FORSVARSMINISTERIET

DET TALTE ORD GÆLDER

Taleseddel samråd A om NOC i Rumænien

Lad mig starte med at slå fast, at spørgsmålet om cybersikkerhed står højt på regeringens dagsorden. Som dansker skal man leve trygt i visheden om, at de digitale løsninger, som vores velfærdssamfund er afhængigt af, er beskyttet og sikre – også med nye komplekse teknologier som 5G. Regeringen ser telenettet som kritisk infrastruktur og dermed også som et spørgsmål om national sikkerhed. Der må derfor ikke herske tvivl om, at det er et spørgsmål, jeg tager meget alvorligt.

Hvis jeg skal være ærlig, så studsede jeg selv over mediehistorierne tidligere på sommeren om udflytningen af den såkaldte NOC. Og på den baggrund forstår jeg også godt de bekymringer, som blev luftet.

Men historierne, som de først kom ud, var jo ikke korrekte. For eksempel er det ikke rigtigt, at man fra Rumænien får adgang til at lytte med på danskernes samtaler og ser deres sms'er. Eller at myndighederne mister muligheden for at holde øje med sikkerheden.

Derfor er jeg også glad for at få lejlighed til at drøfte dagens samrådsspørgsmål. Og lad mig med det samme understrege, at jeg gerne fortsætter drøftelserne efter samrådet – netop fordi vores allesammens cybersikkerhed er så vigtig.

Jeg vil gerne starte med at afstemme forventningerne til dette samråd. Jeg vil selvfølgelig forsøge at besvare alle spørgsmål fyl-

destgørende, men der er nogle begrænsninger i forhold til, hvilke oplysninger jeg kan give her i dag.

For det første kan jeg ikke komme nærmere ind på forhold, der vedrører indholdet af kontrakten mellem TDC og Ericsson, som er en kommercielt fortrolig aftale mellem to private virksomheder. Jeg vil heller ikke kunne gå i dybden med eventuelle spørgsmål af efterretningsmæssig karakter.

For at besvare spørgsmålet bliver jeg nødt til at blive lidt teknisk i dele af min besvarelse, da der i den offentlige debat desværre har været nogle misforståelser, som jeg vil prøve at udrede her i dag.

Teleudbydere i Danmark, hvoraf TDC er den største, er – ligesom teleudbydere i resten af verden – i gang med at indføre næste generations mobilnetværk: 5G.

I forhold til de tidligere mobilteknologier giver 5G højere hastighed og en meget lav reaktionstid i nettet. Det giver mulighed for nye teknologiske landvindinger som f.eks. robotstyring, fjernstyret diagnosticering i sundhedssektoren, selvkørende biler og det såkaldte Internet-of-Things osv.

Den stigende integration mellem den digitale og den fysiske verden vil i endnu højere grad end det nuværende 4G-netværk gøre 5G mobilnettet til en del af kritisk dansk infrastruktur. Derfor er det i forbindelse med etablering af 5G mere påkrævet end nogensinde at have fokus på både sikkerhed og driftsstabilitet.

I forbindelse med TDC's kontrakt for den fremtidige 5G infrastruktur vil Ericsson få ansvar for at levere alle de komponenter, der indgår i mobilnettet. Derudover vil driftsansvaret for disse dele overgå fra Huawei til Ericsson.

Jeg vil også minde om, at TDC's kommercielle valg af Ericsson som leverandør af 5G blev hilst bredt velkommen her i Folketinget.

I såvel TDC's nuværende opbygning af telenettet som i den kommende opbygning, vil alle de fysiske netværkselementer være placeret i Danmark under TDC's kontrol.

Den del, som flyttes fra Danmark tilbage til Rumænien, er udelukkende det driftscenter, som skal sikre driftsstabiliteten. Og når jeg sagde "tilbage til Rumænien", skyldes det, at driften før 2014 også var outsourcet til Ericssons NOC i Rumænien.

At Huaweis NOC i forhold til TDC var placeret i Danmark skyldtes, at Center for Cybersikkerhed i 2014 – før den nuværende lovgivning var på plads – lavede en frivillig aftale med TDC om dette. Det skyldes ikke mindst, at det dengang vakte en del bekymring, at et kinesisk selskab skulle have driftsansvar for et dansk telenet.

Der er ingen dele af mobilnettets infrastruktur, der nu flyttes ud af Danmark, og som allerede nævnt, så vil der ikke være nogen i Rumænien, der kan lytte med eller kigge i danskernes sms'er.

Hvad er det så, som finder sted i Rumænien: For at sikre at driften af mobilnettet er optimal og stabil - ikke mindst i forbindelse med 5G - benytter teleudbydere i stigende grad specialiserede driftscentre. Det er ikke kun i Danmark, det sker, det er globalt.

Det skyldes, at man i driftscentre kan opbygge avancerede driftsværktøjer og specialistkompetencer, som det ville være både dyrt og vanskeligt for det enkelte teleselskab at bære lokalt.

Alle de tre store leverandører af 5G udstyr (Nokia, Ericsson og Huawei), har således opbygget sådanne specialiserede driftscentre, typisk 3 til 4 centre hver, på globalt plan.

Både Nokia, Huawei og Ericsson har, for at servicere primært de europæiske teleselskaber, alle opbygget et sådant driftscenter netop i Rumænien, hvor der er opbygget et stærkt fagligt miljø.

Herfra har alene Ericsson ansvar for driften for mere end 50 teleselskaber, og mere end 300 mio. abonnenter bliver serviceret fra Ericssons NOC, som har leveret driftsydelser siden 2007. Jeg har ikke kendskab til, at der i den periode skulle have været problemer med hverken sikkerheden eller kvaliteten af opgaveløsningen.

I forhold til TDC skal Ericssons NOC i Rumænien monitorere, optimere og vedligeholde netvæksdelen af TDC's danske mobilnet. Hvis der opstår fejl på et netværkselement, vil centret i Rumænien, på baggrund af alarm-data modtaget fra det danske net, sende en fejlrapport til Ericssons danske organisation, som vil stå for den praktiske fejlretning på nettet i Danmark.

Derudover vil NOC'en med specialiserede værktøjer kunne optimere driften af telenettet i Danmark. Det betyder konkret, at hvis der f.eks. er en spidsbelastning et sted i nettet, kan man sikre, at datatrafikken bliver omdirigeret, eller man kan genstarte udstyr, der af forskellige grunde kan være faldet ud.

Det betyder, at det alene er alarmer og trafikstatistik, der automatisk overføres fra det danske telenet til NOC'en i Rumænien. Der overføres ikke brugerindhold – tale, sms, mail, internetdata mv. til NOC'en.

NOC-medarbejdere kan dog, i forbindelse med optimerings- og fejlretningsopgaver, få midlertidig adgang til data om eksempelvis opkaldstidspunkter og geografisk bevægelsesmønster for kunders udstyr. Men de kan ikke tilgå information, der identificerer den enkelte kunde, altså hvem der bruger nummeret. Og når der bliver givet en sådan midlertidig adgang, bliver det kontrolleret af TDC og logget.

De opgaver, som Ericssons NOC udfører for TDC, er kontraktmæssigt underlagt et stramt sikkerhedsregime. Her er der i vidt omfang taget udgangspunkt i de krav og påbudsmuligheder, som findes i den såkaldte NIS-lov og dens tilhørende bekendtgørelser. Det er den lov, som regulerer informationssikkerheden i telesektoren, og den vender jeg tilbage til.

Selve kontrakten mellem Ericsson og TDC er kommercielt fortrolig, og jeg kan derfor ikke komme nærmere ind på specifikt indhold af kontrakten. Men Center for Cybersikkerhed har oplyst, at centret i dialog med TDC har sikret mulighed for at udføre sikkerhedsbesøg hos TDC's driftsleverandør i Rumænien. Og den mulighed forventer jeg, at de vil benytte sig af.

Og lad mig her til sidst kort nævne den lovgivning, som regulerer området og om CFCS' rolle:

Siden 1. juli 2016 har vi haft NIS-loven, som jo blev vedtaget med et bredt flertal i folketinget. I loven blev der fundet en balance mellem hensynet til sikkerheden på den ene side og hensynet til at kunne finde de bedste og billigste løsninger til gavn for danske forbrugere og virksomheder på den anden side.

Med NIS-loven og dens tilhørende bekendtgørelser fik Center for Cybersikkerhed mulighed for at stille krav til teleselskabernes håndtering af sikkerheden og deres kontrol med eksterne leverandører som feks Ericsson.

Med NIS-loven kan man ikke forhindre en leverandør i at outsource dele af driften til udlandet. Men lovgivningen giver mulighed for at stille sikkerhedsmæssige krav, når en leverandør outsourcer driften.

Det er Center for Cybersikkerheds opfattelse, at den løbende dialog mellem Center for Cybersikkerhed, TDC og Ericsson, har vist, at de to firmaer tager sikkerheden meget alvorligt.

Center for Cybersikkerhed oplyser også, at de derfor er tilstrækkeligt betrygget ved det sikkerhedsregime, der er defineret i forbindelse med udflytning af TDC's NOC til Rumænien.

Jeg kan i øvrigt oplyse, at Center for Cybersikkerhed planlægger et besøg ved Ericssons NOC i september måned. Såfremt besøget giver grundlag for det, kan Center for Cybersikkerhed herefter stille krav om, at TDC udsender sikkerhedsgodkendt personale til NOC'en. Men det må bero på en konkret vurdering.

Lad mig slutte af med at gentage, at jeg udmærket godt forstår de bekymringer, som umiddelbart blev luftet på baggrund af mediehistorierne tidligere på sommeren. Men som sagt er vi jo langt fra de skræmmeforestillinger, som blev fremmanet, om man i Rumænien kunne sidde og lytte med i danskernes samtaler, uden at vores myndigheder kan gøre noget.

De muligheder, vi har for at stille krav til sikkerheden i vores telenet, udspringer af NIS-loven, som et bredt flertal stod bag.

NIS-loven og dens tilhørende bekendtgørelser har nu været i kraft i 3 år, og Forsvarsministeriet lovede i forbindelse med behandlingen af lovforslaget, at der i 2019 ville blive udarbejdet en rapport om erfaringerne med NIS-loven.

Jeg kan oplyse, at det arbejde er i gang, og når det foreligger, vil det være en god lejlighed til, at vi fra politisk side kan drøfte, om der er brug for justering af loven.

Lad mig derfor slutte af med at gentage, at jeg meget gerne fortsætter drøftelserne efter dette samråd, netop fordi vores alle sammens cybersikkerhed er så vigtig.