FORSVARSMINISTERIET

DET TALTE ORD GÆLDER

Taleseddel samråd B-G om Huawei

Jeg vil naturligvis besvare alle spørgsmål, men med udvalgets tilslutning vil jeg rykke lidt rundt på rækkefølgen og besvare B, E og F under ét, da disse spørgsmål i vidt omfang hænger sammen.

[Spørgsmål C:]
Lad mig starte med spørgsmål C om, hvorvidt telenettet som kritisk infrastruktur også er et spørgsmål om national sikkerhed.

Svaret er ja. Derfor har regeringen defineret telesektoren som en af vores seks samfundsvigtige sektorer – sammen med energi-, sundheds-, transport-, søfarts- og finanssektoren.

Grundlæggende funktioner i vores samfund er afhængige af et velfungerende telenet:

Vi skal kunne komme i kontakt med hinanden, og vi skal kunne ringe efter hjælp, når noget går galt. Vi skal kunne betale for vores varer. Vi skal kunne arbejde på vores computere. Intet af det kan vi, hvis ikke telefoner og internetforbindelser virker.

Og én ting er, hvis det bryder ned i en halv time. Så kan det nok håndteres. Men hvad hvis nogen for alvor får telenettet til at bryde sammen?

Så stopper udbetalinger og overførsler. Private virksomheder og offentlige myndigheder må lukke ned. Vil tog og busser kunne køre? Kan vores hospitaler fungere?

Men sikkerhed i telenettet handler jo også om, at vi skal kunne stole på, at de forkerte ikke lytter med på vores kommunikation. Vi skal kunne føle os trygge ved, at kriminelle og fremmede stater ikke spionerer mod vores myndigheder, virksomheder og borgere.

Med andre ord er det alvorlige sager, vi drøfter i dag, og jeg deler fuldt ud opfattelsen af, at telenettet er et spørgsmål om national sikkerhed.

[Spørgsmål B, E og F:]
Samrådsspørgsmål B, E og F drejer sig alle om vores tillid til Huawei. Og for den sags skyld andre kinesiske televirksomheder.

Helt overordnet har vores tilgang været at sikre, at man fandt de bedste og mest konkurrencedygtige leverandører, samtidig med at der var fokus på sikkerheden.

Udfordringerne med Huawei er ikke ikke et nyt spørgsmål. Det var jo ikke mindst på grund af Huaweis rolle i TDC's 4G-netværk, at vi i Danmark opdaterede lovgivningen på området med "lov om net- og informationssikkerhed" eller "NIS-loven".

Med NIS-loven fik vi *ikke* mulighed for direkte at forbyde bestemte leverandører i vores telenet.

Men loven styrkede reguleringen af informationssikkerheden og beredskabet på teleområdet, og den skærpede kravene til teleselskabernes sikkerhed. På daværende tidspunkt kunne vi se en alvorlig stigning i cyberangreb og avanceret industrispionage, som er fortsat de seneste år.

Det var således for at kunne håndtere udfordringerne med udenlandske leverandører med tæt tilknytning til fremmede stater, at lovgivningen blev opdateret. Vi var fuldt ud opmærksomme på, at man med visse udenlandske firmaer i vores telenet kunne øge risikoen for at lukke døren op for spionage, industrispionage og potentielt ødelæggende angreb.

Så det er altså ikke nyt, at vi har haft fokus på Huawei og andre leverandører af teknologi til vores telesektor. Og at vi løbende forsøger at tage de nødvendige - og proportionelle - forholdsregler.

Vores opmærksomhed er så på det seneste blevet skærpet.

Som dagens samrådsspørgsmål også nævner, har en række lande på det seneste været ude at advare mod eller ligefrem forbyde at bruge Huawei som leverandør i telenettet.

Det er ikke mindst sket i lyset af den forestående introduktion af den nye 5G-teknologi.

Det understreger for det første, at det var godt, at vi tog de forholdsregler, vi gjorde med vedtagelsen af NIS-loven. Men det giver naturligvis også anledning til fornyede overvejelser, også fra den danske regerings side.

Det er klart, at danske borgere og virksomheder skal kunne føle sig helt trygge ved, at de systemer, vi bruger til vores kommunikation, er tilstrækkeligt sikre.

Derfor har Center for Cybersikkerhed løbende brugt de muligheder, der er i loven for at bl.a. at føre tilsyn med teleselskaberne for at øge sikkerheden. Og derfor følger Center for Cybersikkerhed udviklingen meget tæt.

En særlig del af centerets indsats er målrettet en løbende og tæt dialog med telesektoren med henblik på at styrke informationssikkerheden og beredskabet i telesektoren.

Men jeg håber også, at der er forståelse for, at vi ikke kan være helt åbne om indholdet af den dialog, der foregår mellem regeringen, Center for Cybersikkerhed og forskellige private aktører. Men der skal ikke herske tvivl om, at regeringen tager spørgsmålet alvorligt og er i gang med at se på, hvordan vi kan håndtere situationen til gavn for Danmarks sikkerhed.

[Spørgsmål G:]
Alvoren i sagen er jo også knyttet til samrådsspørgsmål G om den kinesiske lovgivning, som pålægger kinesiske virksomheder at hjælpe kinesiske myndigheder.

Kina har organiseret sig anderledes, end vi har her i Danmark, hvad angår sondringen mellem stat og private virksomheder i kinesisk lovgivning.

Alle kinesiske virksomheder kan potentielt blive anvendt som værktøj for den kinesiske stats strategiske mål. De fleste større virksomheder som Huawei har tætte forbindelser til det politiske system, og realiteten er, at Huawei er omgærdet af nogle ugennemsigtige ejerforhold.

Det fremgår direkte af kinesisk lovgivning, at personer og virksomheder er forpligtet til at hjælpe den kinesiske efterretningstjeneste.

Derfor kan jeg godt forstå, at spørgeren bringer dette op, og jeg er helt enig i, at det giver anledning til bekymring. Og derfor har

vi også et særligt fokus på den dynamik, der er mellem den kinesiske stat og kinesiske virksomheder som Huawei.

[Spørgsmål D:]
Det sidste samrådsspørgsmål på listen er spørgsmål D, om Danmark som eksempelvis Tyskland bør indføre no-spy klausuler.

Som nævnt er den kinesiske lovgivning, og sondringen mellem den kinesiske stat og kinesiske virksomheder, anderledes end det vi kender i Vesten. Det er regeringen og Center for Cybersikkerhed helt opmærksom på.

Det er ikke umiddelbart vurderingen, at NIS-loven giver mulighed for at pålægge en teleudbyder at indsætte klausuler i leverandøraftaler om det vi kalder en 'no-spy' klausul.

Til gengæld kan Center for Cybersikkerhed stille en række krav til teleselskaberne. Herunder kan centret kræve, at et teleselskab sikrer, at det kan hjemtage opgaver fra en udenlandsk leverandør, hvis kontrakten misligholdes.

Der kan også stilles krav om, at der bliver lavet en uafhængig sikkerhedsevaluering, når man køber kritiske netkomponenter mv. fra en specifik leverandør, ligesom der kan stilles krav om, at særligt personale skal sikkerhedsgodkendes.

Der findes altså i loven en række redskaber til at imødegå trusler mod informationssikkerheden, der kan stamme fra de leverandører, teleselskaberne anvender.

[Afslutning:]

Afslutningsvis vil jeg blot gentage, at spørgsmålet om Huawei i det danske telenet er noget, regeringen tager meget alvorligt. Og at vi løbende forholder os til, hvordan vi bedst kan håndtere situationen til gavn for Danmarks sikkerhed.

Vi har selvfølgelig brug for konkurrence, så vi får de bedste løsninger til gavn for danskerne. Men vi skal ikke være naive, og vi er som sagt i gang med at se på, hvad vi kan gøre for at sikre tryghed ved de leverandører, vi bruger til det danske telenet. Tak.