



DET KONGELIGE  
SAMFERDSELSDEPARTEMENT

Justis- og beredskapsdepartementet  
Postboks 8005 Dep  
0030 OSLO

Deres ref

Vår ref

Dato

15/4195- SOA/HEN

18.03.2016

### Høring NOU 2015:13 Digital sårbarhet - sikkert samfunn

Samferdselsdepartementet viser til Justis- og beredskapsdepartementets høring av NOU 2015:13 Det digitale sårbarhetsutvalgets utredning: «*Digital sårbarhet – sikkert samfunn*» ("Utvalget"). Fristen for høringsinnspill er 15. mars 2016. Departementet har hatt kontakt med Luftfartstilsynet, Avinor AS, Jernbaneverket AS, Statens jernbanetilsyn, Vegdirektoratet, Kystverkets hovedkontor og NSB AS som en del av grunnlaget for departementets egen høringsuttalelse. Etatene er i tillegg oppfordret til å levere egne mer utfyllende høringsuttalelser.

#### 1. SAMFERDSELSDEPARTEMENTET HAR FØLGENDE INNSPILL TIL HØRINGEN:

NOU 2015:13 tar for seg utfordringer knyttet til digitalisering av mange av de mest kritiske kjernepunktene og systemene i samfunnet vårt. Rapporten fremsetter relevante problemstillinger og i mange tilfeller gode forslag til løsninger av disse. Digitaliseringen av samferdselssektoren bidrar til mer effektive og bedre tjenester for brukerne. Bruk av elektronisk kommunikasjon og systemer er kjent for samferdselssektoren helt siden de første telegraflinjene ble etablert i forbindelse med togstyring. Digitale løsninger bidrar i stor grad til å gjøre tjenestene sikrere. Men, som utvalgets rapport viser, så kan den økte avhengigheten av løsningene også skape nye sårbarheter som må vurderes.

Samferdselsdepartementet har ingen konkrete kommentarer til tiltak og anbefalinger knyttet til sårbarhet ved bruk av GNSS til PNT-formål utover at vi slutter oss til anbefalingen om at myndighetsansvaret for norsk romvirksomhet bør tydeliggjøres. Etter vårt syn kan det være

gunstig at en myndighet tilføres kompetanse til å gjøre tverrsektorielle vurderinger av sårbarhet ved bruk av PNT-formål, og hvordan disse eventuelt kan reduseres.

## 2. EKOMSEKTOREN

Innledningsvis viser Samferdselsdepartementet til at Stortinget snart vil få overlevert en nasjonal plan for elektronisk kommunikasjon (ekomplanen). Planen er en selvstendig del av regjeringens melding til Stortinget om *Digital agenda for Norge – IKT for en enklere hverdag og økt produktivitet*. Enkelte av forholdene behandlet i Lysneutvalgets rapport vil bli nærmere omtalt i Ekomplanen.

De sårbarhetene i ekomsektoren som Lysneutvalget har påpekt sammenfaller i stor grad med de vurderinger som blant annet ekommyndigheten har gjort seg. Flere av tiltakene som er foreslått virker fornuftig og egnet.. Vi viser også til egen høringsuttalelse fra Nasjonal kommunikasjonsmyndighet.

Departementet vil likevel komme med enkelte bemerkninger på ekomområdet. Lysneutvalget har fremhevet at Telenors transportnett er bærer av svært mye av den totale elektroniske kommunikasjonen i Norge, og at avhengigheten av én aktør er en sårbarhet som må vurderes. Departementet er enig i dette. Flere alternative føringsveier og kjernesystemer vil ikke bare redusere sårbarheten, men også kunne gi bedre konkurranse i markedet. Dessuten vil den enkelte bruker kunne oppleve en bedre brukerutnyttelse og bedre og mer robuste ekomtjenester. Departementet vil derfor vurdere virkemidler for hvordan det kan legges til rette for landsdekkende og reelle alternativer til Telenors kjernenett. Det vises til Ekomplanen og nærmere omtale der.

Robuste og sikre ekomnett og -tjenester for å møte samfunnets økende krav til tilgjengelige tjenester, er avhengig av at både ekomtilbyderne og samarbeidende aktører har gode og robuste systemer. I dag er ofte kritiske systemer gjensidig avhengige av hverandre. Lysneutvalget viser blant annet til at en av de viktigste årsakene til utfall i ekomnett er strømbrudd. Ett av tiltakene det ble vist til i etterkant av stormen Dagmar var etablering av reservestrøm i landmobile nett for å sikre kraft til basestasjoner i en viss tid etter strømbrudd. Det er store variasjoner i graden av robusthet hos de ulike kraftleverandørene, og departementet mener sårbarheten som ligger i kraftnettene og som påvirker ekomnettene, må reduseres. Samfunnet er tjent med å ha et mer robust kraftnett for fremtiden. Det vil ikke bare komme ekomnett og -tjenester til gode, men hele samfunnet som sådan.

Lysneutvalget etterlyser videre en mer aktiv veiledning fra myndigheten overfor tilbydere og andre om innholdet i rettslige standarder. Departementet viser til at en av utfordringene med bruk av rettslige standarder er å sikre tilstrekkelig forutsigbarhet for ekomtilbyderne i et regelverk som er lagt opp til å være dynamisk og stadig i endring. En økende bruk av rettslige standarder vil stille skjerpede krav til ekommyndigheten samtidig som også samarbeidet mellom ekomtilbyderne og ekommyndighetene må styrkes.

Utvalget peker på at det er en generell trend i mange sektorer med en økende bruk av eksterne leverandører. Drift og utstyr og tjenester plasseres i økende grad i eksterne datasentre. Dette kan utgjøre en sårbarhet som må vurderes og som gjelder mange bransjer og sektorer. Departementet mener det må stilles relevante krav til både myndigheter og private aktører ved bruk av eksterne leverandører. Aktører som velger å benytte eksterne leverandører og sette ut

drift til eksterne, må som et generelt krav tilegne seg økende bevissthet rundt de mulige følgene av outsourcing og hvilken risiko og usikkerhet som kan ligge i et slikt valgt.

Utvalget drøfter også kryptering og betydningen for det som omtales som digitalt grensevern. Departementet støtter utvalgets vurderinger. Kryptering er nødvendig for å ivareta et tilstrekkelig kommunikasjonsvern for brukerne av elektronisk kommunikasjon.

### **3. TRANSPORTSEKTOREN**

#### **3.1 Vegtransport**

Statens vegvesen leverer en utfyllende høringsuttalelse. Vi vil likevel nevne et par sentrale punkter i høringsuttalelsen som vi mener har betydning for flere sektorer. Et viktig premiss for informasjonssikkerhetsarbeidet er at virksomheter har god oversikt over behov for data i virksomhetsprosessene sine. Vegvesenet etterlyser et sterkere fokus på informasjonsforvaltning enn det som fremgår av Lysneutvalgets rapport, i tillegg til at det bør utarbeides bedre veiledninger og kompetansedeling for effektivt arbeid med verddivurdering av data og risikovurderinger av IKT-løsninger. Videre har Vegvesenet pekt på at rapporten ikke fokuserer like mye på digital sårbarhet for enkeltpersoner som for offentlige virksomheter og næringsvirksomhet, dette selv om det flere steder i rapporten drøftes problemstillinger knyttet til enkeltpersoners digitale sårbarhet.

NOUen gir et godt bilde av den omfattende bruken av IKT-løsninger som eksisterer på tvers i transportsektoren og risikoutfordringer knyttet til dette. Det vises videre til at de ulike transportsektorene ikke har kommet like langt på alle områder, men har mange felles problemstillinger knyttet til digital sårbarhet og et potensial for å lære av hverandre. Den videre utviklingen innen digitalisering vil trolig bare forsterke dette. Rapportens anbefaling om tiltak, samarbeid og kompetansedeling på tvers i transportsektoren støttes derfor av Vegvesenet.

Når det gjelder tverrsektorielle sårbarhetsreducerende tiltak bemerker Vegvesenet at etatens samfunnsansvar for veg og kjøretøy krever at det innad i etaten bygges den nødvendige kompetanse og iverksettes de nødvendige tiltak for å bidra til å redusere digital sårbarhet og for å oppnå et sikkert samfunn. Vegvesenet er derfor positive til de forslag rapporten har til fellesarenaer for erfaringsutveksling samt nasjonale strategier og tiltak.

#### **3.2 Kysttransport**

Lysneutvalget kommer med flere konkrete vurderinger og tiltak for å redusere den digitale sårbarheten innen transportsektoren og innen sjøtransport spesielt. Tiltakene vil kunne være ressurskrevende å gjennomføre.

Digital sårbarhet er ikke vurdert opp mot andre sårbarheter i maritim sektor. Dette gjør det vanskelig å vurdere hvor stor risikoen er relativt til risiko på andre områder, og hvor stor ressursinnsatsen for å redusere digital sårbarhet bør være sammenlignet med innsatsen rettet mot andre sårbarheter. Departementet mener at før man eventuelt går videre med de anbefalte tiltakene, bør det gjøres en nærmere nytte-kostnadsanalyse av dem, for å kunne vurdere dem opp mot andre risiko- og sårbarhetsreducerende tiltak innen sjøtransporten.

Vedrørende Lysneutvalgets anbefaling om å tillegge Kystverket ansvar for å ha en helhetsoversikt over IKT-sikkerheten i maritime verdikjeder, mener Samferdselsdepartementet at det er nødvendig med en mer omfattende vurdering av om, og eventuelt hvilken etat som skal ha et slikt ansvar.

### **3.3 Luftfart**

Som en innledende kommentar vil Luftfartstilsynet understreke viktigheten av å ha tilstrekkelig kompetanse og kapasitet til å føre tilsyn med digitale systemer med relevans for flsikkerheten. Dette er en kompetanse som Luftfartstilsynet besitter i begrenset omfang i dag, samt at tilsynsvirksomheten forventes å øke, og bør økes merkbart i årene framover. Kapittelet om luftfart framstår, etter vår vurdering, noe upresist og kunne tjent på en mer tydelig struktur. En beskrivelse av hvordan lufttrafikkjenesten er oppbygd, mangler. Slik det er beskrevet i dokumentet kan det oppfattes som at det kun er fra kontrollsentraler at det utøves lufttrafikkjenester. Det er etablert tårntjenester på alle lufthavner, innflygingskontroller er enten etablert lokalt på lufthavna, eller sentralisert på større lufthavner eller kontrollsentraler. Kontrollsentraler har ansvar for lufttrafikkjenesten i øvre deler av luftrommet (underveisfasen). I tillegg burde det vært beskrevet noe om Gardermoen sin viktighet for luftfartsnettverket i Norge.

Beskrivelsene av SES og SESAR burde tydeligere vise de utfordringene som ligger i at fremtidig teknologi i større grad vil være basert på åpen arkitektur som sannsynligvis vil være mere utsatt for datainntrenging og sabotasje. Det er ikke tydelig i rapporten at dagens ATM-systemer i stor grad er lukkede systemer med beskyttede grensesnitt, noe som også gir større beskyttelse mot ekstern inntrenging i kritiske systemer.

Teknologisk utvikling går i retning av økt grad av standardiserte, åpne løsninger og satellittsystemer vil benyttes som tidsreferanse for synkronisering av systemer for flykontroll (Air Traffic Management, ATM) og flybåren avionikk. Det er derfor viktig med økt oppmerksomhet på IKT-sikkerhet, men også viktig å ha redundante systemer, der det ikke er avhengigheter mellom systemene (eksempelvis separat tidsreferanse). Dette kan være et argument for å investere i eLoran, for å ha et alternativ til GPS-tidsreferanse.

Luftfartstilsynet gjør i sin høringsuttalelse oppmerksom på at tilhørende flsikringstjenester er blant annet lufttrafikkjenester (kontrollsentraler, kontrolltårn og innflygingskontroll) og flynavigasjonstjenester.

Med hilsen

Jørn Ringlund (e.f.)  
avdelingsdirektør

Silje Owren Aarum  
rådgiver

*Dokumentet er elektronisk signert og har derfor ikke håndskrevne signaturer.*