oslo, i justiskomiteen, den 20. mars 2018

Lene Vågslid

leder og ordfører

Svanemerketrykksak, 2041 0654 Trykk og layout: Stortingets grafiske seksjon