TELE INDUSTRIEN
teleselskabernes branchesamarbejde

Forsvarsministeriet
Att.: Specialkonsulent Nicklas B. Baumgarten
Sendt pr. e-mail til nbb@fmn.dk

4. januar 2021

Høring over udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur

Teleindustrien (TI) har noteret sig, at Forsvarsministeriet den 7. december 2020 har sendt udkast til forslag til lov om leverandørsikkerhed i den kritiske teleinfrastruktur i høring med frist kl. 12, den 4. januar 2021.

TI finder det positivt, at regeringen sætter fokus på den digitale infrastrukturs samfundskritiske funktion. Forslaget tager udgangspunkt i, at velfærd og velstand i det danske samfund i høj grad afhænger af en velfungerende og sikker teleinfrastruktur. Det er en vurdering, som telebranchen i allerhøjeste grad deler.

En velfungerende og sikker teleinfrastruktur er afgørende for det danske samfund, teleselskabernes kunder og naturligvis også branchen selv. Med det afsæt har branchen over de seneste 10 år investeret 70 mia. kr. i at udbygge den digitale infrastruktur i Danmark med fokus på både kapacitet og sikkerhed. Udbygningen er sket i tæt dialog med danske myndigheder, herunder særligt Center for Cybersikkerhed. Det er med dette udgangspunkt, at nedenstående høringssvar skal læses.

Generelt
Forudsigelige rammer og en markedsbaseret udvikling har siden telemarkedets liberalisering været grundlæggende politiske og regulatoriske principper, der har ført til massive investeringer i en robust og sikker dansk teleinfrastruktur.

Lovudkastet indeholder imidlertid en række vidtrækkende beføjelser, som er yderst indgribende i aftalefriheden for TI's medlemmer, og som potentielt kan medføre, at en teleudbyder, der har støttet ret på en lovlig indgået aftale, kan blive tvunget til at omlægge sin infrastruktur. En forceret omlægning kan indvirke negativt på den operati-

onelle og sikkerhedsmæssige stabilitet af telenettet og kan medføre omkostninger i milliardklassen.

Dertil kommer, at konkurrencen blandt leverandører af teleinfrastruktur er afgørende for, at der fortsat er incitament for leverandørerne til at udvikle innovative løsninger og sikre, at omkostningerne holdes nede, hvilket i sidste ende er til gavn for brugerne af tjenesterne på markedet og samfundet som helhed.

Såfremt det med lovforslaget er tanken helt at udelukke bestemte leverandører, vil det for eksempelvis betyde, at udbyderens muligheder for valg af leverandør af radionetværk til mobilnettene vil blive meget begrænset. Lovforslaget vil dermed medføre en betydelig svækkelse af konkurrencen.

Tilmed lægges der op til, at Danmark indfører et af de mest restriktive og uforudsigelige forbudsregimer i EU, hvilket i sig selv vil betyde, at nogle af de mest innovative netværksleverandører vil fravælge Danmark. Det vil andet lige betyde højere priser og mindre innovative produkter til de danske forbrugere.

Det er derfor helt afgørende for TI, at det endelige lovforslag tilrettes således, at der skabes en langt højere grad af regulatorisk forudsigelighed, tilstrækkelige retssikkerhedsmæssige garantier for teleudbyderne, og at indgrebsmuligheden alene anvendes helt undtagelsesvis og efter en nøje vurdering af truslen mod statens sikkerhed på den ene side og de operationelle sikkerhedsaspekter samt markedsmæssige konsekvenser på den anden side.

Efter TI's opfattelse bør lovforslaget som minimum tilrettes på følgende centrale punkter:

1) Forbudsbeslutninger skal foretages af Forsvarsministeriet efter indstilling fra Center for Cybersikkerhed og høring af andre relevante myndigheder.
2) Teleudbyderne skal sikres mulighed for partshøring og begrundelse for afgørelserne.
3) Afgørelser om forbud kan kun udstedes, hvis påbud efter lov om net- og informationssikkerhed har vist sig ikke at være tilstrækkelige.
4) Lovens tilbagevirkende kraft for aftaler indgået før 7. december 2020 udgår eller udskydes til tidligst 1. januar 2030.
5) Teleudbyderen skal have ret til fuld erstatning ved forbud, der får betydning for anvendelse af lovligt leveret udstyr uanset, om det kan anses for at udgøre ekspropriation.
6) Der skal indføres regler om effektiv prøvelse af afgørelser og tilsyn med Center for Cybersikkerhed.
7) Definitionen af "kritisk infrastruktur" er uklar og skal præciseres væsentligt.

TI har i det følende nærmere redegjort for disse overordnede punkter. Derudover følger en række yderligere forslag til præcisering af lovud-

kastet for at sikre en nødvendig og højere grad af forudsigelighed for teleudbyderne.

Ad 1) Forbudsbeslutninger skal foretages af Forsvarsministeriet efter indstilling fra Center for Cybersikkerhed og høring af andre relevante myndigheder

TI har i forbindelse med vedtagelsen af CFCS-loven og lov om net- og informationssikkerhed kritiseret, at tilsynet med telesektoren er lagt i en forvaltningsmyndighed under Forsvarets Efterretningstjeneste og ikke som al anden erhvervsrettet lovgivning i den civile del af forvaltningen. Det medfører, at reguleringen af telesektoren på dette område ikke ses i sammenhæng med den øvrige regulering, og at selskaberne ikke har den nødvendige sikkerhed for inddragelse af andre samfundshensyn end snævre militære strategiske overvejelser.

Det er fortsat TI's principielle synspunkt, at Center for Cybersikkerheds opgaver på dette område, som tilfældet er i hovedparten af de øvrige EU-lande, bør flyttes til den civile del af forvaltningen. TI er dog opmærksom på, at en sådan ressortændring næppe er mulig inden for den tidsramme, der er sat for det fremlagte lovudkast.

Der er imidlertid med lovudkastet tale om meget indgribende foranstaltninger, der kan have vitale markedsmæssige konsekvenser, og som foretages på grundlag, som udbyderne ikke har indsigt i, hvilket stiller udbyderne i en svag retssikkerhedsmæssig position.

Det er derfor nødvendigt, at indgrebsmuligheden alene anvendes helt undtagelsesvis og efter en nøje vurdering af truslen mod statens sikkerhed på den ene side og de markedsmæssige konsekvenser på den anden side. Det bør derfor sikres, at en beslutning om forbud forberedes grundigt og træffes på højeste niveau i ministeriet. Efter opsplitningen af den tidligere IT- og Telestyrelse er kompetencer og viden om telebranchen i dag spredt på en række myndigheder. Energistyrelse, Erhvervsstyrelsen og Konkurrence- og Forbrugerstyrelsen har alle indgående kendskab til tekniske og markedsmæssige forhold på teleområdet og bør derfor høres, inden der træffes afgørelse. TI skal derfor opfodre til, at en afgørelse om forbud træffes af Forsvarsministeriet efter indstilling fra Center for Cybersikkerhed og efter høring af andre relevante ministerier og myndigheder.

Der henvises i øvrigt til det lovforslag, der er sendt i høring af Erhvervsstyrelsen den 9. december 2020 om lov om screening af visse udenlandske direkte investeringer m.v. i Danmark (Investeringsscreeningsloven)[1], hvor afgørelser om forbud mod investeringer træffes af Erhvervsministeriet efter indstilling fra Erhvervsstyrelsen og høring af andre relevante myndigheder.

Det fremgår af rapporten fra den tværministerielle arbejdsgruppe[2] (s. 153 ff), der er udarbejdet forud for udkastet til Investeringsscree-

[1] https://hoeringsportalen.dk/Hearing/Details/64672

[2] Rapprt om en kommende generel ordning for screening af udenlandske investeringer mv. (windows.net)

ningsloven, at det er arbejdsgruppens anbefaling, at forbudsbeslutninger træffes af ministeriet og efter høring af andre relevante myndighederne. Det begrundes bl.a. i, at et forbud er vidtgående og andre lande, som Finland, Frankrig og Tyskland, Norge og USA, der har indført regler om forbud mod investeringer ikke har delegeret kompetencen for at træffe afgørelser om forbud væk fra ministeriet.

Der er vanskeligt at se, hvorfor samme hensyn ikke skal tages i forhold til indgreb overfor leverandører af kritisk teleinfrastruktur, henset til at indgrebet for den enkelte virksomhed kan have mindst lige så indgribende karakter som et indgreb mod udenlandske investeringer.

TI skal derfor henstille til, at lovforslaget ændres, så kompetencen til at træffe afgørelser om forbud mod visse leverandører ligger hos ministeriet.

Ad 2) Teleudbyderne skal sikres mulighed for partshøring og begrundelse for afgørelserne

Det fremgår af lovudkastet § 5, at offentlighedsloven (bortset fra lovens § 13), og forvaltningslovens kapitel 4-6 ikke finder anvendelse.

Efter lovbemærkningerne til lovforslaget (s. 16-17) må det forstås, at undtagelsen fra offentlighedsloven og forvaltningslovens principper om partshøring og begrundelse af afgørelser er mere vidtgående end den undtagelse, der er gælder i forhold til Center for Cybersikkerheds øvrige virksomhed, hvor det er forudsat, at centeret trods den generelle undtagelse til forvaltningsloven og offentlighedsloven i det væsentlige skal efterleve de forvaltningsretlige retssikkerhedsprincipper om partshøring og begrundelse. Der er således tale om en meget vidtgående indskrænkning i teleudbydernes retstilling og mulighed for at varetage deres interesser.

Det er efter TI's opfattelse stærkt kritisabelt, at teleudbyderne dermed afskæres fra helt grundlæggende retssikkerhedsgarantier. Dette skal særligt ses i forhold til, at et forbud efter lovudkastet vil være langt mere indgribende end de foranstaltninger, Center for Cybersikkerhed kan påbyde efter lov om net- og informationssikkerhed. Der er derfor i højere grad behov for, at teleudbydernes retssikkerhed styrkes og ikke indskrænkes.

TI har selvsagt forståelse for, at der kan være oplysninger, der indgår i vurderingen af, om en leverandør udgør en trussel mod statens sikkerhed, som af hensyn til nationale og internationale sikkerhedsinteresser ikke kan videregives til den teleudbyder, der er part i sagen. Det begrunder dog ikke, at partshøring og begrundelse for afgørelsen helt undtages.

I udkastet til Investeringsscreeningsloven, hvor Erhvervsstyrelsen og Erhvervsministeriet skal foretage sagsbehandling af tilsvarende for-

hold, er der ikke lagt op til en generel undtagelse for forvaltningslovens kap 4-6.

Det fremgår bl.a. således af lovbemærkningerne til § 38 i udkastet til Investeringsscreeningsloven (s. 92):

> *"Samtidig er det også væsentligt i videst muligt omfang at beskytte rettighederne for parterne i sagen, og ikke fravige mere fra reglerne i offentlighedsloven og forvaltningsloven end nødvendigt. Parterne i sager efter loven bør derfor som udgangspunkt have mulighed for at blive gjort bekendt med oplysninger i sagen, herunder navnlig oplysninger om deres personlige forhold. Der bør derfor kun være mulighed for at afskære fra partsaktindsigt i det omfang hensyn til national sikkerhed og offentlig orden efter en konkret vurdering gør det nødvendigt. Endvidere bør øvrige regler om sagsbehandling i offentlighedsloven og forvaltningsloven, der ikke vedrører aktindsigt, gælde også for sager efter denne lov."*

Sammenholdes de to lovudkast, vil den foreslåede retstilstand betyde, at danske teleudbydere opnår en ringere retsbeskyttelse end udenlandske parter, der ønsker at investere i et selskab, der råder over kritisk infrastruktur.

Det bemærkes endvidere, at det fremgår af udkastet til lovforslag om leverandørsikkerhed § 2, stk. 2, og § 3, stk. 4, at Center for Cybersikkerhed kun kan nedlægge forbud, hvis hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger.

For at Center for Cybersikkerhed kan foretage den vurdering, er det nødvendigt, at centeret er forpligtet til at partshøre teleudbyderen, da centeret sjældent vil have tilstrækkeligt viden om teleudbyderens infrastruktur og sikkerhedssystemer til at foretage en tilstrækkelig afdækning af de faktiske forhold og dermed undersøge alternative forholdsregler.

Det fremgår af bemærkningerne (s. 33), at

> "*Bestemmelsen [§ 2] typisk vil finde anvendelse, efter at der gennem længere tid har været dialog mellem teleudbyderen og Center for Cybersikkerhed om den pågældende aftale*."

Dette finder TI positivt, men forudsætningen om forudgående partshøring af teleudbyderen bør indføres direkte i loven.

På den baggrund skal TI henstille til, at lovudkastets § 5 udgår og erstattes med tilsvarende regler, som fremgår af § 38 i udkastet til Investeringsscreeningsloven.

Ad 3) Afgørelser om forbud skal kun udstedes, hvis påbud efter lov om net- og informationssikkerhed har vist sig ikke at være tilstrækkelige.

Det fremgår af § 2, stk. 2, og § 3, stk. 4, at det er en forudsætning for et forbud, at Center for Cybersikkerhed konkret har vurderet, at hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger end et forbud. Det fremgår i tilknytning hertil af lovbemærkningerne (s. 14f), at det således vil være en forudsætning, at Center for Cybersikkerhed har forsøgt at rådgive teleudbyderen om de tilpasninger af aftalen, som vil være nødvendige, for at den ikke længere vurderes at udgøre en trussel mod statens sikkerhed. Center for Cybersikkerhed vil også skulle have vurderet relevante muligheder i net- og informationssikkerhedsloven, herunder eksempelvis muligheden for at give påbud om, at teleudbyderen skal foretage konkrete sikkerhedsforanstaltninger.

TI er enig i, at et forbud ikke bør udstedes, før andre mindre indgribende foranstaltninger har været bragt i anvendelse.

Det gælder særligt i en situation, hvor teleudbyderen har indgået en aftale, efter aftalen har været anmeldt iht. lov om net- og informationssikkerhed, og Center for Cybersikkerhed ikke har fundet anledning til at udstede påbud efter lov om net- og informationssikkerhed. I en sådan situation (uanset om aftalen er indgået før eller efter lovudkastet er bragt i høring) har teleudbyderen indrettet sig i tillid til, at aftalen og de eventuelle iværksatte sikkerhedsforanstaltninger, som teleudbyderen har foretaget, ikke udgør nogen trussel mod statens sikkerhed.

Der bør derfor stilles skærpede krav til, hvornår et forbud efter § 3, stk. 1 og 2, kan bringes i anvendelse overfor allerede indgåede aftaler. TI har noteret sig, at det er en forudsætning for anvendelsen af § 3, at der ikke blot kan konstateres en trussel mod statens sikkerhed, som er tilfældet med forbud efter § 2, men at truslen skal være ”væsentlig”. Der er dog ikke nogen kvalificering af væsentlighedsbegrebet i lovens bemærkninger, idet de eksempler, der henvises til i lovbemærkningerne (s. 37), ikke adskiller sig fra de forhold, som kan begrunde et indgreb efter § 2. Kriteriet om, at der skal foreligge en ”væsentlig” trussel mod statens sikkerhed, udgør således ikke nogen reel beskyttelse af teleudbyderne.

Tilsvarende bør der tages særlige hensyn forud for anvendelse af forbud efter § 2 overfor aftaler, der vedrører en forlængelse eller genforhandling af eksisterende aftaler.

Et forbud mod indgåelse af en forlængelse af en aftale om fx support eller reservedele til udstyr, der er leveret iht. en allerede indgået aftale, kan være nødvendig for, at det allerede leverede udstyr fortsat kan anvendes. Det er helt sædvanligt, at sådanne supportaftaler ikke indgås med en varighed, der svarer til udstyrets levetid, og det derfor er nødvendigt med en løbende tilpasning af disse aftaler. Et forbud mod indgåelse af en sådan aftale om forlængelse eller genforhandling

kan derfor de facto medføre, at det allerede leverede og lovlige udstyr er ubrugeligt, og dermed tvinges udbyderen til at udskifte fuldt lovligt udstyr. Udbyderen kan også stå i en situation, hvor den operationelle stabilitet og sikkerhed påvirkes negativt, hvis eksisterende udstyr ikke længere må bruges, men ikke kan udskiftes, fordi der ikke umiddelbart er en anden mulig leverandør.

Tilsvarende gør sig gældende i forhold til softwareopdateringer, for eksempel sikkerhedsopdateringer, platformsudvidelser eller andre nødvendige funktionelle opdateringer til systemet til sikring af dets fortsatte drift og support af markedsinitiativer. Sådanne naturlige forlængelser og udbygninger af eksisterende aftaler, som er indgået i god tro før 7. december 2020 og under Center for Cybersikkerheds tilsyn i medfør af lov om net- og informationssikkerhed, bør som udgangspunkt ikke betragtes som værende omfattet af forbud efter § 2. Denne problemstilling forværres desuden af lovforslagets meget uklare definition af begrebet "kritisk infrastruktur", der potentielt kan omfatte stort set alle IT-systemer, der anvendes i en teleudbyders forretning, jf. nedenfor.

TI skal opfordre til, at det direkte fremgår af lovteksten, at forbud efter lovens § 2 for så vidt angår forlængelse eller genforhandling af eksisterende aftaler og forbud efter § 3 ikke kan bringes i anvendelse med mindre, der er sket en konkret og væsentlig ændring af den sikkerhedsmæssige vurdering i forhold til den konkrete aftales parter og indhold, og før mindre indgribende foranstaltninger, som Center for Cybersikkerhed har taget i anvendelse, jf. lov om net- og informationssikkerhed, har vist sig utilstrækkelige.

Ad 4) Lovens tilbagevirkende kraft for aftaler indgået før 7. december 2020 udgår eller udskydes til tidligst 1. januar 2030.
Det fremgår af udkastet til lovforslag § 17, stk. 3, at loven får tilbagevirkende kraft på aftaler indgået før 7. december 2020. Som begrundelse herfor anføres det i lovbemærkningerne (s. 14):

> *Endvidere finder Forsvarsministeriet, at også aftaler, der er indgået før høringstidspunktet, bør omfattes af reguleringen fra den 1. januar 2026. Det er ministeriets vurdering, at meget få aftaler vil have så lang løbetid, men ordningen vil sikre, at der bliver mulighed for at tage stilling til, om sådanne aftaler skal forbydes, dog således, at teleudbyderne har haft næsten fem år til at indrette sig på, at aftalerne bliver omfattet af den skærpede regulering.*

TI skal gøre opmærksom på, at det ikke er korrekt, at teleudbyderne allerede ved lovens fremsættelse kan begynde at indrette sig, da det er fuldstændig uklart, hvilke lande og hvilke specifikke leverandører Center for Cybersikkerhed anser for at udgøre en trussel mod statens sikkerhed. Først når den viden er konkretiseret og kommunikeret til udbyderne, kan de begynde at lægge planer for udskiftning af allerede leveret infrastruktur.

Det er i øvrigt underordnet, at der er tale om få aftaler, der vil have så lang løbetid. Det er de enkelte aftalers omfang og det leverede udstyrs levetid, der er relevant, og selv om der vil være tale om få aftaler samlet set, så er de grundlaget for betydelige dele af infrastrukturen i på det danske marked.

Det bemærkes i den forbindelse, at Center for Cybersikkerhed har et indgående kendskab til de leverandøraftaler, der anvendes på det danske marked, samt hvilke aftaler der fra 7. december 2020 er på vej til at blive indgået. Det bør derfor allerede ved lovforslagets fremsættelse gøres entydigt klart, om der er leverandører, som Center for Cybersikkerhed anser som en trussel mod statens sikkerhed. I det omfang dette ikke fremgår, må det kunne lægges til grund, at Center for Cybersikkerhed på nuværende tidspunkt ikke finder, at der er leverandører på det danske marked, der på nuværende tidspunkt udgør en risiko for statens sikkerhed.

En udfasning og udskiftning af allerede leveret infrastruktur forudsætter, at der først igangsættes analyse af behov, herefter en udbudsfase og kontraktindgåelse og dernæst en implementering af den nye leverandørs udstyr og udfasning af tidligere leverandører. En sådan proces vil være forceret frem mod 2026 og kan ikke gennemføres uden betydelige omkostninger for de berørte udbydere, hvilket kan stille dem væsentlig ringere i konkurrencen overfor andre udbydere på telemarkedet.

En forceret udfasning kan også få vital betydning for driftsstabiliteten af netværkene og kan i værste fald betyde, at udbyderne ikke kan benytte en kritisk leverandør til at forhindre et nedbrud, hvilket i sig selv vil være samfundskritisk og udgøre en alvorlig sikkerhedsmæssig trussel.

Det bemærkes i øvrigt, at den britiske regering med en beslutning fra november 2020[3] har meddelt operatørerne på det britiske marked, at RAN-udstyr fra en navngiven leverandør skal være ude af mobilnettene pr. 1. januar 2028. Det er værd at bemærke, at forbuddet alene omfatter en specifik leverandørs leverancer af RAN-udstyr i mobilnetværkene, og at perioden er mere end 2 år længere end den, der lægges op til i det danske lovforslag.

TI skal på den baggrund opfordre til, at lovens tilbagevirkende kraft helt opgives eller alternativt tidligst får virkning fra 1. januar 2030.

Tilsvarende bør lovens ikrafttrædelse udskydes for aftaler om forlængelse eller genforhandling af eksisterende aftaler indgået før 7. december 2020, idet et forbud mod indgåelse af sådanne aftaler de facto vil medføre, at allerede lovligt leveret udstyr vil være ubrugeligt, jf. bemærkningerne ovenfor.

---

[3] https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy/5g-supply-chain-diversification-strategy

Ad 5) Teleudbyderen skal have ret til fuld erstatning ved forbud, der får betydning for anvendelse af lovligt leveret udstyr uanset, om det kan anses for at udgøre ekspropriation

Det er positivt, at der i lovudkastet § 4 er taget stilling til, at der skal ydes fuld erstatning i tilfælde af afgørelser, der efter loven udgør et ekspropriativt indgreb.

Ved en nærmere gennemgang af lovbemærkningerne er det dog uklart, hvornår der er tale om ekspropriation, og hvordan grundlovens begreb "fuldstændig erstatning" skal forstås i forbindelse med ekspropriation efter lovforslaget.

Det fremgår også af bemærkningerne, at det er Forsvarsministeriets vurdering, at det er et begrænset antal afgørelser, hvor der vil være tale om ekspropriation.

Det fremgår således af bemærkningerne (bl.a. s. 21):

> *Navnlig det forhold, at forbud mod indgåelse af en aftale efter § 2, stk. 1, opretholdelse af en indgået aftale efter § 3, stk. 1, eller anvendelse af kritiske komponenter, systemer m.v. efter § 3, stk. 2, er begrundet i hensyn til statens sikkerhed, må antages at tale med en vis vægt imod, at der vil være tale om ekspropriation.*
> *(TI's understregning)*

Dette synes ikke at give nogen stor sikkerhed for, at indgreb med afståelse af ejendomsret til følge formelt vil blive betragtet som et ekspropriativt indgreb. De anførte bemærkninger giver dermed ikke noget reelt incitament for Center for Cybersikkerhed til at træffe forbudsafgørelser, hvor der er sikret den rette proportionale balance mellem statens sikkerhed og hensynet til teleudbydernes ejendomsret og investeringer.

Dertil kommer, at lovforslaget, så vidt det ses, ikke tager stilling til, at krav efter lovforslaget kan medføre betydelige direkte og indirekte negative økonomiske følgevirkninger i form af øgede udgifter til nyanskaffelser, forringede netværksoplevelser for kunderne og med evt. tabte markedsandele til følge m.m.

Der er TI's klare opfattelse, at et forbud mod direkte eller indirekte anvendelse af allerede leveret og lovligt udstyr vil udgøre et ekspropriativt indgreb.

TI henstiller derfor til, at det eksplicit præciseres i lovbemærkningerne, at et forbud mod allerede indgåede aftaler, herunder forbud der direkte eller indirekte får betydning for anvendelse af lovligt leveret udstyr, vil give udbyderen ret til fuld erstatning. Det gælder særligt aftaler, der er indgået før 7. december 2020.

Ad 6) Der skal indføres regler om effektiv domstolsprøvelse af afgørelser og tilsyn med Center for Cybersikkerhed

Det fremgår af lovudkastet §§ 6 og 7, at Center for Cybersikkerheds afgørelser ikke kan påklages til anden administrativ myndighed, og at eneste prøvelse af afgørelserne kan foretages af domstolene. Med de begrænsninger, der fremgår af §§ 8-13, er der tilmed tale om en begrænset prøvelse af grundlaget for afgørelserne.

TI mener, at en indbringelse af en forbudsafgørelse for domstolene automatisk bør få opsættende virkning. En domstolsprøvelse uden opsættende virkning kan have den konsekvens, at teleoperatøren, uanset udfaldet af retssagen, vil være nødt til at enten slukke eller nedtage og udskifte den del af netværket, som er omfattet af tvisten. Dette kan medføre uoprettelig skade for den udbyder, det går ud over, men også for konkurrencen på markedet, hvilket vil være direkte til skade for slutbrugerne. Sådanne skadegørende virkninger af en ulovlig afgørelse vil ikke fuldt ud kunne kompenseres ved, at der ydes en økonomisk erstatning til den udbyder, det går ud over.

TI mener i øvrigt, at lovudkastet skal tilrettes således, at der gives teleudbyderen mulighed for fuld partsrepræsentation ved egen advokat. Med den foreslåede § 9 afskæres udbyderne imidlertid for en sådan adgang. Det forhold, at udbyderne ikke selv må lade sig repræsentere, men skal anvende en særlig udpeget sikkerhedsadvokat, der ikke må dele fortroligt materiale med udbyderen, vil gøre det nærmest umuligt for udbyderne at bidrage til sagens oplysning. Selv når en dommer har besluttet, at relevante oplysninger skal forelægges for udbyderen, kan Forsvarsministeren afskære adgangen til de pågældende oplysninger, selvom de har været afgørende for forbudsafgørelsen, jf. § 9, stk. 3.

I forbindelse med prøvelse af en afgørelse er det afgørende, at udbyderens advokat i det mindste har fuld indsigt i grundlaget for afgørelsen, og at sagen kan drøftes med udbyderen – også når advokaten har fået indsigt i fortroligt materiale. Det bør derfor kun være indholdet af de fortrolige oplysninger om statens sikkerhed, der ikke må drøftes med udbyderen. I det omfang, udbyderen har sikkerhedsgodkendt personale, bør det desuden være muligt at drøfte sådanne oplysninger med udbyderen.

Hvis der er oplysninger, der har ligget til grund for Center for Cybersikkerheds oprindelige afgørelse, og en dommer mener, at der er oplysninger, som udbyderen bør se, vil det være helt urimeligt, at Forsvarsministeren kan beslutte, at oplysningerne ikke længere skal indgå i sagen. Hvis denne mulighed opretholdes i lovforslaget, bør konsekvensen være, at oplysningerne ikke kan indgå i prøvelsen, og dermed ikke vil kunne tillægges vægt ved domstolens vurdering af, om forbuddet er lovligt.

Center for Cybersikkerheds administration af loven bør også underlægges et effektivt tilsyn. Henvisningen i lovbemærkningerne (s. 11) til Tilsynet med Efterretningstjenesterne kan give det misvisende ind-

tryk, at Tilsynet med Efterretningstjenesterne også fører tilsyn med Center for Cybersikkerheds aktiviteter efter lov om leverandørsikkerhed. Det er imidlertid ikke tilfældet. Henset til, at der i forbudsafgørelser efter lovforslaget vil være oplysninger, som ikke kan deles med udbyderen, ligesom Center for Cybersikkerhed i dialogen med udbyderne forud for en eventuel forbudsafgørelse uretmæssigt kan få udbyderen til at give tilsagn om at implementere byrdefulde sikkerhedsmæssige foranstaltninger, bør der føres et effektiv tilsyn med, at Center for Cybersikkerhed forvalter sine beføjelser i overensstemmelse med lovens hensigt.

TI skal derfor anbefale, at der indsættes en bestemmelse i loven, der giver Tilsynet med Efterretningstjenesterne hjemmel til at føre et effektivt tilsyn med Center for Cybersikkerheds forvaltning af såvel lov om leverandørsikkerhed og lov om net- og informationssikkerhed.

Ad 7) Definitionen af "Kritisk infrastruktur" er uklar og skal præciseres væsentligt

Det er afgørende, at der er en klar og entydig definition af begrebet kritisk infrastruktur og kritiske netkomponenter.

Den nuværende definition i lovudkastet § 1, nr. 1, svarer til samme definition i lov om net- og informationssikkerhed. Definitionen er meget bred, og de anvendte begreber som fx "operations support systemer" og "business support systemer" udgør ikke nogen entydig branchemæssig forståelse, hvorved stort set alle IT-systemer, der anvendes i en teleudbyders forretning, herunder tjenesteudbydere, der ikke har eget netværk, men anvender egne support-systemer, bliver omfattet af loven.

Det er også uklart, hvad der forstås ved "centrale routere og servere i backbonenettet". Der er ingen afgrænsning af, hvad der er "centrale" og "ikke-centrale" routere. Udbyderne er således overladt til Center for Cybersikkerheds uforudsigelige vurdering af, om et netværkselement er omfattet.

Det er tilsvarende uklart, hvad der menes med "hardware […], der anvendes i core-net". Det er uklart, om det også betyder, at fx passive dele som fiberkablerne i et core-net omfattes, selvom et fiberkabel vanskeligt kan indeholde aflytningsudstyr eller kan kompromitteres af leverandøren.

TI skal opfodre til, at de dele af udbydernes infrastruktur, der omfattes af loven, entydigt angives, samt at dette afgrænses til kun at gælde det absolut mest nødvendige.

Yderligere bemærkninger

Ud over ovennævnte bemærkninger har TI i det følgende oplistet en række yderligere forslag til præcisering af lovudkastet for at sikre en højere grad af forudsigelighed for teleudbyderne.

Pligtsubjekter - konkurrenceforvridning
TI har noteret, at loven alene finder anvendelse på "væsentlige erhvervsmæssige udbydere", jf. § 1, nr. 3. Dermed falder fx ejere af private netværk udenfor for lovens anvendelsesområde. Dette skal sammenholdes med, at mobiludbyderne står overfor en kommende auktion af nye frekvenser, hvorefter en udbyder sandsynligvis vil blive forpligtet til at stille frekvensressourcer til rådighed for private netværk gennem erhvervelse af en frekvensmængde afsat til dette formål. En sådan udnyttelse til private formål vil i praksis blive relevant, hvis mobiludbyderne ikke tilbyder de specialtjenester, som de private virksomheder efterspørger. Hvis kun mobiludbyderne forbydes at anvende udstyr fra visse leverandører, kan der opstå en konkurrenceforvridende situation ved, at de private virksomheder kan indgå aftaler med de selvsamme leverandører, som udbyderne er afskåret fra at anvende.

Såfremt udkastet til lovforslag fastholdes, bør det sikres, at et forbud mod anvendelse af en bestemt leverandør også gælder for ejere af private net, der anvender frekvenser, der er tildelt en udbyder ved udbud eller auktion.

Trussel mod statens sikkerhed – uklare og uforudsigelige kriterier
Kriterierne i § 2 for vurdering af, om der foreligger en "trussel mod statens sikkerhed", er uklare og uforudsigelige. Der mangler indsigt i, hvordan de fire kriterier skal fortolkes. Der henvises i lovbemærkningerne til, at kriterierne er objektive, men reelt er de meget brede og uigennemskuelige. Dette medfører en meget stor regulatorisk usikkerhed for såvel teleselskaber som udstyrsleverandører.

Det ser imidlertid ud til, at der skal meget lidt til at bringe forbud i anvendelse. Det fremgår fx af § 2, stk. 1, nr. 4, at en aktør kan anses for at udgøre en trussel mod statens sikkerhed, hvis aktøren har været involveret i aktiviteter, der har medført "en negativ påvirkning af statens sikkerhed, informationssikkerheden eller den offentlige orden." Kriteriet er cirkulært formuleret, idet det åbenbart kan være en trussel mod statens sikkerhed, hvis aktøren har haft en negativ påvirkning af statens sikkerhed. Derudover kan selv en undskyldelig fejl i et stykke software udgøre en "negativ påvirkning af informationssikkerheden", og dermed være en trussel mod statens sikkerhed. Det er vanskeligt at se, at der heri er tale om objektive og klare kriterier.

Sammenholdes dette med udkastet til Investeringsscreeningsloven, synes der at være noget højere krav til, at et forbud efter Investeringsscreeningsloven kan tages i anvendelse. Det fremgår således heraf, at et forbud forudsætter, at den "Nationale sikkerhed" eller den "Offentlige orden" er truet, og begge begreber er udførligt afgrænset i loven og dens bemærkninger. Eksempelvis er den "Nationale sikkerhed" eksplicit defineret i lovudkastets § 4, stk. 1, nr. 1 med følgende afgrænsning:

> *Forhold der vedrører Danmarks territorielle integritet og befolkningens overlevelse, risikoen for forstyrrelse af internationale relationer eller nationernes fredelige sameksistens samt trusler mod militære interesser, samt handlinger, der har til hensigt at forvolde Danmark skade, som er i strid med hensynet til national sikkerhed, herunder forbrydelser mod statens selvstændighed eller forbrydelser mod statsforfatningen og de øverste statsmyndigheder*

TI skal derfor henstille til, at der bringes overensstemmelse mellem begreberne i hhv. Leverandørsikkerhedsloven og Investeringsscreeningsloven for at undgå tvivl om, hvad der forstås ved hhv. "Statens sikkerhed" og "National Sikkerhed".

Det fremgår derudover af lovudkastet § 2, stk. 1, at Center for Cybersikkerhed i sin vurdering af en leverandør kan lægge vægt på "*aktører, der udøver kontrol over eller har betydelig indflydelse på leverandøren*". Det er dog uklart, hvad der forstås ved "kontrol" og "betydelig indflydelse". Det er nærliggende at antage, at begrebet må forstås i overensstemmelse med selskabslovens § 7 om "bestemmende indflydelse", men da det ikke er nærmere forklaret i lovbemærkningerne, skal TI henstille til, at dette præciseres.

Det er heller ikke klart for TI, hvilke lande Danmark har indgået sikkerhedsaftaler med, og som dermed i tilstrækkeligt omfang opfylder kriteriet. Dermed er det ikke muligt at vurdere, om en leverandør opfylder kriteriet i § 2, stk. 1, nr. 1. Og eftersom dette kan ændre sig, og Center for Cybersikkerhed får hjemmel til at forbyde opretholdelsen af allerede eksisterende aftaler, er der brug for adgang til en liste, der kontinuerligt opdateres.

Det synes derudover ikke nærmere defineret, hvad der forstås ved begrebet "tilsvarende sikkerhedssamarbejder". Af bemærkningerne til bestemmelsen fremgår således kun:

> *"Bestemmelsen omfatter også tilsvarende sikkerhedssamarbejder, hvor der ikke nødvendigvis er indgået en formel sikkerhedsaftale. Mere indirekte sikkerhedssamarbejder, der f.eks. indgås via internationale organisationer, vil ikke være omfattet af begrebet tilsvarende sikkerhedssamarbejder.*
>
> *En eventuel fastlæggelse, af hvilket land leverandøren, underleverandøren eller aktøren er hjemmehørende i, foretages af Center for Cybersikkerhed efter en konkret vurdering."*

Fraværet af en konkret og brugbar definition sammenholdt med, at kredsen af potentielt omfattede lande fastlægges af Center for Cybersikkerhed fra sag til sag, gør i store træk bestemmelsen uanvendelig som vejledning for såvel teleudbydere som udstyrsleverandører.

Tilsvarende har udbyderne heller ikke indsigt i, hvilke lande det efter lovgivningen er muligt at pålægge leverandører eller deres underleve-

randører at udføre eller deltage i forhold, som vil udgøre spionage eller sabotage. Det er fx uklart, om amerikanske selskaber og underleverandører har forpligtelser i forhold til NSA, og om NSA har aktiviteter i Danmark, som kan karakteriseres som spionage[4].

Der fremgår også af kriterierne i § 2, stk. 1, nr. 2 og 3, at der udover lande, hvor leverandøren er hjemmehørende, også kan lægges vægt på lande, hvor produktionen eller driften varetages fra. Det er uklart, hvad denne sondring indebærer, idet næsten alle leverandører fra vestlige lande, som Danmark formentlig har en aftale om sikkerhedssamarbejde med, har henlagt hele eller dele af deres produktion til ikke-vestlige lande, som Danmark formentlig ikke har en sikkerhedsaftale med. Det er uklart, om teleudbyderne kan indgå aftaler med sådanne leverandører uden risiko.

TI foreslår derfor, at Center for Cybersikkerhed med loven forpligtes til løbende at udarbejde og offentliggøre en oversigt over lande og producenter, som potentielt udgør en trussel mod statens sikkerhed.

Ikke-anonyme afgørelser
Center for Cybersikkerhed kan efter lovudkastet § 14, stk. 1, beslutte at offentliggøre ikke-anonyme afgørelser.

Det fremgår af lovbemærkningerne, at formålet hermed er at udstille de udbydere, der vælger at indgå aftaler med leverandører, der udgør en trussel mod statens sikkerhed.

Henset til, at kriterierne for, hvornår loven kan finde anvendelse, er uklare og uigennemskuelige, er det helt urimeligt, at Center for Cybersikkerhed kan anvende offentliggørelse af en afgørelse som pression. Det gælder særligt i tilfælde, når et forbud er nedlagt efter lovudkastets § 3, hvor udbyderen har indgået en aftale uden, at Center for Cybersikkerhed på forhånd har nedlagt forbud, og hvor der på tidspunktet for aftaleindgåelse ikke forelå omstændigheder, der udgjorde en trussel mod statens sikkerhed.

TI skal derfor opfodre til, at lovudkastets § 14 udgår.

Stand-still periode udvides
Af § 18 i lovudkastet fremgår det, at "Stand still-perioden" i net og informationssikkerhedsloven § 4 udvides fra 10 til 25 arbejdsdage. Isoleret set kan det umiddelbart anses som rimeligt, da en saglig vurdering af et muligt forbud vanskeligt kan gennemføres på 10 arbejdsdage.

Denne forlængelse skal dog ses i lyset af, at teleudbyderne efter net- og informationssikkerhedslovens § 4, nr. 2, 1. punkt, og § 3 i bekendtgørelse om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed skal underrette Center for Cybersikkerhed forud for, at der indledes forhandlinger med en leverandør, og Center

[4] Se fx https://www.dr.dk/nyheder/indland/hemmelige-rapporter-usa-spionerede-mod-danske-ministerier-og-forsvarsindustri

for Cybersikkerhed på den baggrund kan påbyde udbyderen at indsende et færdigt udkast til aftale til centeret. Centeret kender således til aftaleforhandlingerne lang tid før, et færdig udkast til aftale indsendes til centeret.

Der dog ikke i lovgivningen fastsat nogen frist for, hvornår Center for Cybersikkerhed skal give et påbud om at få det færdigt udkast til aftale indsendt.

Teleudbyderen kan således stå i en situation, hvor centeret ikke har reageret på en underretning om opstart af forhandlinger med en leverandør, og udbyderen kan dermed have indrette sine forhandlinger på, at aftalen kan indgås uden anmærkninger fra Center for Cybersikkerhed.

Det vil i en sådan situation være helt urimeligt, hvis centeret har forholdt sig passivt og umiddelbart før aftaleforhandlingernes afslutning kan udstede et påbud om indsendelse af aftalen og tilmed anvende 25 arbejdsdage (5 uger) på at behandle forhold, som med rimelighed kunne være afdækket tidligere i forløbet.

TI skal derfor foreslå, at der i stedet for en forlængelse af fristen i lovens § 4 indsættes en bestemmelse om, at Center for Cybersikkerhed senest 20 arbejdsdage efter, underretning er foretaget, skal træffe afgørelse om i) et færdigt udkast til aftale skal indsendes til Center for Cybersikkerhed, ii) hvilke påtænkte påbud CFCS agter udstede, hvis aftale med leverandøren indgås eller iii) at Center for Cybersikkerhed vil indstille til Forsvarsministeriet, at der skal nedlægges forbud efter leverandørsikkerhedslovens § 2. Såfremt konkrete forhold ikke gør det umuligt for Center for Cybersikkerhed at træffe en afgørelse inden for fristen, kan der gives Center for Cybersikkerhed mulighed for at forlænge fristen med fx 2 gang 10 arbejdsdage.

Med en sådan ordning, vil udbyderen kunne få en vis sikkerhed for, om det kan betale sig at indlede forhandlinger med en leverandør, og såfremt forhandlingerne indledes, kan det endeligt afklares inden for 50 arbejdsdage (20+10+10+10) eller ca. 2 ½ måned, om der udstedes et forbud mod leverandøren.

Der mangler kompenserende initiativer og fælles europæiske koordinering

Som det er anført ovenfor, vil en begrænsning af leverandører på markedet medføre betydelig risiko for, at konkurrencen mindskes på udstyr, hvilket vil medføre øgede omkostninger, mindre innovation og højere priser til kunderne.

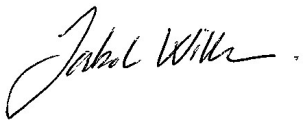
Hvis Folketinget vælger at vedtage lovforslaget, må der politisk tages initiativer til at adressere den manglende konkurrence, som dette utvivlsomt vil medføre, og som kan have langtrækkende betydning for både det danske og det europæiske telemarked. Der kan fx henvises til den Britiske regering, der har været meget bevidst om denne problemstilling og blandt andet har nedsat et udvalg med deltagelse

fra branchen til at vurdere, hvordan man kan få flere leverandører ind på markedet for teleudstyr[5]. Dette kunne fx ske gennem fælles europæisk målrettet stimulering og finansiering af øget forskning på området.

For at sikre gode investeringsvilkår og gode vilkår for konkurrencen, er det også vigtigt, at Danmark ikke går enegang i EU, og at der stiles mod ensartede regler i EU. Med det foreliggende udkast til lov lægges der op til, at Danmark indfører et af de mest restriktive forbudsregimer i EU. TI ser derfor helst, at den danske regering arbejder for en koordineret implementering af de sikkerhedskrav, der indføres i de forskellige EU-lande, jf. EU Kommissionen 5G tool box[6], inden der indføres danske særregler. TI kan dog forstå, at en fælles koordinering ikke kan nås, inden lovens fremsættelse. TI skal derfor opfodre til, at loven ikke bliver mere indgribende, end hvad der er absolut nødvendigt, og at loven tages op til revision om senest 2 år med henblik på en tilpasning i forhold til reglerne i de øvrige EU-lande.

Teleindustrien står naturligvis til rådighed for en eventuel uddybelse af ovenstående høringssvar.

Med venlig hilsen



Jakob Willer
Direktør

[5] https://www.gov.uk/government/publications/5g-supply-chain-diversification-strategy/5g-supply-chain-diversification-strategy

[6] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123