DET KONGELIGE
JUSTIS- OG BEREDSKAPSDEPARTEMENT
Statsråden

Stortinget
v/Kontroll- og konstitusjonskomiteen
0026 OSLO

Deres ref.	Vår ref.	Dato
	12/7113 - ROB	13.11.2012

Spørsmål fra Kontroll- og konstitusjonskomiteen i Stortinget vedrørende utbyggingen av mobilnett og sikkerhetsgraderte anskaffelser

Jeg viser til brev fra Kontroll- og konstitusjonskomiteen av 26.10.2012 vedrørende utbyggingen av mobilnett og sikkerhetsgraderte anskaffelser. Jeg viser også til skriftlige svar som ble gitt av Samferdselsministeren 26.09.2012 og Forsvarsministeren 15.10.2012 til Stortinget om samme tema.

1. Hvilke konkrete rutiner har Justis- og beredskapsdepartementet og underliggende organer for vurdering av sikkerhetsgraderte anskaffelser i sivil sektor?
Forsvarsdepartementet har forvaltningsansvaret for sikkerhetsloven. Nasjonal sikkerhetsmyndighet (NSM) har ansvar for å koordinere de forebyggende sikkerhetstiltak og kontrollere sikkerhetstilstanden i henhold til loven. NSM er administrativt underlagt Forsvarsdepartementet, med delt rapporterings- og ansvarslinje til Justis- og beredskapsdepartementet for sivil sektor og Forsvarsdepartementet for forsvarssektoren.

En sikkerhetsgradert anskaffelse er en anskaffelse foretatt av anskaffelsesmyndighet som innebærer at leverandøren av varen eller tjenesten vil kunne få tilgang til skjermingsverdig informasjon eller objekt, eller som innebærer at anskaffelsen må sikkerhetsgraderes av andre årsaker, jf. sikkerhetsloven § 3 første ledd nr. 17.

Kravene til sikkerhetsgraderte anskaffelser er de samme for sivil og militær sektor. Rutinene på dette området tar utgangspunkt i at det er *anskaffelsesmyndigheten* som vurderer behovet for å sikkerhetsgradere en anskaffelse. Dersom *bruker* er en annen

Postadresse: Postboks 8005 Dep, 0030 Oslo
Kontoradresse: Gullhaug Torg 4a Telefon: 22 24 51 00 Telefaks: 22 24 95 33
Org. nr.: 972 417 831

enn anskaffelsesmyndigheten, er det førstnevnte som skal foreta vurderingen, jf. forskrift om sikkerhetsgraderte anskaffelser § 2-1.

Om det dreier seg om en sikkerhetsgradert anskaffelse skal det inngås en sikkerhetsavtale mellom anskaffelsesmyndigheten og leverandøren. Denne fastsetter nærmere detaljer om ansvar og plikter av betydning for sikkerheten. Slik sikkerhetsavtale kan også, om NSM bestemmer det, inngås når det er tilgang til skjermingsverdig objekt eller andre grunner som er årsak til at anskaffelsen sikkerhetsgraderes, jf. lovens § 27 og forskrift om sikkerhetsgraderte anskaffelser § 2-5.

Ved sikkerhetsgraderte anskaffelser som innebærer at en leverandør får tilgang til informasjon klassifisert som KONFIDENSIELT, er det et krav om *leverandørklarering* for aktuell sikkerhetsgrad. Leverandørklarering kan også kreves når andre grunner gjør dette nødvendig, jf. lovens § 28 og forskrift om sikkerhetsgraderte anskaffelser kap. 3.

Anskaffelsesmyndigheten fremmer anmodning om leverandørklarering til NSM. NSM treffer avgjørelse om leverandørens sikkerhetsmessige skikkethet, på bakgrunn av en vurdering av innhentede opplysninger om leverandøren.

Hvis en virksomhet underlagt sikkerhetsloven skal foreta en anskaffelse fra en utenlandsk leverandør, plikter virksomheten å orientere NSM dersom det er mulig at leverandøren vil bli brukt i en sikkerhetsgradert anskaffelse, jf. forskrift om sikkerhetsgraderte anskaffelser § 4-2.

Med bakgrunn i en slik orientering kan NSM innhente nødvendig informasjon om hvorvidt leverandøren innehar nødvendig leverandørklarering gitt av hjemlandet. Dette foretas rutinemessig av NSM.

Ved bruk av utenlandsk leverandør i en sikkerhetsgradert anskaffelse, kan det bare inngås sikkerhetsavtale etter godkjenning fra NSM. Sikkerhetsgradert informasjon kan ikke utleveres til, eller tilvirkes av, leverandøren før NSM har gitt sitt samtykke. Alle henvendelser vedrørende sikkerheten hos utenlandsk leverandør skal skje via NSM.

Det er en forutsetning for bruk av utenlandsk leverandør ved sikkerhetsgraderte anskaffelser at det foreligger en sikkerhetsavtale på nasjonalt nivå mellom landene. Der en sikkerhetsgradert anskaffelse gjennomføres med et norsk firma som benytter utenlandske underleverandører, stilles de samme krav til underleverandør som til hovedleverandør.

2. Kan statsråden bekrefte at Huaweis rolle i utbyggingen av norske mobilnett ikke er nærmere vurdert av departementet og/eller underliggende organer, herunder i forbindelse med kravet om inngåelse av sikkerhetsavtale med utenlandske leverandører, jf. sikkerhetsloven § 27? Hvis ja – hvilke tanker gjør

statsråden seg om den betydelige skepsisen til Huaweis rolle i utbyggingen av mobilnett i land som USA, Australia og Canada?

NSM og Politiets sikkerhetstjeneste(PST) hadde dialog med Telenor i desember 2009. Det ble i denne forbindelse uttrykt bekymring knyttet til ulike aspekter ved sikkerheten i mobilnettverket. Videre ble det formidlet at Telenor må gjøre de nødvendige risikovurderinger knyttet til avtaleinngåelse med utenlandske leverandører av varer og tjenester til sin kritiske infrastruktur. Det ble også gitt generell informasjon om forebyggende sikkerhet.

I 2009 vurderte NSM at Telenors anskaffelse av infrastruktur ikke var sikkerhetsgradert. Denne vurderingen ble gjort på bakgrunn av dagjeldende regelverk og situasjon.

I 2010 vurderte NSM hvorvidt sikkerhetsloven og lov om elektronisk kommunikasjon hadde mekanismer for å redusere risiko som beskrevet. Det ble innhentet vurderinger også fra Post- og teletilsynet i denne prosessen. NSMs daværende konklusjon var at det forelå en risiko, men at ingen av regelverkene var anvendelige. Dette er en problemstilling jeg vil se nærmere på, blant annet i forbindelse med en gjennomgang av sikkerhetsloven. Det er viktig at vi har et regelverk som ivaretar myndighetenes behov for å komme med inngripen.

I 2010 hadde PST et møte med Netcom der etterretningstrusselen knyttet til utenlandske leveranser til norsk kritisk infrastruktur ble lagt frem.

Selv om andre lands myndigheters vurderinger har betydning, må nasjonale vurderinger gjøres på bakgrunn av norsk regelverk og hensynet til norske interesser. Den generelle problemstillingen vi må adressere er hvilke mekanismer vi skal ha overfor leverandører til kritisk infrastruktur når disse er fra land vi ikke har et nært sikkerhetsmessig samarbeid med. Dette er en problemstilling som jeg er særlig opptatt av at blir drøftet i den pågående gjennomgangen av sikkerhetsloven.

3. Er statsråden tilfreds med den tilsynelatende praksisen med at private selskaper delegeres myndighet til selv å vurdere om en anskaffelse skal vurderes som sikkerhetsgradert eller ikke?

Alle må erkjenne sitt ansvar for god sikkerhet, også næringslivet selv. God sikkerhet begynner med den enkelte. Sviktende sikkerhet i kritisk infrastruktur rammer ikke bare samfunnet. Det rammer i særlig grad virksomhetene selv, både i funksjonsdyktighet og i omdømme. Et nært samarbeid mellom myndigheter og næringsliv også på områder som ikke er strengt lovregulert er derfor svært viktig.

Sikkerhetsloven gjelder i utgangspunktet for forvaltningsorganer. Det påhviler da det aktuelle forvaltningsorgan å vurdere hvorvidt det er behov for å sikkerhetsgradere en anskaffelse, eller deler av en anskaffelse.

Det er gitt anledning til å bestemme at loven helt eller delvis skal gjelde for ethvert annet rettssubjekt, jf. sikkerhetsloven § 2 tredje ledd. Slikt vedtak er fattet for en rekke private rettssubjekter, herunder Telenor ASA.

Etter ordlyden i loven er det bare *forvaltningsorganer* som kan gjennomføre sikkerhetsgraderte anskaffelser, jf. lovens § 3 første ledd nr. 17, jf. nr. 16, samt virkeområdebestemmelsen i § 2 andre ledd. Omtalen av sikkerhetsgraderte anskaffelser i lovens forarbeider synes også å underbygge dette, jf. Ot.prp. nr. 21 (2007-2008) kap. 10. Jeg legger imidlertid til grunn at det ikke har vært lovgivers intensjon å ekskludere private rettssubjekter underlagt sikkerhetsloven iht. særskilt vedtak, jf. § 2.

Forsvarsdepartementet fattet vedtak 7. februar 2005 om at Telenor ASA skal omfattes av sikkerhetsloven. Vedtaket er begrunnet i Telenors befatning med sikkerhetsgradert informasjon og deres eierskap til skjermingsverdige objekter. Vedtaket er ikke begrenset til deler av loven.

Intensjonen bak regelverket, å etablere et helhetlig beskyttelsesregime for informasjon og objekter av vital nasjonal betydning, tilsier at det ikke bør være avgjørende hvorvidt anskaffende virksomhet er offentlig eller privat. En bør heller ikke isolere sikkerhetsspørsmålet til hvorvidt en bestemt leverandør kan representere en risiko overfor en bestemt sektor eller bransje.

Imidlertid er alle virksomheter som sikkerhetsloven gjelder for underlagt NSMs tilsyn, herunder hvorvidt vurderinger er forsvarlige iht. regelverket. NSM kan gi pålegg om forbedringer. Virksomhetene vil også kunne be om faglig veiledning fra NSM.

4. I sikkerhetsloven § 27 fremgår det bl.a. at sikkerhetsavtale med utenlandske leverandører bare kan inngås etter godkjenning av Nasjonal sikkerhetsmyndighet. Videre heter det: «Nasjonal sikkerhetsmyndighet kan bestemme at sikkerhetsavtale også skal inngås dersom leverandøren vil kunne få tilgang til skjermingsverdig objekt eller dersom det andre grunner er nødvendig å sikkerhetsgradere anskaffelsen.» Mener statsråden at det vil være naturlig å sikkerhetsgradere anskaffelsen av nøkkelkomponenter til bruk i kritisk infrastruktur, som f.eks. mobilnett?
Hvert enkelt departement skal utpeke skjermingsverdige objekter innen sitt myndighetsområde. I prosessen skal disse objektenes avhengighetsforhold til andre objekter kartlegges, jf. sikkerhetsloven § 17 og forskrift om objektsikkerhet, kap. 2. Kartleggingen skal også lede frem til identifisering av understøttende tjenester og komponenter man er avhengig av for at objektet skal fungere.

Skjermingsverdige objekter er «objekter som etter en skadevurdering anses helt essensielle for samfunnsviktige sikkerhetsinteresser», jf. lovens § 3 første ledd nr. 12.

Jeg legger til grunn at anskaffelser av kritiske komponenter som vil kunne gi tilgang til et skjermingsverdig objekt eller av andre grunner vil kunne påvirke objektets funksjonalitet vil kunne gjennomføres som en sikkerhetsgradert anskaffelse, med den ekstra sikkerhet dette gir.

Fristen for utpeking av skjermingsverdige objekter fra sektorene er satt til 1. januar 2013. En beslutning om hvorvidt anskaffelser er sikkerhetsgraderte vil imidlertid kunne gjøres uavhengig av dette.

Avsluttende bemerkninger
Risiko og sikkerhet knyttet til samfunnets bruk av informasjons- og kommunikasjonsteknologi er noe norske myndigheter tar meget alvorlig. Alle samfunnssektorer er avhengig av denne felles infrastrukturen, og dette skaper en samfunnsmessig sårbarhet som vi må følge nøye. I tillegg er infrastrukturen gjenstand for en rivende teknisk utvikling. Nye bruksmønstre skapes hurtig. Det gjør ikke utfordringen mindre. Det skal ikke være lett å utnytte våre sårbarheter. Derfor må vi være på vakt mot at ondsinnede mekanismer blir installert i teknisk utstyr. I statsbudsjettet for 2013 foreslår vi en betydelig styrking av NSM.

Vi må bruke de muligheter som dagens regelverk gir. Samtidig må regelverket tilpasses fremtidens risikobilde. Flere av de problemstillinger som er reist i det siste rundt beskyttelsen av kritisk IKT-infrastruktur dreier seg ikke utelukkende om teleinfrastrukturen. Problemstillingene er som IKT-systemene selv sektorovergripende. Det vil derfor bli vurdert om disse kan la seg løse i et sektorovergripende regelverk, felles for alle.

Sikkerhetsloven, som forvaltes av Forsvarsdepartementet, er under evaluering. Justis- og beredskapsdepartementet deltar i arbeidet. Formålet med denne loven er som kjent å motvirke spionasje, sabotasje og terrorhandlinger. Det vil være naturlig at de sektorovergripende nasjonale behovene for robusthetsskapende og forebyggende sikkerhet finner sin løsning der. Dette vil jeg følge tett fremover.

Med hilsen
Grete Faremo