

Landsrettens begrundelse og resultat

1. Sagens baggrund og hovedproblemstillinger

Sagen angår i første række en prøvelse af CFCS's afgørelse af 21. marts 2023 over for TDC om forbud efter telesikkerhedslovens § 3, stk. 1, 1. pkt., mod fra den 31. december 2026 at opretholde "Amendment 4" indgået mellem TDC og Huawei, samt forbud efter telesikkerhedslovens § 3, stk. 2, 1. pkt., mod fra den 1. januar 2027 at anvende de kritiske netkomponenter, systemer og værktøjer, der er leveret i henhold til "Amendment 4".

Der er mellem parterne enighed om, at det udstyr og komponenter mv., Huawei har leveret i henhold til "Amendment 4" til TDC's DWDM-netværk, opfylder den legale definition i telesikkerhedslovens § 1, nr. 1, for netkomponenter, systemer og værktøjer. Endvidere er der mellem parterne enighed om, at TDC opfylder den legale definition som en væsentlig, erhvervsmæssig udbyder af offentligt tilgængelige elektroniske kommunikationsnet og -tjenester, jf. telesikkerhedslovens § 1, nr. 3, litra a) og b).

Huawei har i henhold til rammeaftalen med TDC fra 2011 ("Master Agreement") løbende leveret udstyr og komponenter mv. til TDC's DWDM-netværk. Der er mellem parterne endvidere enighed om, at det ikke er praktisk muligt at adskille det udstyr og de komponenter mv., der er leveret i henhold til "Amendment 4" fra det udstyr og komponenter mv., der er leveret i henhold til tidligere aftaler), hvorfor det som følge af de ved afgørelsen af 21. marts 2023 nedlagte forbud er nødvendigt for TDC at foretage en total udskiftning af hele det af Huawei leverede DWDM-netværk.

TDC har gjort gældende at have været nødsaget til at efterleve afgørelsen af 21. marts 2023. Selskabet har derfor ikke gjort gældende, at afgørelsen af 21. marts 2023 er ugyldig og skal ophæves, men derimod gjort gældende, at afgørelsen ikke har fornøden hjemmel i telesikkerhedsloven og dermed er ulovlig. Det er herudover gjort gældende, at afgørelsen desuden er væsentlig mangelfuld og retsstridig, hvorfor CFCS ifølge TDC samlet set – uanset at afgørelsen ikke skal ophæves som ugyldig – har pådraget sig et erstatningsansvar over for TDC. Sagen angår i givet fald størrelsen af et sådant erstatningskrav.

I modsat fald angår sagen i anden række, om afgørelsen da er udtryk for ekspropriation over for TDC. Sagens sidste hovedspørgsmål er i bekræftende fald opgørelsen af ekspropriationserstatningen.

Herudover har CFCS gjort gældende, at TDC's påstand 2 skal afvises, ligesom sagen giver anledning til spørgsmål om den særlige advokats påstand på vegne af TDC, jf. straks nedenfor.

2. TDC's påstand 2 og den særlige advokats påstand

2.1. TDC's påstand 2

CFCS har gjort gældende, at TDC's påstand 2 skal afvises, idet påstanden efter sin formulering reelt er et anbringende til støtte for de øvrige påstande.

Efter ordlyden af påstand 2 og dennes sammenhæng med formuleringen af påstand 1 og 3 og de fremsatte anbringender, navnlig angående spørgsmålet om hjemmel, jf. nedenfor, finder landsretten, at påstand 2 reelt er et anbringende til støtte for påstand 1, hvorfor påstand 2 ikke er egnet til at indgå i en domskonklusion.

TDC's påstand 2 afvises derfor.

2.2. Den særlige advokats påstand

Som anført ovenfor har TDC under sagens åbne del eksplicit og flere steder i påstandsdokumentet anført, at det ikke gøres gældende, at afgørelsen af 21. marts 2023 er ugyldig og skal ophæves, idet TDC har efterlevet afgørelsen. Derimod er det gjort gældende bl.a., at afgørelsen ikke har fornøden hjemmel i telesikkerhedsloven og dermed er ulovlig, på hvilken baggrund der kræves erstatning. Landsretten lægger til grund, at valget af påstande er nøje overvejet af TDC og selskabets advokater.

Også efter at spørgsmålet har været rejst af landsretten i et retsmøde forud for hovedforhandlingen i sagens lukkede del, har den særlige advokat på vegne af TDC nedlagt endelig subsidær påstand om ophævelse af afgørelsen.

Det fremgår af forarbejderne til telesikkerhedsloven, de specielle bemærkninger til § 8, stk. 2, at den særlige advokat vil udøve partsbeføjelser på vegne af parten med hensyn til de fortrolige oplysninger, men ikke i øvrigt vil være part eller partsrepræsentant i sagen. Videre fremgår det, at den særlige advokat ikke vil optræde på vegne af parten, i det omfang parten sammen med sin advokat vil kunne udøve sædvanlige civilprocessuelle partsbeføjelser, herunder med hensyn til oplysninger, som vil være videregivet til parten og fremlagt i retten.

Endvidere fremgår det af de specielle bemærkninger til § 9, stk. 1, at den særlige advokat ikke må udtale sig i retsmøder, hvor parten eller dennes advokat er til stede, når de fortrolige oplysninger er videregivet til den særlige advokat, hvilket ifølge forarbejderne også stemmer med, at parten og dennes advokat i videst muligt omfang varetager sædvanlige civilprocessuelle partsbeføjelser i sagen.

Idet den påstand, den særlige advokat har nedlagt under sagen, ikke kan indeholdes i – men er i modstrid med – de påstande og anbringender, TDC's advokater under sagens åbne del har nedlagt, finder landsretten, at den påstand, der

er nedlagt af den særlige advokat, uanset at den er subsidær til de øvrige påstande, ligger ud over de civilprocessuelle partsbeføjelser, han er tillagt, hvorfor den særlige advokats påstand afvises.

3. CFCS' afgørelse af 21. marts 2023 efter telesikkerhedslovens § 3

3.1. TDC's hovedindsigelse mod afgørelsen

TDC har gjort gældende navnlig, at afgørelsen af 21. marts 2023 ikke har hjemmel i telesikkerhedslovens ikrafttrædelsesbestemmelser (overgangsregler), hvorfor forbuddene i afgørelsen er nedlagt uden fornøden hjemmel, jf. nærmere afsnit 3.2. nedenfor.

Herudover har TDC gjort gældende navnlig, at afgørelsens begrundelse er mangelfuld og misvisende, jf. nærmere afsnit 3.3. nedenfor. Herunder har TDC anfægtet, at CFCS i afgørelsen har lagt vægt på den manglende testning i HC-SEC, Huawei's manglende udlevering af fuld kildekode, og at CFCS lagde vægt på bekymring i forhold til det af Huawei leverede og idriftsatte hardware og software, jf. nærmere afsnit 3.3.1. nedenfor.

Det er videre gjort gældende, at afgørelsen er uproportional, jf. nærmere afsnit 3.3.2. nedenfor, og at der ikke foreligger "særlige tilfælde", jf. telesikkerhedslovens § 3, stk. 1, ligesom der ikke var tale om, at der på afgørelsestidspunktet forelå forhold, som udgjorde "en væsentlig trussel mod statens sikkerhed" i bestemmelsens forstand, jf. nærmere afsnit 3.3.3 nedenfor. Endvidere er der gjort en række yderligere indsigelser gældende, jf. nedenfor, afsnit 3.3.4.

Endelig er det gjort gældende, at der ikke har været grund til at nedlægge forbuddet mod anvendelse af NCE-T styresystemet i radiokædenetværket, da dette ikke er en del af den kritiske teleinfrastruktur, jf. nedenfor, afsnit 3.3.5.

3.2. TDC's indsigelse angående telesikkerhedslovens ikrafttrædelsesbestemmelse

Det fremgår af telesikkerhedslovens § 17, stk. 1, at loven træder i kraft den 1. juli 2021. Af bestemmelsens stk. 2, fremgår dog, at bl.a. lovens § 3 allerede har virkning for aftaler, der er indgået den 7. december 2020 eller senere. Det følger endelig af § 17, stk. 3, at bl.a. lovens § 3 først har virkning for aftaler, der er indgået før den 7. december 2020, fra den 1. januar 2026.

Det er altså af betydning for, hvorvidt forbuddene efter telesikkerhedslovens § 3, kunne nedlægges ved afgørelsen af 21. marts 2023, hvornår "Amendment 4" må anses for indgået.

TDC har i første række gjort gældende, at "Amendment 4" alene er en forlængelse af den allerede bestående rammeaftale ("Master Agreement") fra 2011 eller forligsaftalen fra 2019, hvorfor aftalen må anses for indgået længe før den 7.

december 2020. Det er herunder gjort gældende, at "Amendment 4" i alt væsentlighed alene forlængede den eksisterende aftale på uændrede vilkår.

Herom bemærker landsretten, at det fremgår af TDC's anmeldelse af 15. september 2020 til CFCS af genforhandling af DWDM-aftalen, at TDC's aftale med Huawei oprindeligt blev indgået i 2011, blev forlænget i 2016 og ville udløbe i 2021. Tilsvarende fremgår det af "Amendment to Agreement" underskrevet af TDC og Huawei den 1. juni 2018, at rammeaftalen fra 2011 ("Master Agreement"), "Supply Agreement" og "Support Agreement" kun ville være i kraft indtil 31. december 2021.

Landsretten lægger således til grund, at rammeaftalen mellem TDC og Huawei og de dertil knyttede "Supply Agreement" og "Support Agreement" ville udløbe og bortfalde ved udgangen af 2021, såfremt der ikke forinden blev indgået aftale om forlængelse som sket med "Amendment 4".

På denne baggrund, og henset til indholdet af "Amendment 4", som også indeholdt flere nye og ændrede vilkår i forhold til parternes hidtidige aftalegrundlag, og dermed havde selvstændig karakter, finder landsretten, at "Amendment 4" ikke kan anses for indgået allerede ved rammeaftalen fra 2011, forlængelsen af rammeaftalen fra 2018 eller forligsaftalen fra 2019.

I anden række har TDC gjort gældende, at "Amendment 4" aftaleretligt må anses for indgået forud for den 30. november 2020, hvor CFCS i medfør af § 5 i bekendtgørelse nr. 1256 af 27. november 2019 om oplysnings- og underretningspligter vedrørende net- og informationssikkerhed udstedte påbud til TDC om at fremsende de endelige udkast til aftaler med Huawei og gjorde opmærksom på, at aftalen først kunne indgås, når CFCS havde givet tilbagemelding herpå. Herunder har TDC gjort gældende, at "Amendment 4" må anses for indgået den 5. november 2020, hvor TDC's bestyrelse godkendte aftalen, der forinden havde været genstand for forhandlinger mellem TDC og Huawei.

Landsretten bemærker herom, at det af pkt. 16 i rammeaftalen fra 2011 mellem TDC og Huawei fremgår, at enhver tilføjelse til eller ændring i parternes aftale skulle ske skriftligt ved underskrift fra de respektive behørigt bemyndigede repræsentanter for hver af parterne. Det er efter bevisførelsen ikke godtgjort, at dette krav om skriftlighed og underskrift er fraveget mellem parterne. Parternes vedtagelse af "Amendment 1" fra august 2011, "Amendment to Agreement" fra juni 2018, "Accession Agreement" fra december 2018 og "Settlement Agreement" (forligsaften) fra oktober 2019, der alle er både skriftlige og underskrevet af parterne, understøtter derimod, at parterne praktiserede og i alle tilfælde overholdt kravet om skriftlighed.

At både TDC og Huawei anså underskrift af aftalen som nødvendig, er endvidere understøttet af mailen af 27. november 2020 fra TDC til Huawei, hvor aftaledokumenterne blev sendt frem, og det blev anført, at der snart kunne iværksættes underskriftsprocedure.

Det er ubestridt, at TDC underskrev "Amendment 4" den 7. december 2020, hvilket var samme dag som CFCS havde givet en tilbagemelding vedrørende TDC's fremsendelse af endeligt aftaleudkast den 30. november 2020.

På denne baggrund finder landsretten, at "Amendment 4" i overensstemmelse med dateringen af aftalen, blev indgået den 7. december 2020.

Ud over det anførte om skriftlighedskravet i parternes aftaleforhold er der tillige lagt vægt på, at det ikke er godtgjort, at den viljeserklæring, som bestyrelsens beslutning af 5. november 2020 måtte være udtryk for, blev afgivet til eller kom frem til Huawei på noget tidligere tidspunkt end ved underskriften af aftalen den 7. december 2020.

Da "Amendment 4" således blev indgået den 7. december 2020, finder telesikkerhedslovens § 17, stk. 2, om aftaler, der er indgået den 7. december 2020 eller senere anvendelse, hvorfor CFCS havde hjemmel til i medfør af lovens § 3 at nedlægge de i sagen omhandlede forbud ved afgørelsen af 21. marts 2023.

3.3. Afgørelsens begrundelse angående anvendelse af telesikkerhedslovens § 3

3.3.1. Testning ved HCSEC, fuld kildekode og binær ækvivalens

3.3.1.1. Aftaler mv. mellem CFCS, TDC og Huawei

Landsretten lægger efter bevisførelsen til grund, at der siden indgåelsen af Rammeaftalen fra 2011 mellem TDC og Huawei og de tilhørende "Supply Agreement" og "Support Agreement" i maj 2011 i varierende omfang har været en løbende dialog mellem på den ene side CFCS og forud herfor Forsvarsministeriet, og på den anden side TDC angående TDC's leverandørforhold til Huawei. Denne dialog har dels manifesteret sig i udarbejdelse af "Skriftlig forståelse nr. 1" fra februar 2013 og "Skriftlig forståelse nr. 2" af 11. september 2013 og dels af løbende møder, herunder et møde i november 2014 og løbende "kvar-talsmøder", i hvert fald fra foråret 2017. Der har endvidere været fremlagt et udkast til "Skriftlig forståelse nr. 3" fra november 2019, som CFCS og TDC imidlertid aldrig opnåede enighed om. Landsretten lægger dog til grund, at parterne havde forhandlet herom længe, og at indholdet af udkastet i vidt omfang var udtryk for parternes standpunkter på daværende tidspunkt.

Herudover har der været en dialog mellem CFCS og Huawei i hvert fald i form af disse parter "Fælles forståelse" af 24. april 2012. Videre har der været fremlagt en række aftaler mellem TDC og Huawei, navnlig Rammeaftalen fra 2011 og de efterfølgende forlængelser, "Amendments", ligesom landsretten lægger

til grund, at der som følge af det tætte forretningsmæssige forhold mellem TDC og Huawei har været en løbende kontakt mellem disse parter.

Endelig har der i hvert fald i et enkelt tilfælde, den 10. december 2015, været afholdt et møde med deltagelse af repræsentanter fra CFCS, TDC og Huawei, hvorfra der foreligger et dokument af 11. december 2015 med et skema med en "Fælles status vedrørende efterlevelse af de 16 punkter i den fælles forståelse". Landsretten lægger efter ordlyden af dette dokument til grund, at de punkter, der blev drøftet på mødet, og som er gengivet i skemaet, er de forhold, der fremgår af den mellem CFCS og Huawei indgåede "Fælles forståelse" af 24. april 2012. Uanset, at det efter forklaringen fra [redacted] må lægges til grund, at TDC på daværende tidspunkt ikke var bekendt med, at det anførte i skemaet rent faktisk var "Fælles forståelse" mellem CFCS og Huawei, blev TDC dog i forbindelse med mødet bekendt med indholdet heraf.

Det fremgår af pkt. 33 i Rammeaftalen mellem TDC og Huawei fra 2011, at der skulle oprettes og igennem hele kontraktens levetid opretholdes en enhed til at teste Huaweis produkter ("Testing, Verification and Certification Cell") svarende til det, der var oprettet i Storbritannien, altså HCSEC. Manglende efterlevelse af dette ville blive betragtet som et kontraktbrud, der berettigede TDC til at hæve kontrakten.

Ved "Fælles forståelse" mellem Forsvarsministeriet og Huawei fra 2012 blev det aftalt, at HCSEC som "celle" skulle varetage en risikobegrænsende funktion for teleudbyderen på det danske marked og for den danske stat. Videre fremgår det heraf, at Huawei var forpligtet til at udlevere komplet hardware- og software-redesigninformation, herunder komplet kildekode mv., til HCSEC med henblik på, at der kunne kompileres eksekverbar kode. Videre fremgår det af den fælles forståelse, at HCSEC skulle foretage sikkerhedsvurdering af opdateringer til software, hardware og firmware mv., som blev leveret og implementeret i teleudbyderens danske net. Herved skulle der foretages en analyse, der kunne verificere, at enhver form for formodet ændring i software, firmware eller hardware skyldtes kundekrav og/eller produktudviklingskrav, og at de pågældende ændringer ikke utilsigtet eller bevidst forringede systemsikkerheden, og at dette kunne verificeres ud fra kildekoden. Endvidere skulle der på baggrund af analysen ud fra kildekoden genereres en komplet installerbar systemsoftware (et "image") på betroet udstyr hos HCSEC, som svarede til det, der var på Huawei-leveret udstyr. Der skulle også leveres en kopi af nævnte "image" til TDC.

I "Skriftlig forståelse nr. 1" fra foråret 2013, indgået mellem CFCS og TDC, blev det i pkt. 2 aftalt, at TDC ville sikre, at udstyr og software fra Huawei, der forventedes benyttet i TDC's net, blev verificeret af cellen, altså af HCSEC.

CFCS og TDC aftalte ved pkt. 16. i "Skriftlig forståelse nr. 2" fra efteråret 2013, der supplerede "Skriftlig forståelse nr. 1", men primært angik udstyr til telenetværket ("RAN-udstyr"), at TDC skulle sikre, at selskabets kontrakter med Huawei understøttede den skriftlige forståelse, og at det i kontrakterne skulle fastslås, at Huawei var forpligtet til at sikre, at HCSEC til enhver tid rådede over den fornødne kapacitet. Det blev dog også aftalt, at såfremt Huawei var afskåret fra at indrette HCSEC til at sikre efterlevelse af den skriftlige forståelse, kunne der anvendes en anden tilsvarende sikkerhedsfacilitet, der var godkendt af CFCS. Videre blev det i pkt. 6. aftalt, at RAN-udstyr leveret til TDC skulle valideres af HCSEC, herunder i form af typegodkendelse af hardware og verifikation af softwareopdateringer. Der blev i samme punkt aftalt en procedure for verifikation i tilfælde af større kritiske fejlsituationer.

Ved fremsendelsen af "Skriftlig forståelse nr. 2" den 13. september 2013 tilkendegav CFCS bl.a., at den godkendelsesprocedure for udstyr, komponenter og software, der var vedtaget i pkt. 6 i "Skriftlig forståelse nr. 2", også kunne gælde for det, der var omfattet af "Skriftlig forståelse nr. 1". Det samme gjorde sig gældende for bl.a. pkt. 16 i "Skriftlig forståelse nr. 1".

Af "Amendment" til rammeaftalen fra 2011, underskrevet af TDC og Huawei den 1. juni 2018, hvorved der skete en forlængelse af rammeaftalen, "Supply Agreement" og "Support Agreement" frem til udgangen af 2021, fremgår det bl.a., at en langsigtet aftale med de danske cybersikkerhedsmyndigheder, altså CFCS, var under forhandling, og at parterne forpligtede sig til at overholde ("comply") den aftale, der måtte blive indgået. Indtil da forpligtede Huawei sig til at overholde sin forpligtelse til at levere relevant testning ved HCSEC, såfremt produktet skulle leveres til det engelske marked. For andre produkter ville Huawei i henhold til aftalen sikre tests ved en anden godkendt testenhed.

Landsretten lægger derfor til grund, at det mellem TDC og Huawei, mellem CFCS og Huawei og mellem CFCS og TDC var aftalt, at der skulle ske testning af udstyr og software i HCSEC, at det mellem CFCS og Huawei var aftalt, at Huawei var forpligtet til at udlevere fuld kildekode mv. til HCSEC, og at det mellem CFCS og TDC var aftalt, at der alene kunne ske fravigelse af testning ved HCSEC, såfremt CFCS godkendte den alternative sikkerhedsfacilitet.

3.3.1.2. Ændrede forhold i 2019 og 2020

Efter bevisførelsen lægger landsretten til grund, at der fra 2019 forelå en ny situation som følge af, at den amerikanske regering i foråret 2019 fjøede Huawei til den såkaldte "Entity List", hvilket indebar, at Huaweis muligheder for at anvende amerikanske produkter, software og teknologi blev stærkt begrænsede. Som det fremgår af det materiale, TDC præsenterede på kvartalsmødet med CFCS den 28. oktober 2019, ville Huawei overgå fra at anvende det tidligere U2000-management system til DWDM-netværket, der også indeholdt ameri-

kanske komponenter, til et kinesisk produceret managementsystem, NCE-T, som udelukkende bestod af kinesiske komponenter, og som i det hele var udviklet af Huawei. Af samme præsentationsmateriale fremgår videre, at "compliance" ikke var mulig som følge af, at testning i HCSEC ikke var tilgængelig eller kun i meget begrænset omfang.

Det fremgår af materialet til kvartalsmødet mellem CFCS og TDC den 26. maj 2020, at der ikke var foretaget systemtest i HCSEC, men at der var planlagt en systemtest i sidste kvartal af 2020. Dette fremgår ligeledes af CFCS' interne referat af 29. maj 2020, som C under sin vidneforklaring bekræftede rigtigheden af. Imidlertid fremgår det af præsentationsmaterialet fra kvartalsmødet den 15. marts 2021 sammenholdt med CFCS' interne referat fra mødet af 6. december 2021, at der ikke var sket testning i HCSEC som forudsat.

Landsretten finder, at der herefter, hvor TDC gik fra at anvende et management system til DWDM-netværket, der havde været testet i HCSEC, og som bestod af en blandet "stack", til en ren kinesisk produceret "stack", samtidig med at der ikke blev foretaget systemsikkerhedsevalueringer i HCSEC, og hvor kravet om udlevering af fuld kildekode ikke blev overholdt, bestod en helt ny sikkerhedsmæssig situation, som indebar en markant øget risiko for sårbarheder i systemet.

Videre lægger landsretten vægt på, at det fremgår af konklusionerne fra den årlige rapport for 2019 fra HCSEC Oversight Board, der på vegne af de britiske myndigheder førte tilsyn med arbejdet i HCSEC, at Oversight Board kun i begrænset omfang kunne forsikre, at truslerne mod den britiske nationale sikkerhed som følge af Huaweis involvering i den britiske kritiske teleinfrastruktur kunne mitigeres i tilstrækkeligt omfang på lang sigt. Denne konklusion blev gentaget i rapporten fra 2020. Tilsvarende fremgår det af konklusionerne fra HCSEC Oversight Boards rapport fra 2021, at man i løbet af året var blevet ved med at finde forhold, der indikerede, at der ikke var sket nogen overordnet forbedring af kvaliteten af software eller cybersikkerhed.

3.3.1.3. Binær ækvivalens

Den 11. maj 2021 afholdtes et møde mellem TDC og CFCS, der angik bl.a. TDC's risikovurdering, en alternativ testplan og en tidsplan for udskiftning af Huawei DWDM-udstyr til en anden leverandør. Af opfølgningen den 12. maj 2021 på mødet, fremgår bl.a., at CFCS stillede som et krav, at TDC ved udarbejdelsen af risikovurderingen skulle sikre sig, at de sikkerhedsmæssige problemer med dårlig kodekvalitet og sikring af binær ækvivalens, som HCSEC Oversight Board havde beskrevet siden 2017, blev inddraget i risikovurderingen.

Landsretten finder, at også kravet om sikring af binær ækvivalens lå inden for rammerne af, hvad Huawei ved indgåelsen af "Fælles forståelse" i 2012 over for

CFCS havde forpligtet sig til at sikre, hvilke krav som nævnt havde været genstand for drøftelse under det fælles møde mellem CFCS, TDC og Huawei i 2015, ligesom kravet lå inden for rammerne af, hvad Huawei over for TDC havde forpligtet sig til at sikre.

3.3.1.4. Testning ved HCSEC

Det lægges efter bevisførelsen, herunder forklaringerne fra [A] [B] [C] [D], [E] og [F] til grund, at der som følge af, at HCSEC var oprettet på foranledning af britiske myndigheder og Huawei med det formål at teste Huawei produkter til det engelske marked, i hvert fald i slutningen af perioden frem mod 2020, kun i mindre omfang skete testning i HCSEC af produkter, som skulle leveres af Huawei til TDC. Det lægges således til grund, at der i tiltagende grad ikke skete testning i HCSEC som forudsat og ønsket af både TDC og CFCS.

Videre må det efter bevisførelsen, herunder de fremlagte referater fra navnlig kvartalsmøderne mellem TDC og CFCS, udkastet til "Skriftlig forståelse nr. 3" og vidneforklaringerne fra [A] [B], [C] [D] og til dels [F] og [G] lægges til grund, at TDC løbende, herunder under kvartalsmøderne, kontinuerligt gav udtryk for et ønske om, at der kunne ske testning af udstyr og komponenter mv. ved andre aktører end HCSEC.

Det må endvidere efter samme bevisførelse lægges til grund, at der i et vist omfang faktisk skete testning af udstyr og komponenter mv. ved private leverandører, herunder Atsec, hvilket CFCS i hvert fald i enkelte tilfælde havde accepteret. [G] har endvidere forklaret, at der var patches til software, der ikke blev testet, fordi det skulle gå hurtigt. CFCS var derfor nødt til at acceptere, at der skete tests hos Atsec, fordi systemet potentielt kunne gå ned eller blive ustabil, hvis patchen ikke blev installeret. Hensynet til forsyningssikkerheden gjorde altså, at CFCS blev nødt til at leve med, at der ikke skete godkendelse af alle patches. Landsretten lægger derfor til grund, at i hvert fald en del af de tests, der skete hos Atsec, var tests i henhold til pkt. 6. b. – e. i "Skriftlig forståelse nr. 2", hvorefter TDC kunne få foretaget tests andre steder end i HCSEC i tilfælde af fejlretning mv. af større, kritiske fejlsituationer, og hvor man af tidsmæssige årsager ikke kunne afvente testning i HCSEC.

Efter bevisførelsen, herunder forklaringen fra [C] lægger landsretten endvidere til grund, at der kun skete tests af enkelte dele hos Atsec, der således ikke foretog systemsikkerhedsevalueringer.

Uanset, at der således i et vist omfang skete testning hos Atsec, er det hverken dokumenteret eller sandsynliggjort, at CFCS på noget tidspunkt må anses for at

have accepteret, at kravet om testning ved HCSEC generelt set var fraveget, og i alle tilfælde ikke, at der kunne ske systemsikkerhedsevalueringer hos andre end HCSEC.

Dette er understøttet af udkastet til "Skriftlig forståelse nr. 3", hvoraf det fremgår af udkastet til pkt. 6.a., at der var en afgørende sondring mellem sikkerhedsevalueringer og systemsikkerhedsevalueringer, hvoraf sidstnævnte kun kunne foretages af HCSEC, medmindre andet var aftalt med CFCS. Landsretten lægger til grund, at dette var udtryk for CFCS' standpunkt på tidspunktet for udarbejdelsen af udkastet.

Den omstændighed, at CFCS som beskrevet i nogle tilfælde accepterede testning af enkelte dele af udstyr og komponenter mv. ved private leverandører som et alternativ til testning i HCSEC, konstituerer således hverken forvaltningsretligt eller aftaleretligt en bindende praksis eller fravigelse af det aftalte om testning i HCSEC.

Efter bevisførelsen, herunder det anførte i Oversight Board rapporter og forklaringen fra [redacted] F [redacted] G [redacted] og til dels [redacted] D [redacted], lægger landsretten til grund, at HCSEC besad unikke kompetencer i forhold til testning af udstyr, komponenter mv. fra Huawei, som andre testleverandører ikke kunne levere, og at det derfor var sagligt, at CFCS i videst muligt omfang fastholdt testning i HCSEC.

Det kan efter landsrettens opfattelse ikke tillægges afgørende betydning, at CFCS ved at opretholde de ovenfor beskrevne aftalte og meddelte krav om testning i HCSEC og udlevering af kildekode mv. fastholdt krav til TDC, der de facto var umulige for TDC at overholde. Landsretten lægger herved vægt på, at kravene som nævnt på intet tidspunkt havde været frafaldet, at kravene var saglige i relation til varetagelsen af formålet om beskyttelse af risici mod statens sikkerhed, og at ansvaret for overholdelsen af kravene efter de indgåede aftaler i sidste ende påhvilede TDC.

3.3.1.5. *Sammenfattende om testning ved HCSEC, fuld kildekode og binær ækvivalens*

På ovenstående baggrund finder landsretten, at CFCS ved afgørelsen af 21. marts 2023 angående testning i HCSEC, adgang til fuld kildekode mv. og binær ækvivalens har lagt vægt på et korrekt faktum, forfulgt et sagligt formål og med rette tillagt forholdene betydning ved sagens afgørelse.

3.3.2. *Proportionalitet*

Af telesikkerhedslovens § 3, stk. 4, følger, at CFCS kun kan nedlægge forbud efter stk. 1 og 2, hvis hensynet til statens sikkerhed ikke effektivt kan varetages ved mindre indgribende foranstaltninger. Der skal altså – i overensstemmelse med det i forvaltningsretten almindeligt gældende proportionalitetsprincip, jf.

herved også lovens forarbejder, de specielle bemærkninger til § 3, stk. 4 – foretages en proportionalitetsafvejning af, om formålet med forbuddet ville kunne være nået ved mindre indgribende foranstaltninger end et forbud.

Videre følger det samme sted af lovens forarbejder, at det er en forudsætning for at træffe afgørelse efter § 3, stk. 1, og 2, at CFCS har forsøgt at rådgive teleudbyderen om de tilpasninger af aftalen eller de sikkerhedsmæssige ændringer af kritiske komponenter, systemer mv., som vil være nødvendige, for at der ikke længere vurderes at være en væsentlig trussel mod statens sikkerhed, ligesom CFCS også skal have overvejet de relevante muligheder i lov om sikkerhed i net og tjenester, herunder eksempelvis muligheden for at give påbud om, at teleudbyderen skal foretage konkrete sikkerhedsforanstaltninger.

Som beskrevet ovenfor lægges det til grund, at der igennem hele den periode, hvor der bestod et kontraktforhold mellem TDC og Huawei, var løbende kontakt mellem CFCS og TDC, som "Skriftlig forståelse nr. 1 og 2", kvartalsmøderne, tilbagemeldingerne mv. er udtryk for. Det lægges videre til grund, at CFCS i den kontakt løbende rådgav TDC om aftalegrundlaget med Huawei og de sikkerhedsmæssige aspekter af kritiske komponenter, systemer mv., som CFCS vurderede nødvendige. Herunder lægger landsretten til grund, at CFCS vejledte og havde dialog med TDC om selskabets mulighed for, med hjemmel i pkt. 33 i Rammeaftalen mellem TDC og Huawei fra 2011, at ophæve kontrakten.

Videre må det lægges til grund, at formålet med afgørelsen af 21. marts 2023 ikke kunne være opnået ved afgørelser efter anden lovgivning, herunder lov om sikkerhed i net og tjenester, hvor der ikke var hjemmel til at nedlægge forbud mod indgåede aftaler eller levering af udstyr.

Landsretten lægger tillige vægt på, at CFCS ved tilbagemeldingen til TDC allerede den 7. december 2020 havde anbefalet TDC at afslutte leverandørforholdet med Huawei, og at der efterfølgende var en omfattende dialog herom, men uden at det førte til en løsning, der imødekom de forhold om trusler mod statens sikkerhed, som bl.a. førte til den senere afgørelse af 21. marts 2023.

Endvidere lægger landsretten vægt på, at CFCS torsdag den 2. december 2021 indkaldte den øverste ledelse i TDC i form af både CEO L og bestyrelsesformand M til et møde mandag den 6. december 2021. Ifølge afsenderen af indkaldelsen, F var det CFCS' vurdering, at sagens alvor nødvendiggjorde, at man involverede den øverste ledelse i TDC. Mødet med disse personer blev imidlertid ikke afholdt, idet der i stedet for blev afholdt et møde den 14. december 2021, hvor senior vice president Q og bestyrelsesmedlem N deltog fra TDC's side.

Landsretten finder på denne baggrund, at CFCS i fornødent omfang – og på flere niveauer af TDC's organisation – havde forsøgt at rådgive TDC om de tilpasninger af aftalen og de sikkerhedsmæssige ændringer af kritiske komponenter, systemer mv., som vil være nødvendige, for at der ikke længere vurderes at foreligge en væsentlig trussel mod statens sikkerhed.

Derfor finder landsretten samlet set, at formålet med forbuddet ikke ville kunne være nået ved mindre indgribende foranstaltninger end et forbud, og at betingelsen i telesikkerhedslovens § 3, stk. 4, derfor er opfyldt.

3.3.3. *"Særlige tilfælde" og "en væsentlig trussel mod statens sikkerhed"*

3.3.3.1. *Det retlige grundlag*

Det fremgår af forarbejderne til telesikkerhedsloven, de almindelige bemærkninger, pkt. 4.1., at retten til kontradiktion og princippet om parternes ligestilling, er fundamentale bestanddele af retten til en retfærdig rettergang i artikel 6, stk. 1, i Den Europæiske Menneskerettighedskonvention, men at rettighederne imidlertid ikke er absolutte, hvilket også gør sig gældende for adgangen til sagens materiale. Konventionsstaterne har således ifølge forarbejderne en skønsmargin ved begrænsningen af disse rettigheder, og modstridende interesser, såsom statens sikkerhed mv., skal vejes op imod partens rettigheder. Der er i den forbindelse tale om en helhedsvurdering af sagens samlede omstændigheder. Der vil dog alene kunne ske begrænsninger i rettigheder, som ikke berører kernen ("the very essence") af rettighederne i artikel 6, stk. 1.

Videre fremgår det samme steds af forarbejderne, at de særlige regler for domstolsbehandlingen, som foreslås i §§ 7- 13, med de nødvendige tilpasninger svarer til reglerne om domstolsbehandling i kapitel 7 b og i udlændingeloven og § 8 F i lov om dansk indfødsret og varetager hensynet til, at fortrolige og sikkerhedsmæssige oplysninger ikke prigsives i forbindelse med en eventuel domstolsbehandling af en afgørelse om nedlæggelse af forbud. Samtidig sikres det, at alle sagens oplysninger som udgangspunkt fremlægges for retten, ligesom den pågældende part beskikkes en særlig advokat til at varetage sine interesser i forhold til det materiale, der af sikkerhedsmæssige grunde vurderes ikke at kunne videregives til den pågældende. Noget tilsvarende om lovens ordning fremgår af de specielle bemærkninger til lovens § 7.

Af U 2011.2673 H og U 2011.2695 H, der begge angik prøvelser af afgørelser om udvisning af udlændinge, som var til fare for statens sikkerhed, og som i henhold til den dagældende udlændingelovs kapitel 7 b, blev behandlet under en åben og en lukket del, fremgår, at formålet med den særlige domstolsbehandling er at skabe en balance mellem på den ene side behovet for hemmeligholdelse af oplysninger af sikkerhedsmæssige grunde og på den anden side hensynet til, at der er en reel mulighed for effektiv varetagelse af udlændingens inter-

esser under sagen. En sådan opdeling i en lukket og åben del var ikke i strid med den europæiske menneskerettighedskonvention, jf. U 2010.2910 H.

Det fremgår af telesikkerhedslovens § 3, stk. 1 og 2, at det er en forudsætning for at nedlægge forbud i henhold til bestemmelsen, at der er tale om "særlige tilfælde", og at der kun kan nedlægges forbud, hvis videreførelse af en aftale, der vedrører kritiske netkomponenter, systemer og værktøjer, herunder varetagelsen af driften heraf (stk. 1), henholdsvis anvendelse af netkomponenter, systemer og værktøjer mv. leveret i henhold til aftalen (stk. 2), udgør "en væsentlig trussel mod statens sikkerhed".

Ved vurderingen heraf kan Center for Cybersikkerhed i henhold til § 3, stk. 1, sidste pkt., og § 3, stk. 2, sidste pkt., lægge vægt på bl.a. de fire momenter, der er nævnt i lovens § 2, stk. 2, nr. 1-4, om i hvilket land bl.a. leverandøren er hjemmehørende, om det i det land, bl.a. leverandøren er hjemmehørende i, er muligt at pålægge bl.a. leverandører at udføre eller deltage i forhold, som vil udgøre spionage eller sabotage mod Danmark, om bl.a. leverandøren direkte eller indirekte kontrolleres af et andet lands statslige organer, herunder militære myndigheder, og om bl.a. leverandøren har været involveret i aktiviteter i Danmark eller andre lande, som har medført en negativ påvirkning af statens sikkerhed, informationssikkerheden eller den offentlige orden.

Af lovens forarbejder, de almindelige bemærkninger, pkt. 1, fremgår bl.a., at hovedformålet med loven var at skabe hjemmel til, at telemyndighederne kan forbyde konkrete leverandøraftaler vedrørende den kritiske teleinfrastruktur, hvis aftalerne vurderes at udgøre en trussel mod statens sikkerhed, at vurderingen heraf vil ske på baggrund af objektive kriterier, og at der ved lovforslaget ville blive taget et vigtigt skridt til at sikre en robust teleinfrastruktur og derigennem beskytte Danmark mod bl.a. spionage, sabotage og nedbrud af samfundskritiske funktioner. Der ville i henhold til forarbejderne herved ske en væsentlig reduktion af risikoen for, at Danmark kunne blive mål for pression fra fremmede stater under en konflikt.

Angående begrebet "særlige tilfælde" fremgår det af forarbejderne til loven, de specielle bemærkninger til både lovens § 2 og til § 3, at der herved forstås tilfælde, hvor der dels er tale om en trussel mod statens sikkerhed, dels ikke er mulighed for at anvende mindre indgribende midler.

Betingelsen om "særlige tilfælde" i bestemmelsens forstand er således opfyldt, såfremt videreførelsen af aftalen mv., eller anvendelse af netkomponenter, systemer og værktøjer mv. leveret i henhold til aftalen, udgør "en væsentlig trussel mod statens sikkerhed", jf. straks nedenfor, og hvis formålet med forbuddet ikke kunne være nået ved mindre indgribende foranstaltninger end et forbud, jf. lovens § 3, stk. 4, og nærmere afsnit 3.3.2. ovenfor.

Af lovens forarbejder, de almindelige bemærkninger, pkt. 3.1.3 og de specielle bemærkninger til § 2 og til § 3, fremgår, at CFCS, ved vurderingen af om en konkret aftale udgør "en væsentlig trussel mod statens sikkerhed", vil skulle foretage en samlet vurdering af, om aftalen, henholdsvis netkomponenter, systemer og værktøjer mv. leveret i henhold til aftalen, må anses for at udgøre en trussel mod statens sikkerhed. I vurderingen kan indgå de objektive kriterier, der er nævnt i § 2, stk. 2, nr. 1-4, jf. ovenfor. Udtrykket "statens sikkerhed" skal i henhold til forarbejderne forstås i overensstemmelse med det EU-retlige udtryk "den nationale sikkerhed", hvormed der som udgangspunkt hører væsentlige trusler mod samfundskritiske funktioner, herunder medarbejderes kommunikation.

Videre fremgår det af lovens forarbejder, de specielle bemærkninger til § 3, at bestemmelsens kerneområde vil være situationer, hvor CFCS vurderer, at der nu er en risiko for, at en leverandør vil misbruge en aftale, henholdsvis de komponenter, systemer mv., der er leveret i henhold til en aftale, til at forberede eller udføre sabotage mod telenettet, som kan medføre, at telenettet helt eller delvist afbrydes. Som eksempler er i forarbejderne nævnt tilfælde, hvor CFCS vurderer, at der nu er risiko for, at leverandøren indbygger bagdøre, som gør det muligt for leverandøren at afbryde eller på anden måde foretage uautoriseret påvirkning af dele af telenettet. Det vil i henhold til forarbejderne også være tilfældet, hvis aftalen omfatter drift af systemer, hvor der nu vurderes at være risiko for, at leverandøren gennem adgangen til systemerne vil være i stand til at foretage en hel eller delvis afbrydelse.

Som et andet eksempel er i forarbejderne nævnt situationer, hvor CFCS vurderer, at aftalen, henholdsvis de komponenter, systemer mv., der er leveret i henhold til aftalen, indebærer risiko for, at en leverandør vil misbruge aftalen til at foretage spionage mod samfundskritiske funktioner, herunder deres medarbejderes eller samarbejdspartneres kommunikation. Den potentielle trussel og dennes karakter vil skulle vejes op mod karakteren af komponenten, systemet mv. Jo mere kritiske dele af telenettet, som komponenten, systemet mv. anvendes i, des mindre vil der skulle til, for at der kan siges at være tale om en væsentlig trussel mod statens sikkerhed. Der vil endvidere kunne lægges vægt på, om et forbud vil kunne have negative konsekvenser for telenettets drift, som overstiger de potentielt negative konsekvenser, hvis den vurderede trussel bliver en realitet

3.3.3.2. Vurderingen efter § 3, jf. § 2, stk. 2, nr. 1-4.

Huawei er hjemmehørende i Kina, som Danmark efter det oplyste ikke har indgået en sikkerhedsaftale eller tilsvarende sikkerhedssamarbejde med, og hvor det efter det oplyste om artikel 7 i den kinesiske "National Intelligence Law", er muligt at pålægge leverandører eller deres underleverandører at udføre eller

deltage i forhold, som vil udgøre spionage, jf. herved telesikkerhedslovens § 2, stk. 2, nr. 1-2. Dette er tillige understøttet af vidneforklaringen fra F [redacted] og den svenske Post- og Telestyrelse afgørelse af 20. oktober 2020 som stadfæstet af de svenske domstole.

CFCS har i afgørelsens begrundelse ikke henvist til oplysninger omfattet af telesikkerhedslovens § 2, stk. 2, nr. 4, der er tilgængelige i sagens åbne del. Landsretten finder dog efter bevisførelsen, herunder navnlig vidneforklaringen fra P [redacted] hvorunder bl.a. oplysningerne i Bloombergs artikel af 15. juni 2023 blev bekræftet, anledning til at bemærke, at det er sandsynliggjort, at Huawei i forbindelse med TDC's valg af leverandør til 5G-netværket har været involveret i aktiviteter i Danmark, som har medført negativ påvirkning af den offentlige orden, jf. herved telesikkerhedslovens § 2, stk. 2, nr. 4, eller dennes analogi.

3.3.3.3. Karakteren af DWDM-netværket

Som nævnt er der mellem parterne enighed om, at DWDM-netværket er en del af den kritiske teleinfrastruktur i Danmark. Dette er tillige understøttet af bevisførelsen i øvrigt, herunder forklaringerne fra N F [redacted] og O [redacted] ligesom der ikke ses mellem parterne at være tvist om det, der er anført herom i afgørelsen af 21. marts 2023, pkt. 4.2.1. Landsretten lægger derfor til grund, at DWDM-netværket er en helt central og essentiel del af data- og telekommunikation i Danmark. Videre lægger landsretten efter bevisførelsen følgende grund, at det vil få særdeles store negative konsekvenser for det danske samfund, hvis DWDM-netværket bliver ustabil, lukket ned eller på anden måde kompromitteret.

Endelig lægger landsretten efter bevisførelsen, herunder forklaringerne fra vidnerne F [redacted] og G [redacted] til grund, at det ikke kan udelukkes, og at der dermed er en risiko for, at DWDM-netværket kan kompromitteres, herunder derved, at der i den leverede software, f.eks. ved installation af en opdatering, som ikke har været sikkerhedstestet, muligt gennem en "out of band", kan indbygges en bagdør, som kan give adgang til DWDM-udstyret, herunder NCE-T styresystemet, hvorved man ville kunne gøre netværket ustabil eller i værste fald afbryde det eller aflæse data herfra.

Det kan ikke tillægges afgørende betydning, at der ikke er oplyst om konkrete tilfælde, hvor DWDM-netværket har været eller har været forsøgt kompromitteret, idet landsretten bemærker, at der i hverken lovens ordlyd eller forarbejder er krav herom. Derimod fremgår det som nævnt af lovens forarbejder, at jo mere kritiske dele af telenettet, som komponenten, systemet mv. anvendes i, des mindre vil der skulle til, for at der kan siges at være tale om en væsentlig trussel mod statens sikkerhed.

Det i forarbejderne, de specielle bemærkninger til § 3, omtalte om, at "truslen er mere konkretiseret" angår efter landsrettens opfattelse den situation, at CFCS efter lovens § 2 ikke har fundet anledning til at nedlægge et forbud mod indgåelsen af en aftale, men hvor efterfølgende forhold ved samme aftaleforhold viser sig senere at udgøre en trussel mod statens sikkerhed. Da vil der skulle være tale om, at de efterfølgende forhold udgør en væsentlig trussel mod statens sikkerhed, som er mere konkretiseret, end da aftalen først blev indgået, og der ikke blev nedlagt et forbud efter § 2. Dette krav kan ikke antages at gælde i den foreliggende situation, hvor loven ikke var trådt i kraft, da TDC oprindeligt indgik aftalen med Huawei, hvorfor der i sagens natur ikke kan være tale om vurdering af efterfølgende forhold, som skulle være mere konkretiserede.

3.3.3.4. Sammenfattende om "særlige tilfælde" og "en væsentlig trussel mod statens sikkerhed" under sagens åbne del

På ovenstående baggrund finder landsretten, at CFCS's vurdering af, at videreførelse af "Amendment 4", samt anvendelse af netkomponenter, systemer og værktøjer mv. leveret i henhold til "Amendment 4", udgør en "væsentlig trussel" mod statens sikkerhed, jf. herved telesikkerhedslovens § 3, stk. 1 og 2, er faktisk underbygget i det materiale, der er fremlagt under sagens åbne del, idet der herved også henvises til afsnittet ovenfor angående testning ved HCSEC, fuld kildekode og binær ækvivalens (afsnit 3.3.1.).

3.3.3.5. Sagens lukkede del

Det fremgår af forarbejderne til telesikkerhedsloven, de specielle bemærkninger til § 11, at rettens afgørelse affattes under hensyntagen til, at der kan være oplysninger, der er indgået i CFCS' afgørelse, som af sikkerhedsmæssige grunde ikke kan videregives til parten. Det er derfor i forarbejderne forudsat, at rettens afgørelse affattes og begrundes på grundlag af sagens åbne materiale, som parten har kendskab til og har haft lejlighed til at kommentere, men således at retten i sin afgørelse kan henvise til, at oplysninger i det åbne materiale er godtgjort eller sandsynliggjort i de fortrolige oplysninger, som er fremlagt for retten og den særlige advokat.

Landsretten finder som nævnt, at opfyldelsen af betingelserne "væsentlig trussel mod statens sikkerhed" og "særlige forhold" i telesikkerhedslovens § 3, er tilstrækkeligt godtgjort i den åbne del af sagen.

Landsretten finder dog anledning til at bemærke, at det ovenfor anførte i afsnit 3.3.3.2. angående telesikkerhedslovens § 3, jf. § 2, stk. 2, nr. 1-4, afsnit 3.3.3.3. angående karakteren af DWDM-netværket og afsnit 3.3.3.4. angående en sammenfatning af afsnit 3.3.3. tillige er sandsynliggjort i de oplysninger, der er fremkommet under sagens lukkede del, mens det i det ovenfor i afsnit 3.3.2. om proportionalitet anførte ikke er afsvækket i de fortrolige oplysninger, der er fremkommet under sagens lukkede del.

3.3.3.6. Konklusion angående "særlige tilfælde" og "en væsentlig trussel mod statens sikkerhed"

På ovenstående grundlag, og da der ikke i øvrigt findes grundlag for at tilside-sætte CFCS' vurdering, finder landsretten det således godtgjort, at der den 21. marts 2023, hvor CFCS traf afgørelse, både forelå "særlige tilfælde", og at vi-dereførelse af TDC's aftale med Huawei ved "Amendment 4", der vedrørte kri-tiske netkomponenter, systemer og værktøjer, herunder varetagelsen af driften heraf (stk. 1), henholdsvis anvendelse af netkomponenter, systemer og værktø-jer mv. leveret i henhold til aftalen (stk. 2), udgjorde "en væsentlig trussel mod statens sikkerhed".

3.3.4. Øvrige forhold

3.3.4.1. Den særlige advokat og kontradiktion

Efter det anførte i forarbejderne til telesikkerhedsloven sammenholdt med U 2010.2910 H, U 2011.2673 H og U 2011.2695 H finder landsretten, at opdelingen af sagen i en åben og lukket del er i overensstemmelse med kravene i artikel 6, stk. 1, i Den Europæiske Menneskerettighedskonvention, men at det under sa-gen skal sikres, at TDC via kontradiktion har haft en reel mulighed for effektiv varetagelse af sine interesser.

Det bemærkes, at rettens prøvelse efter på den ene side udlændingelovens kapi-tel 7 b og § 8 F i lov om dansk indfødsret, og på den anden side prøvelsen efter telesikkerhedslovens §§ 7- 13 ikke fuldstændig kan sidestilles, da den først-nævnte prøvelse angår fortrolige oplysninger angående parten selv (udlændin-gen), mens den sidstnævnte prøvelse angår fortrolige oplysninger, der ikke di-rette angår parten selv.

Hertil kommer, at kravet om kontradiktion, herunder muligheden for, at den særlige advokat kan drøfte sagens oplysninger med parten, TDC, må angå de væsentlige forhold, der er blevet lagt vægt på i den afgørelse, der er til prøvelse. Således kan det ikke kræves, at den særlige advokat har anledning til med par-ten at drøfte ethvert detailforhold, der er indgået i sagens omfattende materiale, for at kunne varetage partens interesser under sagens lukkede del.

Som nævnt ovenfor i afsnit 3.3.3.5. finder landsretten, at oplysningerne angå-ende "en væsentlig trussel mod statens sikkerhed" og "særlige forhold", jf. te-lesikkerhedslovens § 3, er tilstrækkeligt godtgjort i den åbne del af sagen.

På ovenstående grundlag og efter en samlet vurdering finder landsretten, at TDC via kontradiktion har haft en reel mulighed for effektiv varetagelse af sine interesser under sagen.

3.3.4.2. Hjemmelsmangler i øvrigt

Efter det ovenfor under afsnit 3.2. og 3.3. anførte finder landsretten, at der ikke er grundlag for at antage, at afgørelsen af 21. marts 2023 ikke havde tilstrækkelig hjemmel i telesikkerhedslovens § 3 og § 17, eller at afgørelsen i øvrigt lider af hjemmelsmangler.

3.3.4.3. Officialprincippet

Endvidere finder landsretten, at der med det under sagen fremkomne ikke er grundlag for at antage, at CFCS ved tilblivelsen af afgørelsen har tilsidesat officialprincippet eller baseret afgørelsen på et ukorrekt eller misvisende faktum.

3.3.4.4. Adressaten for påbuddet af 30. november 2020

Det fremgår af påbuddet af 30. november 2020, at dette er adresseret til TDC Group A/S. TDC har under retssagen gjort gældende, at påbuddet er uden retsvirkning for selskabet under henvisning til, at rette adressat for afgørelsen var TDC ("TDC NET A/S"), hvilket parterne i øvrigt er enige om.

Henset til, at det af afgørelsen fremgår, at den angår aftalen af 7. december 2020 ("Amendment 4") indgået mellem TDC ("TDC NET A/S") og Huawei, at TDC de facto har overholdt påbuddet, og at der ikke forud for, at sagen blev anlagt i august 2023 har været rejst indsigelser herimod, finder landsretten, at TDC ikke på noget tidspunkt kan anses for at have været i tvivl om, hvem påbuddet var rettet mod. Angivelsen af TDC Group A/S som adressat for påbuddet kan derfor ikke føre til, at TDC ("TDC NET A/S") ikke er bundet heraf.

3.3.4.5. Tidspunktet for iværksættelse af høring over lovforslag nr. 190 af 10. marts 2021

Efter en samlet vurdering af forløbet frem til den 7. december 2020, formålet med telesikkerhedsloven, oplysningen om, at afgørelsen af 21. marts 2023 er den eneste afgørelse, der er truffet efter loven, samt den omstændighed, at loven for så vidt angår bl.a. § 3 har tilbagevirkende kraft for afgørelser, der indgås fra netop den 7. december 2020, jf. § 17, stk. 2, finder landsretten det ubetænkeligt at lægge til grund, at det ikke beror på et tilfældigt tidsmæssigt sammentræf, at iværksættelsen af høringen over lovforslaget skete samme dag som CFCS gav en tilbagemelding på det fremsendte udkast til "Amendment 4", således at TDC tidligst netop denne dato kunne indgå aftalen, jf. nærmere afsnit 3.2. ovenfor, og at datoen anført i lovens § 17, stk. 2, skal ses i samme lys.

Idet TDC ikke har anfægtet selve den omstændighed, at loven blev vedtaget med tilbagevirkende kraft som beskrevet, og da der som nævnt ikke er grundlag for at tilsidesætte afgørelsen angående telesikkerhedslovens § 3, som blev truffet for at forfølge et lovligt og sagligt formål, finder landsretten, at sammenhængen mellem tilbagemeldingen på aftaleudkastet og høringen over lovudkastet samme dag ikke, som anført af TDC, indebærer, at det er CFCS, der skal bevise, at der ikke er sket en uhensigtsmæssig sammenblanding af den udøvende

og lovgivende magt, eller at CFCS på dette grundlag er erstatningsansvarlig over for TDC.

Uanset, om det måtte lægges til grund, at der fra politisk side fra foråret 2020 var et ønske om at begrænse kinesiske leverandører til den kritiske teleinfrastruktur, er det ikke med det under sagen fremkomne sandsynliggjort, endsige godtgjort eller bevist, at afgørelsen af 21. marts 2023 har været båret af politiske hensyn.

Ligeledes kan det – uanset om det måtte lægges til grund, at TDC af højtstående embedsmænd var blevet lovet at få telesikkerhedsloven i en fortrolig præhøring – ikke tillægges betydning for de spørgsmål, der er til prøvelse under denne sag, at dette ikke skete.

3.3.4.6. Høringen over CFCS' udkast til afgørelse

Det er under sagen oplyst, at der er forskelle i det udkast til afgørelse, CFCS hørte TDC over, og den endelige afgørelse af 21. marts 2023.

Landsretten finder, at der ikke er grundlag for at antage, at den omstændighed, at der fra udkastet til den endelige afgørelse og indtil den endelige afgørelse, navnlig som følge af TDC's høringssvar, skete væsentlige ændringer, var båret af usaglige hensyn, eller at dette kan føre til, at CFCS er erstatningsansvarlige over for TDC.

Det bemærkes herved, at det er afgørelsen af 21. marts 2023, der er til prøvelse.

3.3.4.7. Afviklingsfristen

Det fremgår af telesikkerhedslovens § 3, stk. 3, at CFCS kan fastsætte en frist for, hvornår en aftale skal være afviklet efter bestemmelsens stk. 1, eller hvornår anvendelse af kritiske komponenter mv. skal være ophørt efter bestemmelsens stk. 2. Det fremgår af lovens forarbejder, de specielle bemærkninger til bestemmelsen, at CFCS efter høring af teleudbyderen foretager en vurdering af på den ene side behovet for hurtigst muligt at fjerne en væsentlig trussel mod statens sikkerhed og på den anden side hensynet til den fortsatte og stabile drift af den kritiske teleinfrastruktur. Videre fremgår det samme sted, at nedlæggelse af forbud således ikke bør føre til, at der sker afbrydelser på telenettet, fordi teleudbyderen ikke har haft mulighed for at indgå eller implementere en ny aftale, hvorfor CFCS som udgangspunkt bør fastsætte en nærmere frist, som er baseret på, hvornår en loyalt agerende teleudbyder kan have taget de nødvendige forholdsregler.

I afgørelsen af 21. marts 2023 blev fristen for afvikling af "Amendment 4" fastsat til den 31. december 2026 og fristen for ophør med at anvende de i henhold til "Amendment 4" leverede kritiske netkomponenter, systemer mv. til den 1.

januar 2027. Dermed blev der fastsat en længere frist end angivet i høringsskrivelsen af 10. oktober 2022. Det anføres i afgørelsen, at CFCS herved har imødekommet TDC's anmodning om en afviklingsfrist på fire år, ligesom det anføres, at CFCS under visse betingelser efter anmodning fra TDC vil være indstillet på at genoptage afgørelsen for så vidt angår spørgsmålet om fristfastsættelsen.

På denne baggrund samt efter det oplyste om TDC's indgåelse af en aftale med Ciena om installation af det nye DWDM-netværk finder landsretten, at der ikke er grundlag for at tilsidesætte fristerne den 31. december 2026 for afvikling af "Amendment 4", henholdsvis den 1. januar 2027 for ophør med at anvende det i henhold til "Amendment 4" leverede kritiske netkomponenter, systemer mv.

3.3.5. "Radiokædenetværket"

Det er under sagen oplyst, at det af Huawei leverede NCE-T managementsystem også anvendes i det såkaldte "radiokædenetværk", hvor datatransmissionen foregår via radiomaster i en kæde. Radiokædenetværket anvendes som alternativ til fibernetværk i områder over hele Danmark, hvor det er vanskeligt eller ikke-rentabelt at nedgrave fibernet.

Parterne er uenige om, hvorvidt sagen også omhandler NCE-T managementsystemet i radiokædenetværket. TDC har i den forbindelse under sagen oplyst, at en udskiftning af NCE-T managementsystemet i radiokædenetværket vil indebære en udgift på 60-100 mio. kr.

CFCS har under sagen oplyst, at TDC kan fortsætte med at anvende NCE-T managementsystemet til styring af radiokædenetværket under givne forudsætninger, som TDC selv har indflydelse på. Herved har CFCS henvist til brev til TDC af 31. august 2023, hvoraf fremgår bl.a., at NCE-T efter omstændighederne fortsat vil kunne anvendes til radiokæde efter den 1. januar 2027, i det omfang der for anvendelsen af NCE-T til radiokæde kan etableres og påvises et regime, der vurderes som sikkerhedsmæssigt forsvarligt.

På denne baggrund har CFCS gjort gældende, at afgørelsen af 21. marts 2023 ikke udelukker TDC's anvendelse af NCE-T managementsystemet til styring af radiokædenetværket. Da der ikke foreligger nogen afgørelse, der udelukker anvendelse af NCE-T managementsystemet til styring af radiokædenetværket, er spørgsmålet ikke omfattet af landsrettens prøvelse under denne sag.

Idet landsretten herefter lægger til grund, at NCE-T managementsystemet til styring af radiokædenetværket ikke nødvendigvis er omfattet af forbuddet i afgørelsen af 21. marts 2023, hvilket i øvrigt er understøttet af, at TDC under hovedforhandlingen overbragte en ansøgning om en tilpasning af NCE-T managementsystemet til styring af radiokædenetværket til CFCS' repræsentanter, finder landsretten, at spørgsmålet om afgørelsens rækkevidde i forhold til NCE-T

managementsystemet til styring af radiokædenetværket ikke har en sådan konkret karakter, at det kan indgå i prøvelsen af sagen. Landsretten bemærker herved også, at TDC's påstand 5, der er en nærmere specificeret betalingspåstand, ikke indeholder delkrav, der er relateret til udskiftning af NCE-T managementsystemet til styring af radiokædenetværket.

3.4. Sammenfatning om afgørelsens hjemmel og begrundelse for forbuddet efter telesikkerhedslovens § 3

På den anførte baggrund er der således ikke grundlag for at tilsidesætte den del af CFCS' afgørelse af 21. marts 2023, der angår anvendelsen af telesikkerhedslovens § 3, ligesom der ikke er grundlag for at antage, at afgørelsen lider af hjemsmangler.

Der er følgelig heller ikke grundlag for at fastslå, at CFCS som følge af forhold ved afgørelsen af 21. marts 2023 er erstatningsansvarlig over for TDC, hvorfor CFCS frifindes for TDC's påstand 1 og 3.

4. Ekspropriation

4.1. Betingelserne for ekspropriation

Af grundlovens § 73, stk. 1, fremgår, at ejendomsretten er ukrænkelig, og at ingen kan tilpligtes at afstå sin ejendom, uden hvor almenvellet kræver det, ligesom ekspropriation kun kan ske ifølge lov og mod fuldstændig erstatning, jf. herved også artikel 1 i tillægsprotokol 1 til Den Europæiske Menneskerettighedskonvention og artikel 17 i EU's charter om grundlæggende rettigheder.

I telesikkerhedsloven er det lagt til grund, at afgørelser efter telesikkerhedslovens §§ 2-3 kan indebære ekspropriation, idet det af lovens § 4, stk. 2, fremgår, at der ydes fuldstændig erstatning til den eller de berørte parter, såfremt en afgørelse efter disse bestemmelser udgør et ekspropriativt indgreb.

Det er almindeligt antaget, at det er en betingelse for, at der foreligger ekspropriation efter grundlovens § 73, stk. 1, at der er tale om indgreb i "ejendom", at det, indgrebet retter sig imod, indehaves af en ejer, som er beskyttet af bestemmelsen, og at indgrebet har karakter af afståelse. Parterne er enige om, at de to førstnævnte betingelser er opfyldt.

CFCS har derimod i afgørelsen anført – og under sagen gjort gældende – at det indgreb i TDC's ejendom, som afgørelsen udgør, ikke har karakter af afståelse og dermed ikke er ekspropriativt.

Almindeligvis er det antaget, hvilket tillige er lagt til grund i CFCS' afgørelse af 21. marts 2023, at vurderingen af, om der foreligger afståelse, skal ske efter en samlet vurdering, hvori indgår indgrebets intensitet, indgrebet begrundelse

(causa), indgrebets generelle eller konkrete karakter, og om der sker en overførsel af rettigheder fra den hidtidige ejer til en ny.

4.2. *Indgrebets intensitet*

Det fremgår af afgørelsen af 21. marts 2023, at fastsættelsen af afviklingsfristen, hvorved denne er to år længere end aftalens udløb, medfører, at forbuddet i relation til opretholdelsen af aftalen har en meget begrænset intensitet. Det er dog i afgørelsen også anerkendt, at den omstændighed, at TDC ikke havde mulighed for at udnytte optionen på at forlænge supportaftalen, ligesom TDC ville være afskåret fra at anvende udstyr indkøbt under aftalen, i sagens natur ville have "en vis forstyrrende indvirkning på TDC's virksomhed og være forbundet med økonomiske konsekvenser".

I forarbejderne til telesikkerhedsloven, de specielle bemærkninger til § 4, er det anført bl.a., at afgørelser efter lovens § 3 kan udgøre indgreb mod konkrete aftaler, som efter omstændighederne vil kunne være af betydelig intensitet over for den pågældende aftalepart, hvorfor det er anført, at det ikke kan udelukkes, at et forbud efter omstændighederne vil kunne anses for at være ekspropriativt.

Som anført ovenfor under afsnit 1 er der mellem parterne enighed om, at det ikke er praktisk muligt at adskille det udstyr og de komponenter mv., der er leveret i henhold til "Amendment 4" fra det udstyr og komponenter mv., der i øvrigt er leveret i henhold til rammeaftalen fra 2011 mellem TDC og Huawei. Forbuddet i afgørelsen mod anvendelse af udstyr leveret i henhold til "Amendment 4" angår således reelt også udstyr leveret fra rammeaftalens indgåelse i 2011 og indtil "Amendment 4" trådte i kraft pr. 1. januar 2022.

Landsretten lægger til grund, at TDC ved indgåelsen af rammeaftalen og de følgende år, i hvert fald frem til december 2015, hvor der blev afholdt et møde mellem TDC, Huawei og CFCS angående opfølgning på bl.a. sikkerhedsmæssige udfordringer, ikke havde nogen grund til at tro, at de danske myndigheder anså forholdet til Huawei for at være så problematisk, at et forbud kunne komme på tale.

På dette grundlag finder landsretten, at TDC altså fra 2011 uden kendskab til de forhold, der senere blev problematiseret, havde indrettet sig på at skulle have et længerevarende leverandørforhold til Huawei, og i flere år i god tro og i tillid hertil fik leveret udstyr, komponenter mv. fra Huawei til etablering og drift af DWDM-netværket.

Videre lægger landsretten efter bevisførelsen til grund, at forbuddene i afgørelsen af 21. marts 2023 har indebåret særdeles store praktiske og økonomiske konsekvenser for TDC, der har været nødsaget til at udskifte hele DWDM-netværket. Den omstændighed, at TDC er et stort selskab med et betydeligt an-

lægsbudget og en organisation med en stor kapacitet, kan ikke ud fra en betragtning om relativitet i sig selv føre til, at indgrebet ikke kan betragtes som økonomisk eller praktisk intensivt.

Den relativt lange afviklingsfrist i afgørelsen kan heller ikke føre til, at indgrebet ikke kan betragtes som intensivt, idet det efter de fremlagte oplysninger om udbudsprocessen og arbejdet med at indkøbe og installere det nye DWDM-udstyr fra Ciena, hvilket er understøttet af vidneforklaringerne fra B, H og I må lægges til grund, at TDC påbegyndte processen med udskiftningen kort tid efter forbuddet var blevet meddelt, og at denne proces står på i hele perioden frem mod årsskiftet 2026/2027, hvor forbuddet henholdt til både telesikkerhedslovens § 3, stk. 2, i afgørelsen af 21. marts 2023 træder i kraft.

Det bemærkes også, at konsekvenserne af afgørelsen både havde indvirkning på TDC's aktuelle råden i form af fortsat drift af det allerede indkøbte udstyr, samt fremtidig udnyttelse af denne ret i form af eventuelle forlængelsesaftaler med Huawei.

Sammenfattende finder landsretten på ovenstående grundlag, at CFCS' afgørelse af 21. marts 2023 har en meget betydelig intensitet i forhold til TDC, der blev hårdt ramt af indgrebet, og at dette med betydelig vægt taler for, at afgørelsen var udtryk for ekspropriation.

4.3. Indgrebets begrundelse (causa)

Det fremgår af forarbejderne til telesikkerhedsloven, de specielle bemærkninger til § 4, at indgreb efter bl.a. § 3, stk. 1 og 2, altid vil have til formål at beskytte statens sikkerhed, og at navnlig det forhold, at forbud mod opretholdelse af en indgået aftale efter § 3, stk. 1, eller anvendelse af kritiske komponenter, systemer mv. efter § 3, stk. 2, vil være begrundet i hensyn til statens sikkerhed, må antages at tale med en vis vægt imod, at der vil være tale om ekspropriation.

Som anført ovenfor under afsnit 3 finder landsretten, at der ikke er grundlag for at tilsidesætte den del af CFCS' afgørelse af 21. marts 2023, der angår anvendelsen af telesikkerhedslovens § 3, hvorfor det lægges til grund, at afgørelsen blev truffet for at afværge en væsentlig fare (risiko mod statens sikkerhed) og således varetog betydelige samfundsmæssige interesser.

Som videre anført ovenfor, under afsnit 4.2, finder landsretten, at TDC ikke har udvist bebrejdellesværdig adfærd i perioden fra indgåelsen af rammeaftalen i 2011 og i hvert fald frem til 2015. Derimod finder landsretten, at TDC senere i forløbet af CFCS blev advaret om de tiltagende sikkerhedsmæssige problemer med at benytte Huawei som leverandør. Landsretten lægger herved, som også anført i afgørelsen af 21. marts 2023, til grund, at TDC's daværende sikkerheds-

chef og legal director i 2017 modtog en klassificeret briefing fra CFCS om de problemer, som CFCS havde identificeret i samarbejdet med Huawei, at der var en markant ændret sikkerhedsmæssig situation i 2019/2020 som beskrevet ovenfor, under afsnit 3.3.1.2, ligesom at TDC i slutningen af 2020 og i 2021 af CFCS flere gange blev anbefalet at afslutte leverandørforholdet, hvilket TDC havde hjemmel til i bl.a. pkt. 33 i rammeaftalen fra 2011. Der henvises også til det ovenfor under pkt. 3.3.2 om proportionalitet anførte om, at formålet med afgørelsen ikke ville kunne være nået ved mindre indgribende foranstaltninger end et forbud.

Sammenfattende finder landsretten, at indgrebets begrundelse (causa) sammenholdt med TDC's adfærd med betydelig vægt taler for, at CFCS's afgørelse af 21. marts 2023 ikke var udtryk for ekspropriation.

4.4. Indgrebets generelle eller konkrete karakter

CFCS har i afgørelsen af 21. marts 2023 anført, at selv om indgrebet konkret rammer TDC, er indgrebet udslag af anvendelse af generelle regler og en vurdering ud fra saglige og objektive kriterier, hvorfor det ikke rammer TDC vilkårligt. Videre er det anført, at indgrebet er hjemlet ved en særlovgivning, der har haft virkning siden der blev foretaget offentlig høring over lovforslaget, hvorfor TDC siden da har haft viden om, at selskabet kunne blive genstand for et forbud.

Landsretten tiltræder, at telesikkerhedsloven er formuleret som generelle regler, og at TDC ikke rammes vilkårligt, men bemærker, at kredsen af de teleselskaber, der kan blive ramt af et forbud i henhold til telesikkerhedsloven, jf. den legale definition i lovens § 1, nr. 3, er snæver.

Som anført ovenfor, afsnit 3.3.4.5., finder landsretten det endvidere ubetænkeligt at lægge til grund, at det ikke beror på et tilfældigt tidsmæssigt sammentræf, at iværksættelsen af høringen over lovforslaget skete samme dag, den 7. december 2020, som CFCS gav en tilbagemelding på det fremsendte udkast til "Amendment 4", således at TDC tidligst netop denne dato kunne indgå aftalen, og at netop den 7. december 2020 af samme grund blev fastsat som ikrafttrædelsestidspunkt for den del af loven, der gjaldt med tilbagevirkende kraft, idet loven i øvrigt havde ikrafttræden den 1. juli 2021. Der henvises herved også til det ovenfor under afsnit 3.2. anførte angående lovens § 17.

Landsretten finder det på denne baggrund videre ubetænkeligt at lægge til grund, at den nævnte tilrettelæggelse skete med henblik på at muliggøre nedlæggelsen af et forbud over for TDC angående leverandørforholdet med Huawei som sket ved den senere afgørelse af 21. marts 2023.

Endelig lægger landsretten efter det oplyste til grund, at afgørelsen af 21. marts 2023 er den eneste afgørelse, der er blevet truffet i henhold til telesikkerhedslovens § 3.

Sammenfattende finder landsretten på ovenstående grundlag, at indgrebet havde en særdeles konkret karakter rettet mod TDC, og at forløbet med betydelig vægt taler for, at CFCS's afgørelse af 21. marts 2023 var udtryk for ekspropriation.

4.5. Overførsel af rettigheder

Det er i afgørelsen af 21. marts 2023 anført, at CFCS ved vurderingen af, at afgørelsen ikke udgør et ekspropriativt indgreb, har lagt vægt på, at TDC's rettigheder ikke overføres til en anden part, og at afgørelsen alene indebærer, at TDC begrænses i sin råden i henhold til indgåede aftaler og i at anvende allerede leveret udstyr.

Det er ubestridt, at der ved afgørelsen ikke sker overførsel af rettigheder fra en tidligere ejer (TDC) til en ny ejer. Derimod har afgørelsen af 21. marts 2023 den konsekvens, at TDC måtte ophøre med sit leverandørforhold til Huawei angående DWDM-netværket, som havde stået på siden 2011, ligesom TDC blev tvunget til at udskifte hele DWDM-netværket, og altså også de dele, der var leveret i perioden fra 2011 og indtil "Amendment 4" trådte i kraft pr. 1. januar 2022. Der er således tale om tilintetgørelse af TDC's rettigheder.

Efter bevisførelsen, herunder skønsmandens besvarelse af spørgsmål 3, 4, 7, 11 og II, samt forklaringerne fra A, H og J og til dels K lægger landsretten til grund, at TDC havde været tilfredse med leverandørforhold til Huawei, og at der for TDC ikke var nogen økonomisk, kommerciel eller teknisk grund til at udskifte Huawei som leverandør af DWDM-netværket.

Videre lægger landsretten til grund, at den tvungne afslutning af leverandørforholdet til Huawei og den deraf følgende udskiftning af DWDM-netværket skete på et tidspunkt, TDC ikke selv havde valgt, ligesom selskabet ved det efterfølgende udbud var begrænset i sit valg af leverandører. Begge dele stillede utvivlsomt TDC dårligere kommercielt.

Uanset, at der som nævnt ikke var tale om overførsel af rettigheder, finder landsretten, at den ved afgørelsen skete tilintetgørelse af rettigheder i form af TDC's ret til anvendelse af allerede indkøbt og installeret udstyr mv. samt TDC's ret til at opretholde et leverandørforhold til Huawei, hvilke rettigheder var af privatretlig karakter, i hvert fald til dels må sidestilles med overførsel af rettigheder.

Sammenfattende finder landsretten, at disse forhold med nogen vægt taler for, at CFCS's afgørelse af 21. marts 2023 var udtryk for ekspropriation.

4.6. Sammenfatning om ekspropriation

Det er ubestridt, at almenvellet – af hensyn til statens sikkerhed, jf. herved det anførte ovenfor, afsnit 3 og 4.3. – krævede, at der skete ekspropriation, ligesom ekspropriationen er hjemlet i telesikkerhedslovens § 4.

Betingelserne i grundlovens § 73, stk. 1, for, at der foreligger ekspropriation, er derfor opfyldt.

På ovenstående baggrund, og efter en samlet vurdering, hvor også beskyttelses-hensynet bag grundlovens § 73, stk. 1, er indgået, finder landsretten herefter, at CFCS's afgørelse af 21. marts 2023 var udtryk for ekspropriation over for TDC, hvorfor TDC's påstand 4 tages til følge.

Landsretten finder, at der ikke er grundlag for mod TDC's protest at hjemvise sagen til fornyet behandling med henblik på administrativ udmåling af ekspropriationserstatningen ved CFCS, der ikke er sagkyndig myndighed herfor. Landsretten tager derfor TDC's betalingspåstand under pådømmelse.

5. Opgørelsen af ekspropriationserstatningen

5.1. Udgangspunktet for erstatningsopgørelsen

Som anført ovenfor er CFCS's afgørelse af 21. marts 2023 udtryk for ekspropriation, hvorfor TDC er berettiget til fuld erstatning, jf. grundlovens § 73, stk. 1, og telesikkerhedslovens § 4, stk. 2.

Kravet om "fuld erstatning" indebærer, at TDC's skal have erstattet ethvert økonomisk tab, som er en adækvat følge af ekspropriationen med henblik på, at TDC i økonomisk forstand i videst muligt omfang stilles, som om indgrebet ikke havde fundet sted. Erstatningen, der under de foreliggende omstændigheder må tage udgangspunkt i genanskaffelsesværdien, skal dog fastsættes i henhold til almindelige erstatningsretlige grundsætninger, herunder berigelsesgrundsætningen, hvorefter TDC ikke må stilles økonomisk bedre, end hvis indgrebet ikke havde fundet sted.

5.2. TDC's opgørelse af erstatningskravet

Som anført ovenfor er der mellem parterne enighed om, at afgørelsen af 21. marts 2023 nødvendiggør en total udskiftning af det af Huawei leverede DWDM-netværk, herunder hardware, software, firmware, support mv., omfattende udstyr mv. leveret fra rammeaftalens indgåelse i 2011 og indtil "Amendment 4" trådte i kraft pr. 1. januar 2022.

Som ligeledes anført ovenfor lægger landsretten til grund, at TDC påbegyndte processen med udskiftningen, kort tid efter forbuddet var blevet meddelt, og at denne proces siden da har stået på og fortsætter frem mod årsskiftet 2026/2027.

TDC har under sagen fremlagt en lang række fakturaer fra navnlig den nye leverandør af DWDM-netværket, Ciena, samt en række ordrer ("quotes") fra samme, der imidlertid endnu ikke er faktureret til eller betalt af TDC. Endvidere har TDC fremlagt en række fakturaer for fiberleje og leje af "co-locations", primært i udlandet, ligesom der er fremlagt oplysninger om forøget strømforbrug ved at have to parallelle DWDM-netværk i drift. TDC har også fremlagt et særdeles omfattende materiale angående registrering af tid for egne medarbejdere, der ifølge TDC har deltaget i udskiftningen af DWDM-netværket og dertil knyttede opgaver.

Det fremgår af skønsmandens besvarelse af spørgsmål 7, 8 og II, at TDC ikke har opnået eller vil opnå relevante økonomiske besparelser ved udskiftningen af det af Huawei leverede udstyr med det af Ciena leverede udstyr, ligesom skønsmanden ved besvarelsen af spørgsmål IG har anført, at det i en periode vil være forbundet med meromkostninger for TDC at have to parallelle DWDM-netværk i drift.

Landsretten lægger derfor til grund, at TDC har haft et betydeligt økonomisk tab, der kan kræves erstattet.

Det af TDC opgjorte tab er imidlertid forbundet med en række betydelige usikkerhedsmomenter, der har væsentlig betydning for opgørelsen af erstatningen. Således indeholder betalingspåstanden for så vidt angår alle erstatningsposterne både afholdte og forventede, fremtidige udgifter, men med forskellige skæringsdatoer, nemlig pr. 1. februar 2026, henholdsvis et "forventet domstidspunkt", som imidlertid ikke har været TDC bekendt.

Udgifterne til indkøb af Ciena DWDM-netværket har endvidere været delt yderligere op, idet de "afholdte/påløbne" omkostninger indeholder beløb, der ifølge TDC allerede er betalt, udgifter, hvor TDC forventede at modtage fakturaer på afgivne ordrer ("quotes"), "Purchase and Licence Orders" for indkøb relateret til den sidste del af udskiftningen, som ifølge TDC forventedes at være faktureret på domstidspunktet, samt 1/3 af estimatet over yderligere indkøb i andet kvartal 2026. Der er således ikke sket en klar sondring mellem allerede afholdte og betalte udgifter over for fremtidige, forventede udgifter, som efter landsrettens opfattelse ikke er så konkretiserede, at de på nuværende tidspunkt kan kræves betalt.

Endvidere har TDC – på trods af skriftveksling herom – ikke redegjort for betydningen af, at TDC på et tidspunkt under alle omstændigheder ville have ud-

skiftet det af Huawei leverede DWDM-netværk. Uanset at landsretten efter bevisførelsen lægger til grund, at Huaweis udstyr havde en lang levetid, finder landsretten det ubetænkeligt at lægge til grund, at TDC på et tidspunkt, uafhængigt af afgørelsen af 21. marts 2023, ville have udskiftet det af Huawei leverede DWDM-netværk, og at der ved TDC's opgørelse af erstatningen burde have været taget højde herfor.

TDC har således ikke godtgjort, at der er grundlag for at opgøre tabet ved indkøbet af Ciena-netværket "en til en" uden hensyntagen til "nyt for gammelt", fremrykkede investeringer eller andre besparelser.

For så vidt angår tabsposten vedrørende interne personaleomkostninger er det ikke godtgjort, at lønomkostningerne ikke i væsentligt omfang er udgifter til personale, som TDC under alle omstændigheder ville have haft. Dette er understøttet af bl.a. forklaringen fra [redacted]^J der har forklaret bl.a., at der helt sikkert var nogle af de medarbejdere, der har været med til TDC's projekt om at udskifte Huaweis udstyr med Cienas, og som optræder i opgørelsen over egen tid, som under alle omstændigheder ville have været i TDC, og som i alle tilfælde skulle have løn, også selvom de ikke arbejdede med projektet.

Endelig har TDC ikke foretaget fradrag for fremtidige sparede udgifter, herunder navnlig fremtidige sparede udgifter til strømforbrug, idet landsretten, uanset skønsmandens forklaring, efter TDC's egne oplysninger lægger til grund, at det af Ciena leverede DWDM-netværk har et lavere forbrug end TDC's tidligere DWDM-netværk leveret af Huawei.

Allerede fordi der ikke foreligger et ansvarsgrundlag i sagen, kan TDC ikke få erstattet sine udgifter til advokatomkostninger, som ikke er omfattet af almindelige sagsomkostninger for sagens førelse.

Landsretten finder på ovenstående baggrund, at TDC's opgørelse af erstatningen – uanset at det lægges til grund, at TDC har lidt et betydeligt tab – er forbundet med så mange og væsentlige usikkerheder, at opgørelsen af erstatningen må ske efter et friere skøn.

Hertil kommer, at det efter landsrettens opfattelse bør indgå i vurderingen af TDC's erstatningskrav, at TDC som beskrevet ovenfor allerede fra 2017 og frem mod 2021 af CFCS var blevet advaret om de sikkerhedsmæssige problemer med Huawei og flere gange var blevet anbefalet at afslutte leverandørforholdet, hvilket TDC havde hjemmel til i aftaleforholdet med Huawei. Landsretten finder herunder, at det på et tidspunkt må have stået TDC klart, at et forbud kunne komme på tale, men at TDC desuagtet fortsatte leverandørforholdet til Huawei, herunder fortsatte med at få leveret udstyr, komponenter mv., der nu kræves erstattet.

Under inddragelse af ovenstående momenter finder landsretten efter en samlet vurdering, at erstatningen skønsmæssigt kan opgøres til 80 mio. kr., hvilket beløb alene indeholder udgifter, der var afholdt af TDC samt "quotes" afgivet pr. 1. februar 2026. Der er ved fastsættelsen af erstatningsbeløbet navnlig henset til de direkte omkostninger til indkøb og drift af det nye DWDM-netværk fra Ciena, og kun i mindre omfang henset til de i øvrigt opgjorte udgifter, herunder udgifter til personale.

I dette omfang tages TDC's påstand 5 herefter til følge.

5.3. Forrentning af erstatningen

TDC har i medfør af rentelovens § 3, stk. 4, nedlagt påstand om forrentning fra sagens anlæg den 15. september 2023. CFCS har protesteret herimod.

Det er ubestridt, at en meget stor del af de økonomiske krav, der er indtalt under sagen, ikke var hverken forfaldent eller afholdt af TDC på dette tidspunkt.

TDC har ikke under sagen fremlagt oplysninger om, hvornår de af TDC afholdte udgifter er betalt. Hertil kommer den ovenfor beskrevne betydelige usikkerhed om opgørelsen af TDC's krav.

Landsretten finder på denne baggrund, at der foreligger sådanne særlige forhold, at ekspropriationserstatningen først skal forrentes fra landsrettens dom i sagen den 24. juni 2026, jf. rentelovens § 3, stk. 5.

6. Sagsomkostninger

TDC må anses for den tabende part angående sagens første hovedspørgsmål om prøvelse af CFCS's afgørelse af 21. marts 2023, samt det hertil knyttede spørgsmål om betaling af erstatning efter dansk rets almindelige regler om erstatning udenfor kontrakt (påstand 1 og 3). Endvidere er TDC's påstand 2 afvist.

TDC må imidlertid anses for den vindende part angående sagens andet hovedspørgsmål om ekspropriation og har i tilknytning hertil, ud af sin betalingspåstand om betaling af knap 195 mio. kr., fået medhold i, at CFCS skal betale 80 mio. kr. (påstand 4 og 5).

Hver af parterne har således for en del tabt og for en del vundet sagen, jf. herved retsplejelovens § 313, stk. 1. CFCS havde dog i forhold til spørgsmålet om betaling nedlagt påstand om frifindelse, hvorfor TDC må betragtes som i overvejende grad at have vundet sagen.

Det fremgår af landsretspræsidenternes vejledende salærtakster, at beløbet til dækning af advokatbistand i sager med en økonomisk værdi over 5,75 mio. kr. skal fastsættes skønsmæssigt efter en vurdering af, hvad der kan anses for rimeligt, også og under hensyntagen til sagens omfang og karakter. Der skal herunder tages hensyn både til arbejdets omfang og det ansvar, der er forbundet med sagens førelse, ligesom der skal lægges vægt på sagens omfang og kompleksiteten af sagens faktum og juridiske problemstillinger, samt forberedelsens og hovedforhandlingens varighed, jf. herved også U 2019.2639 H, U 2021.215 H og U 2022.383 H.

På denne baggrund og efter en samlet vurdering af de nævnte ovennævnte momenter finder landsretten, at CFCS efter sagens udfald i delvise sagsomkostninger til TDC skal betale 5 mio. kr. til dækning af omkostninger til advokatbistand ekskl. moms. Herudover skal CFCS til TDC betale 45.900 kr. til dækning af udgifter til syn og skøn og 4.500 kr. til dækning af retsafgift, således at de samlede sagsomkostninger udgør 5.050.400 kr.

CFCS afholder endeligt udgiften til afhjæmning af skønsmanden.

Der er ikke grundlag for ud over sagsomkostningsbeløbet at godtgøre TDC de afholdte udgifter til indhentelse af egne sagkyndige rapporter eller juridisk respons, ligesom det bemærkes, at udgifter til trykning af ekstrakter og materialesamlinger er indeholdt i beløbet til dækning af omkostninger til advokatbistand.

Der findes ikke at foreligge sådanne særlige grunde, som kan føre til, at der tillægges Dansk Erhverv sagsomkostninger.

THI KENDES FOR RET:

Forsvarets Efterretningstjeneste v/Center for Cybersikkerhed (nu Styrelsen for Samfundssikkerhed) frifindes for TDC NET A/S' påstand 1.

TDC NET A/S' påstand 2 afvises.

Forsvarets Efterretningstjeneste v/Center for Cybersikkerhed (nu Styrelsen for Samfundssikkerhed) frifindes for TDC NET A/S' påstand 3.

Forsvarets Efterretningstjeneste v/Center for Cybersikkerhed (nu Styrelsen for Samfundssikkerhed) skal anerkende, at Center for Cybersikkerheds afgørelse af 21. marts 2023 om nedlæggelse af forbud over for TDC NET A/S indebærer ekspropriation over for TDC NET A/S.

Forsvarets Efterretningstjeneste v/Center for Cybersikkerhed (nu Styrelsen for Samfundssikkerhed) skal til TDC NET A/S betale 80 mio. kr. med procesrente fra den 24. juni 2026.

Den af den særlige advokat nedlagte subsidiære påstand afvises.

I sagsomkostninger skal Forsvarets Efterretningstjeneste v/Center for Cybersikkerhed (nu Styrelsen for Samfundssikkerhed) inden 14 dage betale 5.050.400 kr. til TDC NET A/S. Beløbet forrentes efter rentelovens § 8 a.