

Stortingets Justiskomite  
Stortinget  
0026 Oslo

Oslo, 30. oktober 2017

## Høringsinnspill fra Abelia: Prop.1S 2017-2018: Statsbudsjettet

Abelia er NHOs landsforening for kunnskaps- og teknologibedrifter, og organiserer mer enn 2.100 virksomheter med over 48.000 årsverk. Vår visjon er "Drivkraft for kunnskapssamfunnet". Abelia viser til anmodning om høring til komiteen, og vedlegger her vårt skriftlige innspill. For en digital versjon av dette høringsbrev [https://www.abelia.no/politikk/statsbudsjettet-2018/horinger/horingsinnspill\\_justis/](https://www.abelia.no/politikk/statsbudsjettet-2018/horinger/horingsinnspill_justis/)

### Flere arbeidsplasser i privat sektor

Abelia mener den viktigste politiske oppgaven framover er å bidra i utviklingen av et kunnskapsbasert, innovativt og globalt konkurransedyktig næringsliv. Dette vil sikre framtidig velferd, sysselsetting og verdiskaping. For å få til dette må vi investere i kunnskap, i barnehage og skole, læring gjennom hele livet og forskning.

En kraftfull satsing på utvikling og anvendelse av digitale løsninger er avgjørende i både privat og offentlig sektor. Offentlige aktører som utløser teknologiutvikling og innovasjon bidrar samtidig både til bedre og billigere tjenester for innbyggerne og til utvikling av et næringsliv som kan betale fremtidens skatter.

Abelia ber Stortinget om å:

- Etablere ytterligere 750 nye studieplasser innen IT så det totalt blir 1.250 (estimert tilleggskostnad: 429 millioner kroner årlig)<sup>1</sup>. Noen av disse må øremerkes IT-sikkerhet.
- Be regjeringen om å lage en kartlegging av fremtidige behov for IT-arbeidskraft i et digitalt samfunn, og utarbeide en nasjonal strategi for å styrke den digitale kompetansen på sentrale områder.
- Opprette et felles nasjonalt situasjonsrom for angrep på nasjonal kritisk infrastruktur slik at angrep kan håndteres samlet og ut fra en felles situasjonsforståelse.
- Etterlyse regjeringens varslede nasjonale kompetansestrategi for IT-sikkerhet.
- Etterlyse regjeringens varslede nasjonale strategi for IKT-sikkerhet og den varslede handlingsplanen.
- Legge til rette for opprettelse av et forum for IKT-sikkerhet for samarbeid mellom myndigheter, næringsliv, akademia og interesseorganisasjoner.

### 1.0 Kompetansemangel er en sikkerhetstrussel

<sup>1</sup> Provenyeffekten av å etablere 1.000 nye varige fireårige studieplasser i finansieringskategori D er 572 millioner kroner årlig ved fullt utbygget studieløp i 2021, ifølge Kunnskapsdepartementets budsjettberegninger, altså 572 000 per studieplass. <http://www.statsbudsjettet.no/Statsbudsjettet-2017/Budsjettsporsmal/?parti=arbeiderpartiet&query=&sort=desc>



Vi trenger en sterkere satsning på IT-sikkerhets kompetanse. Regjeringen la i år for første gang fram en melding om IT-sikkerhet, det er en god begynnelse. Det har i løpet av de siste par årene også kommet en rekke meldinger og rapporter som berører IT-sikkerhet. Deriblant Lysneutvalget, Traavikutvalget, Datakrimstrategien og "Risiko i et trygt samfunn". Samtlige rapporter og meldinger har det til felles at mangel på IT-kompetanse framheves og da mangel på IT-sikkerhetskompetanse i særdeleshet. Den manglende IT-kompetansen generelt og IT-sikkerhetskompetansen spesielt, svekker justissektoren, den svekker den almene tilliten til vår rettsoppfatning og den gjør oss som nasjon mer sårbare. IT-sikkerhetskompetanse er derfor også et anliggende for Justiskomiteen. Når politiet har for lav kompetanse og kapasitet til å etterforske, mister de berørte troen på at det er bryet verd å anmelde, de kriminelle vil føle de har større spillerom og vi blir mer sårbare.

Abelia ser fram til den lenge varslede nasjonale kompetansestrategien for IKT-sikkerhet fra regjeringen. Vi er glad for at det er kommet flere studieplasser blant annet til CCIS på Gjøvik. Men det er ikke nok. I et notat fra NIFU skrevet på oppdrag for Justis- og beredskapsdepartementet framskrives tilbuds- og etterspørselsiden til år 2030 med en mangel på vel 4.000 personer med IKT-sikkerhetskompetanse. Abelia er imidlertid bekymret over at det på årets budsjett ikke er avsatt midler til tiltak for den varslede nasjonale kompetansestrategien for IKT-sikkerhet.

Det siste året har det vært flere saker hvor uvedkommende har hatt tilgang til sensitive data om nordmenn og norske selskaper gjennom IT-kontrakter hos blant annet Helse Sør-Øst og Direktoratet for nødkommunikasjon. Det er fortsatt uklart om informasjonen er blitt misbrukt, men dette er alvorlige saker som fortjener oppmerksomhet for å hindre at det skal skje igjen. Det er imidlertid svært alvorlig hvis det på bakgrunn av disse sakene utvikler seg en ubegrunnet frykt i offentlig sektor. Mangel på kunnskap om IT-sikkerhet kan medføre at man vegrer seg for å ta i bruk nettsky, frykter samarbeid med internasjonale selskaper, eller utsetter innovative løsninger fordi "noe kan skje". En slik frykt vil hemme og forsinke den digitaliserings- og effektiviseringstakten vi trenger i offentlig sektor. Løsningen på utfordringen med utkontraktering av IT-prosjekter er ikke å stille krav til at selskaper og ansatte skal være norske, holde utenlandske aktører ute og drive all utvikling i offentlig regi. Svaret må være å sørge for at prosjektene blir sikrere. Det skjer blant annet når det offentlige opptrer som gode bestillere, hvilket krever kompetanse utover dagens nivå.

Abelia ber Stortinget om å:

- Etablere ytterligere 750 nye studieplasser innen IT så det totalt blir 1.250 (estimert tilleggskostnad: 429 millioner kroner årlig)<sup>2</sup>. Noen av disse må øremerkes IT-sikkerhet.
- Be regjeringen om å lage en kartlegging av fremtidige behov for IT-arbeidskraft i et digitalt samfunn, og utarbeide en nasjonal strategi for å styrke den digitale kompetansen på sentrale områder.
- Etterlyse regjeringens varslede nasjonale kompetansestrategi for IT-sikkerhet.

## 2.0 Cybercrime

Mangelen på IT-sikkerhetskompetanse har to alvorlige konsekvenser; vi blir et lettere mål for kriminelle og den generelle digitaliseringstakten kan bli svekket.

---

<sup>2</sup> Provenyeffekten av å etablere 1.000 nye varige fireårige studieplasser i finansieringskategori D er 572 millioner kroner årlig ved fullt utbygget studieløp i 2021, ifølge Kunnskapsdepartementets budsjettberegninger, altså 572 000 per studieplass. <http://www.statsbudsjettet.no/Statsbudsjettet-2017/Budsjettsporsmal/?parti=arbeiderpartiet&query=&sort=desc>



Den store kriminalitets- og sikkerhetsundersøkelsen i næringslivet viser i år at norske selskaper har mistillit til politiets innsats og evne til å håndtere kriminalitet<sup>3</sup>. Hvert tiende norske selskap anmelder ikke kriminalitet fordi 69 prosent av selskapene på forhånd tror sakene blir henlagt. Hvert femte selskap sier rett ut at de ikke anmelder på grunn av «manglende tillit til politiets kompetanse». Dette gjør ikke kun at kriminelle får unødvendig stort spillerom, men at politiet ikke får dannet seg et totalbilde av kriminalitetskomplekset. Manglende anmeldelser og henlagte saker der det er uklart hvem som har ansvaret for å gripe fatt i og sammenstille den informasjonen vi faktisk har, gjør oss sårbare. KRISINO rapporten stiller også spørsmål ved om ressursøkningen i politiet har hatt den ønskede effekten når antall årsverk i politiet har økt med 17% fra 2011 til 2016, mens oppklaringsprosenten er blitt dårligere.

Selv om disse tallene gjelder kriminalitet generelt vet vi fra Mørketallsundersøkelsen i 2016<sup>4</sup> at bildet er nokså likt for datainnbrudd og uønskede hendelser. Over en fjerdedel av norske virksomheter – 412 av 1500, eller 27% – har opplevd uønskede sikkerhetshendelser det siste året. Virksomhetene forteller at dette fører til produktivitetstap i 4 av 10 tilfeller (i form av tapte arbeidstimer), men kun 2 av 10 oppgir at de har hatt kostnader som følge av slike hendelser. Dette viser trolig at virksomhetene mangler oversikt over hva sikkerhetshendelsene koster dem, eller undervurderer disse kostnadene. Kun 9% av virksomhetene som utsettes for angrep tar saken videre til politiet. Det tilsier at det skjuler seg betydelige mørketall, og for kriminelle nettverk er denne typen angrep mot norske virksomheter i praksis straffefrie.

I sin rapport Digital Sikkerhet 2017<sup>5</sup> påpeker Telenor at mangelen på en sammenstilling av et helhetsbilde gjør seg gjeldende også når det gjelder cyberkriminalitet og angrep på nasjonal kritisk infrastruktur. Selskapet mener det er behov for at det opprettes et felles nasjonalt situasjonsrom slik at det kan skapes en felles situasjonsforståelse og en samlet evne til å håndtere slike hendelser. Telenor påpeker også at det i forhold til angrep på kritisk nasjonal infrastruktur er uklart hvem som har det totale overordnede ansvaret for IKT-sikkerhet. Det er ingen enkelt myndighetsaktør som har ansvaret for og leder hendelser i cyberspace i dag. Abelia mener dette er innspill det er verdt å lytte til og å diskutere. Trusselaktører som ønsker å sette nasjonale samfunnsfunksjoner ut av spill angriper ikke i henhold til sektorprinsippet, da bør heller ikke vår evne til å svare kun være basert på dette prinsippet. Samfunnets avhengighet av IKT gjør det nødvendig med samarbeid på tvers av landegrensene, mellom offentlige og private aktører og mellom sivile og militære.

Med bakgrunn i sikkerhetsutfordringene beskrevet over ser Abelia fram til regjeringens varslede nasjonale strategi for IKT-sikkerhet som også skal inkludere en handlingsplan. Vi er imidlertid bekymret over at det ikke er drøftet behov for å sette av midler til eventuelle tiltak i handlingsplanen.

Abelia ber Stortinget om å:

- Opprette et felles nasjonalt situasjonsrom for angrep på nasjonal kritisk infrastruktur slik at angrep kan håndteres samlet og ut fra en felles situasjonsforståelse.
- Etterlyse regjeringens varslede nasjonale strategi for IKT-sikkerhet og den varslede handlingsplanen.
- Legge til rette for opprettelse av et forum for IKT-sikkerhet for samarbeid mellom myndigheter, næringsliv, akademia og interesseorganisasjoner.

---

<sup>3</sup> [https://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/Krisino/KRISINO%20rapport%202017\\_5\\_final.pdf](https://www.nsr-org.no/getfile.php/Dokumenter/NSR%20publikasjoner/Krisino/KRISINO%20rapport%202017_5_final.pdf)

<sup>4</sup> [https://www.nsr-org.no/getfile.php/Bilder/M%C3%B8rketallsunders%C3%B8kelsen/morketallsundersokelsen\\_2016.pdf](https://www.nsr-org.no/getfile.php/Bilder/M%C3%B8rketallsunders%C3%B8kelsen/morketallsundersokelsen_2016.pdf)

<sup>5</sup> [https://www.telenor.no/om/digital-sikkerhet/nasjonalt\\_ansvar.jsp](https://www.telenor.no/om/digital-sikkerhet/nasjonalt_ansvar.jsp)



Abelia ser fram til å diskutere disse punktene og tilliggende sikkerhetstemaer ytterligere når komiteen skal behandle Meld. St. 38 (2016–2017) "IT-sikkerhet – et felles ansvar".

Med vennlig hilsen,

Hilde Widerøe Wibe  
Næringspolitisk direktør

Christine Korme  
Direktør for digitalisering og fornying