FORSVARSMINISTERIET

# Analyse af forankringen af CFCS' virksomheds-rettede indsats

Februar 2023

FORSVARSMINISTERIET

# FORORD

Partierne bag det nuværende forsvarsforlig 2018-2023 (forsvarsforligskredsen) indgik d. 24. juni 2021 *Aftale om et Styrket Cyberforsvar* og understregede i den forbindelse et ønske om en styrkelse af Center for Cybersikkerheds (CFCS) virke med særligt fokus på at øge den samlede indsats over for den private sektor. Med det sigte ønskede partierne, at der skulle igangsættes en analyse af CFCS' forankring under Forsvarets Efterretningstjeneste, herunder fordele og ulemper ved at lægge en del af virksomhedsindsatsen i en civil enhed på Forsvarsministeriets område. Analysen skulle præsenteres og drøftes i forligskredsen inden sommeren 2022.

Forsvarsministeriet har på den baggrund udarbejdet nærværende analyse til brug for en videre drøftelse i forsvarsforligskredsen. Analysen var færdigskrevet i juni 2022, men er, grundet blandt andet Folketingsvalget og regeringsdannelsen, ikke blevet drøftet i forligskredsen i 2022.

I analysens første del kortlægges snitfalder og opgaveansvar på tværs af myndigheder med ansvar for cyber- og informationssikkerhed, herunder opgaver hidtil forankret i Erhvervsstyrelsen og i Digitaliseringsstyrelsen. Med oprettelsen af et Digitaliserings- og Ligestillingsministerium, jf. Kongelig Resolution af 15. december 2022, vil flere af disse opgaver imidlertid blive ressortoverført til det nye ministerium. Den Kongelige Resolution har omvendt ikke ændret på CFCS' opgaveportefølje, og de nævnte snitflader i analysen er grundlæggende uforandrede. Forsvarsministeriet vurderer på den baggrund, at analysens konklusioner fortsat er gældende.

Med venlig hilsen

Forsvarsministeriet

# Indhold

# Resumé

Regeringen og forsvarsforligspartierne besluttede med *Aftale om et Styrket Cyberforsvar* (24. juni 2021) at evaluere og styrke Center for Cybersikkerheds (CFCS) virke med særligt fokus på indsatsen over for den private sektor samt i forhold til forankringen ved Forsvarets Efterretningstjeneste (FE). Forsvarsministeriet har på den baggrund udarbejdet indeværende analyse, som bygger på høringssvar om samarbejdet fra en række erhvervs- og brancheorganisationer samt bidrag fra relevante myndigheder.

Analysen af CFCS' virksomhedsrettede indsats er opdelt i tre dele:

1. En kortlægning af CFCS' ansvar og opgaver relateret til private virksomheder samt snitflader til øvrige relevante myndigheder på cyberområdet.

2. En evaluering af CFCS' virksomhedsrettede indsats baseret på erhvervs- og brancheorganisationernes input.

3. En analyse af de forhold og muligheder, der gør sig gældende i forhold til at imødekomme identificerede udfordringer. På den baggrund præsenteres fordele og ulemper ved to modeller for forankringen af CFCS' virksomhedsrettede indsats.

## CFCS' ansvar, opgaver og snitflader

Med kortlægningen belyses CFCS' brede opgaveportefølje relateret til at styrke cyber- og informationssikkerheden i den kritiske infrastruktur. I relation til den private sektor er CFCS' opgaver fokuseret mod virksomheder, der understøtter samfundsvigtige funktioner, mens CFCS udelukkende indtager en oplysende og vejledende funktion i forhold til små og mellemstore virksomheder (SMV'er) – og dette i et tæt samarbejde med andre myndigheder.

Kortlægningen viser, at der inden for det seneste år er indført en lang række initiativer, som skal styrke cyber- og informationssikkerheden hos private virksomheder. En lang række af initiativerne er rettet mod eksempelvis SMV'er og forankret hos Erhvervsstyrelsen.

## Erfarede tendenser og udfordringer vedrørende CFCS' virksomhedsrettede indsats

Med udgangspunkt i indhentede erfaringer fra både CFCS og erhvervs- og brancheorganisationerne tegnes et billede af en række varierende - og til tider modsatrettede - tendenser, behov og ønsker til CFCS' fremtidige indsats over for den private sektor. De tre hovedtendenser er følgende:

- Der er uklarhed om roller og ansvar i relation til virksomhedsrettede opgaver.

- Der er behov og ønsker vedrørende videndeling, vejledning og dataindsamling.

- Der er særlige forhold vedr. CFCS' rolle i relation til telesektoren.

### 1) Uklarhed om roller og ansvar i relation til virksomhedsrettede opgaver

**Udfordring:**
Med afsæt i høringen af erhvervs- og brancheorganisationerne tegner der sig et billede af uklarhed om fordelingen af ansvar og opgaver på det brede cybersikkerhedsområde. Der er eksempelvis tvivl om, hvor man som virksomhed kan henvende sig, og hvilken hjælp man kan forvente fra forskellige myndigheder, hvis man rammes af en cybersikkerhedshændelse.

**Relevante forhold og mulige løsninger:**
Forsvarsministeriet ser behov for en styrket kommunikationsindsats om, at CFCS' virksomhedsindsats primært er rettet mod virksomheder, der understøtter samfundsvigtige funktioner, hvor andre

øvrige opgaver på området eksempelvis ligger i Erhvervsstyrelsen eller hos Politiet. Misforståelsen gælder særligt i relation til CFCS' begrænsede funktion i forhold til små og mellemstore virksomheder (SMV'er). Samtidig er der med *National Strategi for Cyber- og Informationssikkerhed (NCIS) 2022-2024* og *Delrapport om CFCS' virke i relation til rådgivning, uddannelse, forskning og videndeling (dec. 2021)* igangsat en række virksomhedsrettede initiativer. Initiativerne er igangsat, og den fulde effekt heraf vil forventeligt først optræde ved fuld implementering.

**2) Videndeling, vejledning og dataindsamling**

**Udfordring:**
Erhvervs- og brancheorganisationerne ønsker generelt mere videndeling, rådgivning, åbenhed og hurtigere afklassificering af data fra CFCS. Samtidig er der en (modsatrettet) kritik af, at CFCS ikke må være konkurrenceforvridende i forhold til de virksomheder, der lever af at udarbejde trusselsvurderinger og rådgivning om cybersikkerhed. Herudover er flere virksomheder forbeholdende med at dele viden med en efterretningstjeneste, om end de fleste fortsat ønsker, at CFCS' arbejde tager udgangspunkt i efterretningsdata.

**Relevante forhold og mulige løsninger:**
Forsvarsministeriet ser et behov for en styrket kommunikation og forventningsafstemning mellem CFCS og erhvervs- og brancheorganisationerne. Kommunikationen skal aktivt være med til at skabe en bedre forståelse for CFCS' virke og lovgrundlag, herunder i forhold til samarbejdet med det øvrige FE og forhold vedrørende klassificerede oplysninger. I forlængelse af en øget kommunikationsindsats, ser Forsvarsministeriet behov for at skabe en mere åben kultur for den del af CFCS, som arbejder med de virksomhedsrettede opgaver.

**3) CFCS' rolle i relation til telesektoren**

**Udfordring:**
Nogle af erhvervs- og brancheorganisationerne italesætter, at der er udfordringer i relation til CFCS' rolle over for telesektoren som både rådgivende myndighed og tilsynsmyndighed, da denne dobbeltrolle ifølge bidragsyderne hindrer et hensigtsmæssigt og tillidsfuldt samarbejde mellem televirksomhederne og CFCS.

**Relevante forhold og mulige løsninger:**
For at imødekomme usikkerheden blandt televirksomhederne om, hvornår CFCS giver rådgivning, og hvornår CFCS stiller krav som tilsynsmyndighed, vurderer Forsvarsministeriet, at der er behov for en dialog mellem CFCS og telesektoren om baggrunden for tilsynsenhedens krav til telesektoren. Dette vurderes at kunne skabe transparens og indsigt i fordelene ved at have samlet både rådgivning og tilsyn hos samme myndighed. Herudover kan CFCS styrke kommunikationen om, hvordan oplysningerne fra netsikkerhedstjenesten anvendes, og hvorvidt disse udveksles med tilsynsenheden i CFCS.

## Forsvarsministeriets forslag til vejen frem for CFCS' virksomhedsrettede indsats

Til sidst i analysen præsenterer Forsvarsministeriet de fordele og ulemper, der vil være ved at løse de skitserede udfordringer gennem enten en organisatorisk status quo eller ved placering af CFCS' virksomhedsrettede indsats et andet sted under Forsvarsministeriets ressort. Ved begge løsninger imødekommes flere af de identificerede udfordringer, men der vil dog fortsat være en række fortsatte udfordringer forbundet med begge løsninger.

De respektive fordele og ulemper ved henholdsvis en organisatorisk status quo eller en ny forankring af CFCS' virksomhedsrettede indsats under Forsvarsministeriet er opsummeret i nedenstående figur.

| FORDELE OG ULEMPER VED ORGANISATORISK STATUS QUO | |
|---|---|
| **Fordele** | **Ulemper** |
| • Bedst mulig adgang til efterretningsdata:<br>▪ Giver stærkest mulige indblik i det internationale trusselsbillede og dets aktører<br>▪ CFCS' produkter vil adskille sig fra produkter, der udbydes på det private marked<br>• Samling af begrænsede specialiserede kompetencer<br>• Ingen yderligere fragmentering af cybersikkerhedsområdet | • Manglende videndeling fra CFCS grundet klassifikation<br>• Opfattelse af en lukket efterretningskultur:<br>▪ Medfører informationsasymmetri i samarbejdsrelationen<br>▪ Medfører mytedannelse om CFCS' arbejde<br>• Udfordringer med gensidig tillid<br>• Tilbageholdenhed i forhold til at dele data med CFCS, herunder tilslutning til netsikkerhedstjenesten. |
| **FORDELE OG ULEMPER VED NY FORANKRING UNDER FORSVARSMINISTERIET** | |
| **Fordele** | **Ulemper** |
| • Mulighed for mere åben kultur og identitet<br>• Bedre forudsætning for gensidig tillid og datadeling fra virksomheder<br>• Fortsat adgang (om end mere begrænset) til efterretningsdata<br>• Bedre mulighed for videndeling | • Yderligere fragmentering af cybersikkerhedsområdet og -kompetencer<br>• Begrænset adgang til efterretningsdata<br>• Fortsat begrænset videndeling grundet klassifikation<br>• Risiko for konkurrenceforvridende opgaver<br>• Risiko for opbygning af parallelle kapaciteter og nedsat kvalitet af opgaveløsningen |

# Indledning

Den 18. december 2022 var det 10 år siden, Center for Cybersikkerhed (CFCS) blev oprettet. Ved centerets oprettelse stod det klart, at et digitaliseret land som Danmark er særdeles sårbar over for trusler i cyberspace. Siden oprettelsen af CFCS i 2012 har den digitale og teknologiske udvikling bevæget sig med hastige skridt. Det har tilsvarende afledt en kompleks cybertrussel i tiltagende vækst. Senest har truslen materialiseret sig med Ruslands invasion af Ukraine, der har understreget konsekvenserne af cyberangreb i en væbnet konflikt. Cybertruslen er i dag blevet et grundvilkår i det danske samfund.

## Ønsket om et stærkt cybersikkederheds-samarbejde med den private sektor

Udviklingen på cyberområdet har affødt et stadigt stigende behov for robuste løsninger, og CFCS har gennem en årrække på den baggrund udvidet både sin kapacitet og sin opgaveportefølje. I takt med udviklingen og udvidelsen af opgaver har en række aktører udtrykt bekymring over, om CFCS' organisering er tilstrækkelig befordrende for videndeling og åbenhed, herunder i forhold til CFCS' placering ved Forsvarets Efterretningstjeneste (FE). Dertil kommer spørgsmålet om CFCS' rolle på teleområdet, hvor CFCS fungerer som både IT-sikkerhedsmyndighed, kompetencecenter og tilsynsmyndighed.

Regeringen og forsvarsforligspartierne ønskede med *Aftale om et Styrket Cyberforsvar* (24. juni 2021) at styrke Danmarks robusthed over for cyberangreb. Partierne ønskede specifikt, at CFCS styrker det gensidige samarbejde og partnerskab med den private sektor. Med aftalen blev det derfor besluttet at igangsætte *"en analyse af CFCS' forankring under FE, herunder fordele og ulemper ved at lægge en del af virksomhedsindsatsen i en civil enhed på Forsvarsministeriets område."*[1] Forsvarsministeriet har på den baggrund, og i overensstemmelse med det forligskredsgodkendte kommissorium (bilag 1), udarbejdet nærværende analyse af CFCS' forankring under FE med fokus på CFCS' samarbejde med den private sektor.

Som en del af analyseprocessen ønskede forligspartierne desuden en delrapport om CFCS' virke i relation til rådgivning, uddannelse, forskning og videndeling, hvortil der blev afsat 20 mio. kr. i forligsårene (2022-2023) og 13 mio. kr. til varige driftsomkostninger. Delrapporten mundede i januar 2022 ud i en række konkrete initiativer vedrørende rådgivning og uddannelse på cyberområdet.

## Analysens opbygning

Med afsæt i en analyse af CFCS' virksomhedsrettede indsats, herunder dens forankring ved FE, ser Forsvarsministeriet to organisatoriske løsningsforslag som vejen frem i forhold til at styrke samarbejdet med den private sektor.

De to løsningsforslag tager udgangspunkt i en tredelt analyse, jf. det forligskredsgodkendte kommissorium, med henblik på at belyse de konkrete opgaver, udfordringer og relevante forhold, der spiller ind i opgaveløsningen. Analysen er struktureret som følger:

1. Kortlægning af CFCS' ansvar, opgaver og snitflader til øvrige relevante myndigheder med virksomhedsrettede indsatser på cyberområdet, herunder en beskrivelse af og oversigt over de initiativer på cybersikkerhedsområdet, der relaterer sig til private virksomheder.

2. Analyse af erfaringerne med CFCS' opgavevaretagelse, samarbejde med den private sektor samt forslag, behov og løsninger på baggrund af involvering af relevante erhvervs- og branche-organisationer samt CFCS selv.

3. Analyse af hovedudfordringerne i samarbejdet og muligheder for imødekommelse af samme, samt fordele og ulemper ved to organisatoriske løsningsforslag: en organisatorisk status quo og placeringen af CFCS' virksomhedsrettede opgaver andet steds i Forsvarsministeriets koncern.

## Vidensamling, sparring og involvering af interessenter

Analysen bygger på bidrag fra relevante myndigheder, erhvervs- og brancheorganisationer, udenlandske erfaringer samt sparring med forskere og eksperter.

For at indhente viden om den private sektors erfaringer med samarbejdet med CFCS har Forsvarsministeriet involveret en række relevante erhvervs- og brancheorganisationer som repræsentanter for virksomhederne. Høringssvarene er organisationernes tilkendegivelse af deres medlemmers erfaringer med CFCS, og de enkelte virksomheder kan have divergerende opfattelser. Inddragelsen af en lang række forskellige organisationer har bidraget til, at et bredt udsnit af erfaringerne er repræsenteret. Høringssvarene fremgår af bilag 3 til 11.

Forsvarsministeriet har i den forbindelse modtaget bidrag fra Dansk Erhverv, Dansk Industri, IT-Branchen, Rådet for Digital Sikkerhed, de private medlemmer af Cybersikkerhedsrådet, Industriens Fond, Teleindustrien og SMVdanmark samt NRGi og Finans Danmark, der har afgivet høringssvar i egenskab af deres tidligere medlemskab af Virksomhedsforum for Digital Sikkerhed.

Herudover har Forsvarsministeriet indsamlet viden om organiseringen af cybersikkerhedsområdet i henholdsvis Sverige, Norge, Estland, Nederlandene og Storbritannien. Forsvarsministeriet har suppleret indhentningen med yderlige interviews for så vidt angår de to sidstnævnte lande.

# CFCS - Opgaver, ansvar og snitflader i den brede virksomhedsindsats

Danmark er et højt digitaliseret samfund, og den meget høje cybertrussel mod danske myndigheder og virksomheder udgør en betydelig sikkerhedsrisiko. For at styrke Danmarks beskyttelse mod cyberangreb og samle myndighedernes indsatser, oprettede man CFCS[2] som en del af FE d. 18. december 2012. CFCS er sat i verden for først og fremmest at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur.[3] I praksis omfatter det styrkelse af sikkerheden i Danmarks digitale infrastruktur, der dækker både netværk, computere og andre systemer, som samfundsvigtige funktioner er afhængige af. Samfundsvigtige funktioner omfatter *"de aktiviteter, varer og tjenesteydelser, som udgør grundlaget for samfundets generelle funktionsdygtighed."*[4]

CFCS varetager FE's opgave som Danmarks nationale IT-sikkerhedsmyndighed og er Danmarks netsikkerhedstjeneste samt telesikkerhedsmyndighed.[5] Rollen som national IT-sikkerhedsmyndighed indebærer en række opgaver af både forebyggende og afhjælpende karakter. Det gælder blandt andet oplysning, vejledning og rådgivning af danske myndigheder og virksomheder i forhold til at styrke cyber- og informationssikkerheden, så risikoen for cyberangreb mindskes, og så cyberangreb, hvis de lykkes, imødegås på den mest hensigtsmæssige måde.[6]

**CFCS' PRIMÆRE ANSVARSOMRÅDER:**

1. Drift af netsikkerhedstjeneste (militær og statslig varslingstjeneste)
2. National og militær it-sikkerhedsmyndighed og nationalt kompetencecenter
3. Ansvarlig for vurdering af den nationale cybertrussel
4. Myndighed for informationssikkerhed og beredskab på teleområdet
5. National TSE- og TEMPEST-myndighed
6. Krisestyring i relation til kritisk it-infrastruktur og deltagelse i øvelser
7. Nationalt kontaktpunkt for EU og NATO samt CSIRT iht. NIS-direktivet
8. Støtte og rådgivning vedr. cybersikkerhed i Grønland og på Færøerne

Forsvarsministeriet blev ved Kongelig resolution af 3. oktober 2011 givet ressortansvaret for sager vedrørende beskyttelse af kritisk it-infrastruktur samt statens varslingstjeneste for internettrusler, GovCert.[7] Ved etableringen af CFCS i 2012 gjorde tre forhold sig især gældende i relation til beslutningen om at placere CFCS ved FE: 1) Adgangen til efterretninger, hvilket blev vurderet at have stor betydning for centerets evne til at varsle og rådgive om cyberangreb, 2) FE's specialiserede kompetencer på området, samt 3) en styrkelse af den samlede cyberindsats og undgåelse af at opbygge parallelle kapaciteter. Den samme argumentation er efterfølgende blevet fremhævet i bemærkningerne til CFCS-loven fra både 2014 og 2019.[8]

CFCS' udgangspunkt for arbejdet med cybersikkerhed er trussels- og efterretningsbaseret. Det betyder konkret, at indsigt i trusselsaktørers forudsætninger og fremgangsmåder understøtter CFCS' produkter og rådgivning. Selvom CFCS og den øvrige del af FE tilsammen udgør én myndighed, er der gennem lovgivningen skabt en klar afgrænsning mellem FE's efterretningsmæssige virksomhed og CFCS' virksomhed. De oplysninger, som CFCS i sin rolle som netsikkerhedstjeneste indsamler, kan eksempelvis kun i helt særlige tilfælde udveksles med den øvrige del af FE.[9]

**CFCS' kerneopgaver**

CFCS' opgaver er hjemlet i lovgivning, myndighedsfastsatte forskrifter, internationale aftaler og regelsæt, hvoraf andre opgaver er blevet tilføjet i kraft af regeringsbeslutninger og politiske aftaler. CFCS' tre kerneopgaver er alle lovbestemte:

- CFCS varetager opgaven som netsikkerhedstjeneste og har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos virksomheder og myndigheder, der er tilsluttet netsikkerhedstjenestens sensornetværk.[10] Sensornetværket består af alarmenheder, der monitorerer netværkstrafikken og derved bidrager til at opdage og analysere cyberangreb og cyberspionagetrusler mod de tilsluttede myndigheder og virksomheder.

- CFCS varetager opgaven som national og militær IT-sikkerhedsmyndighed og beskæftiger sig med at oplyse, vejlede og rådgive myndigheder og virksomheder, der understøtter samfundsvigtige funktioner, samt varetager visse af de opgaver, der følger af sikkerhedscirkulæret, herunder sikkerhedsgodkendelse af informationssystemer.[11]

- CFCS er myndighed for cyber- og informationssikkerhed, leverandørsikkerhed og beredskab på teleområdet og har dermed sektoransvar for disse dele af telesektoren.[12]

Herudover fungerer CFCS som nationalt kontaktpunkt i EU[13] og NATO på cybersikkerhedsområdet og varetager rollen som CSIRT (Computer Security Incident Response Team).

CFCS bidrager desuden til krisestyring i relation til kritisk IT-infrastruktur, hvormed CFCS er med til at planlægge og gennemføre beredskabsøvelser i forskellige fora både nationalt og internationalt.

CFCS arbejder bredspektret med at opdage, analysere, varsle og modgå cyberangreb.[14] CFCS' rådgivning og produkter omfatter eksempelvis:

- Trusselsvurderinger af både klassificeret og ikke-klassificeret karakter, såvel som undersøgelsesrapporter fra større cybersikkerhedshændelser hos statslige myndigheder, som deles med samfundsvigtige virksomheder og myndigheder med henblik på forebyggelse.

- Rådgivning til samfundsvigtige virksomheder om blandt andet risikostyring, beredskab, adfærdsorienteret informationssikkerhed, leverandørstyring, uddannelse og kompetencer samt anskaffelser og udbud.[15]

- CFCS driver det nationale cybersituationscenter, der monitorerer sensornetværkets tilsluttede enheder 24/7 og på den baggrund opretholder et nationalt situationsbillede.

**CFCS og de samfundsvigtige funktioner**

CFCS har til opgave at monitorere netværkstrafik hos tilsluttede myndigheder og virksomheder, monitorere hændelser i de samfundskritiske sektorer og opbygge viden om aktører og trends på cybersikkerhedsområdet samt koordinere beredskabsaktørernes behov for samfundsvigtig elektronisk kommunikation i beredskabssituationer mv.[16] Den portefølje giver CFCS en lang række offentlige og private snitflader.

**KRITISK INFRASTRUKTUR**

Kritisk infrastruktur er *"infrastruktur – herunder faciliteter, systemer, processer, netværk, teknologier, aktiver samt serviceydelser – som er nødvendig for at opretholde eller genoprette samfundsvigtige funktioner"*. På det digitale område er det eksempelvis borgerrettede tele- og datasystemer, der er nødvendige for akut udrykning og personregistrering.

Organiseringen af cybersikkerhedsområdet følger sektoransvarsprincippet, hvilket betyder, at den enkelte virksomhed eller myndighed også har ansvaret i en krisesituation.[17] Samtidig er en række tværgående opgaver placeret ved CFCS, Politiets Efterretningstjeneste (PET), Erhvervsstyrelsen og Digitaliseringsstyrelsen. Som led i den Nationale Strategi for Cyber- og Informationssikkerhed (NCIS) 2018-2021 blev seks sektorer (sundhed, transport, energi, tele, finans og søfart) udpeget som samfundskritiske sektorer med ansvar for kritisk infrastruktur. Der blev derfor etableret decentrale cyber- og informationssikkerhedsenheder (DCIS'er) i de seks sektorer. DCIS'erne har til formål at koordinere arbejdet med cyber- og informationssikkerhed i og mellem sektorerne og fungere som kontaktpunkt til CFCS, der leder det tværsektorielle DCIS-forum. Dertil blev der med NCIS'en udarbejdet sektorspecifikke cyber- og informationssikkerhedsstrategier for hver af de seks samfundskritiske sektorer.

**SEKTORANSVARSPRINCIPPET INDEBÆRER BL.A. AT:**

1. Alle ministre skal sikre et forsvarligt beredskab inden for eget ressort
2. Sektoransvaret omfatter alle kritiske funktioner og opgaver, som er pålagt lovgivningsmæssigt, politisk eller administrativt.
3. Myndighedernes beredskabsplanlægning skal bygge på en løbende og systematisk risikovurderingsproces, som er forankret i ledelsen.
4. Myndighederne skal løbende overvåge risikobilledet inden for egen sektor.

Med NCIS for 2022-2024 udvides antallet af ministerområder, der skal oprette DCIS'er og udarbejde delstrategier. Ejerskabet og ansvaret for den kritiske infrastruktur varierer mellem ministerområderne. På nogle ministerområder er den kritiske infrastruktur statsligt ejet eller kontrolleret (f.eks. centrale statslige IT-systemer), mens det på andre ministerområder ligger hos private selskaber. Omfanget af CFCS' myndighedssamarbejde afhænger derfor af det respektive ministerområde.

**DIREKTIV OM FORANSTALTNINGER TIL SIKRING AF ET HØJT FÆLLES CYBERSIKKERHEDSNIVEAU I HELE UNIONEN (NIS2-DIREKTIVET)**

Med revisionen af det nuværende NIS-direktiv øges cybersikkerheden i EU ved, at enheder i væsentlige og vigtige sektorer påtager sig specifikke cybersikkerhedsmæssige foranstaltninger.

Med NIS2-direktivet udvides cybersikkerhedsindsatsen i dybden og i bredden. Direktivet udvider antallet af sektorer, der bliver anset som samfundskritiske, og NIS2 vil derfor omfatte en lang række nye sektorer. Derudover kommer direktivet til at udvide antallet af enheder, der skal stilles krav til i de enkelte sektorer. I relation til udvidelsen i dybden vil de omfattede enheder blive mødt med øgede krav, herunder i forhold til risikostyring, hændelseshåndtering, involvering af topledelse mv.

Den konkrete udmøntning af NIS2 vil ske i de enkelte medlemsstater.

**Telesektoren**
CFCS har en særlig rolle i forhold til telesektoren, idet CFCS har sektoransvar for visse dele af telesektoren. Det betyder konkret, at CFCS – inden for rammerne af sit myndighedsområde - fører tilsyn med telesektoren og koordinerer håndteringen af særlige trusler, der kan påvirke informationssikkerheden i telesektoren. CFCS kan i særlige tilfælde blandt andet forbyde konkrete leverandøraftaler samt anvendelse af kritiske komponenter og systemer i den kritiske teleinfrastruktur, såfremt det vurderes at udgøre en trussel mod statens sikkerhed.[18] Afgørelser efter loven forudsætter et særligt fagligt indblik i henholdsvis efterretningsmæssige og teletekniske forhold, som CFCS besidder.[19] Ydermere rådgiver CFCS samfundets beredskabsaktører om teleberedskab.

**CFCS og den brede virksomhedsindsats**
CFCS' opgaver rettet mod den private sektor fokuserer på virksomheder, der understøtter samfundsvigtige funktioner.[20] CFCS' ansvarsområde dækker ikke de virksomheder, herunder små og mellemstore virksomheder (SMV'er), der ikke understøtter samfundsvigtige funktioner. I forhold til SMV'er indtager CFCS således udelukkende en oplysende og vejledende funktion, og dette i et tæt samarbejde med andre myndigheder.

Erhvervsstyrelsen er den primære ansvarshavende myndighed for den brede virksomhedsrettede indsats inden for cyber- og informationssikkerhed. Det gennemgående mål for Erhvervsstyrelsens arbejde med cybersikkerhed er, at dansk erhvervsliv og særligt SMV'erne får et sikkerhedsmæssigt løft, f.eks. gennem oplysning, vejledning, kampagner, værktøjer, brobygningsaktiviteter og offentlig-private samarbejder. Det sker i tæt samspil med Erhvervsstyrelsens øvrige erhvervs- og digitaliseringspolitiske indsatser, som blandt andet har til formål at fremme digital omstilling blandt danske SMV'er, således at digital vækst og cybersikkerhed tænkes sammen.

**Virksomhedsrettede projekter og initiativer**
CFCS samarbejder tæt med Erhvervsstyrelsen om deres arbejde med at løfte cybersikkerheden hos danske virksomheder, især SMV'erne. CFCS deltager eksempelvis som observatør i og bidrager løbende til arbejdet i Erhvervsstyrelsens Virksomhedsforum for Digital Sikkerhed, der fungerer som en strategisk partner for og giver anbefalinger til regeringen og erhvervslivet om digital sikkerhed med fokus på SMV'er. Som en del af NCIS 2022-2024 etablerer Erhvervsstyrelsen blandt andet en SMV-cybersikkerhedsenhed for at styrke videndeling, facilitere offentlig-private initiativer og koordinere virksomhedsrettet regulering. På baggrund af den russiske invasion af Ukraine, er der herudover lanceret en pulje på 50 mio. kr. til at styrke cybersikkerheden i SMV'er. Puljen er en del af Erhvervsstyrelsens program SMV:Digital. For yderligere at højne cybersikkerhedsniveauet i danske virksomheder har Erhvervsministeriet indgået en cybersikkerhedspagt med Dansk Erhverv, Dansk Industri, Finans Danmark, Forsikring & Pension, HK, IDA, Industriens Fond, IT-branchen og SMVdanmark om at udveksle data og viden om digitale trusler.

**CFCS' VIRKSOMHEDSRETTEDE INDSATS**

CFCS' opgave er først og fremmest at understøtte et højt sikkerhedsniveau i den digitale infrastruktur, som samfundsvigtige funktioner er afhængige af. Størstedelen af CFCS' opgaveløsning er dermed rettet mod både myndigheder og private virksomheder, der understøtter samfundsvigtige funktioner. Det gælder eksempelvis monitorering og varsling som led i CFCS' netsikkerhedstjeneste samt konkret situationsbestemt rådgivning og vejledning. Dertil kommer, at en række af CFCS' myndighedsopgaver som national IT-sikkerhedsmyndighed og myndighed på teleområdet også er rettet mod virksomheder.

Som led i CFCS' opgavevaretagelse modtager CFCS løbende henvendelser fra virksomheder, der ikke understøtter samfundsvigtige funktioner. Efter en konkret vurdering af henvendelsens karakter indtager CFCS normalvis en oplysende og vejledende funktion i et tæt samarbejde med andre myndigheder, så efterspørgslen fra den pågældende virksomhed kan imødekommes bedst muligt. Virksomheden henvises endvidere til øvrige myndigheder, hvis det findes relevant.

Ydermere opretter Erhvervsstyrelsen og Digitaliseringsstyrelsen med understøttelse fra CFCS en fælles cyberhotline inden udgangen af 2022. Hotlinen målrettes borgere og virksomheder og vil være én samlet indgang til rådgivning ved spørgsmål om cybersikkerhed. Erhvervsstyrelsen og Digitaliseringsstyrelsen står herudover bag platformen "Sikkerdigital.dk", hvor råd og vejledning målrettet borgere, virksomheder og myndigheder er samlet. CFCS er samarbejdspartner og bidrager til indholdet på siden. Initiativerne tænkes sammen med politiets indsats og kommunikation ved cyberangreb – en indsats, der styrkes som en del af NCIS'en.

Erhvervsstyrelsen har ligeledes etableret en fælles digital løsning for virksomheders indberetning af brud på IT-sikkerhed og persondatasikkerheden i samarbejde med blandt andet CFCS. CFCS er desuden fast høringspart i forhold til Erhvervsstyrelsens behandling af sager vedrørende dual-use produkter.

Erhvervsstyrelsen er ved at opbygge et nationalt koordinationscenter for cybersikkerhedsindustri, -teknologi og –forskning. Her vil CFCS være en tæt strategisk og teknisk samarbejdspartner. Formålet er at styrke hele cybersikkerhedslandskabet, herunder navnlig i forhold til nystartede virksomheder og SMV'er, og skabe tættere samarbejder mellem centrale europæiske cyberaktører. Hertil er CFCS en faglig sparringspartner for Sikkerhedsstyrelsen og Erhvervsstyrelsens arbejde med udrulning af cybersikkerhedscertificeringer af digitale produkter, ydelser og processer.

Ligesom samfundets generelle robusthed over for cybertruslen er i en kontinuerlig modningsproces, reflekterer samarbejdet mellem CFCS og Erhvervsstyrelsen også behovet for stadigt tættere samarbejde på cyberområdet. Med NCIS 2022-2024 er der sat yderligere skub på den integrationsproces. Præmissen for det tætte myndighedssamarbejde er at skabe synergieffekter og merværdi, undgå duplikering af indsatser samt konkurrenceforvridning i forhold til private sikkerhedsfirmaer. Nedenstående figur opstiller de to myndigheders fokusområder og snitflader på cybersikkerhedsområdet.

CFCS understøtter og deltager herudover i en række fora med fokus på videndeling med virksomheder. Centeret faciliterer blandt andet Strategisk Samarbejdsforum for Cybersikkerhed, hvor repræsentanter fra de største virksomheder og brancheorganisationer i de samfundsvigtige sektorer deltager. CFCS kan både bistå med hjælp til forebyggelse og sikring af den digitale infrastruktur, såvel som understøttelse i situationer, hvor uheldet har været ude.

CFCS deler formandskabet for Cybersikkerhedsrådet med Digitaliseringsstyrelsen. Cybersikkerhedsrådet rådgiver regeringen om, hvordan den digitale sikkerhed styrkes og sikrer videndeling mellem myndigheder, erhvervsliv og forskningsverdenen. CFCS bidrager også til samarbejdsfora såsom Danish Hub for Cybersecurity og Bestyrelsesforeningen, hvor CFCS er med til at uddanne virksomhedsbestyrelser i arbejdet med cybersikkerhed. CFCS støtter og samarbejder også med virksomheder i forsvarsindustrien, herunder i forhold til sikkerhedsgodkendelse og akkreditering af industriens produkter i henhold til blandt andet EU- og NATO-sikkerhedsbestemmelser.

**CFCS og sikkerhedsmyndighedernes virksomhedsindsats**

Foruden den brede virksomhedsrettede indsats har CFCS et tæt myndighedssamarbejde med politiet og Politiets Efterretningstjeneste (PET). CFCS samarbejder og koordinerer indsatser med PET, der som national sikkerhedsmyndighed rådgiver og bistår offentlige myndigheder og virksomheder i sikkerhedsspørgsmål. Desuden er PET IT-sikkerhedsmyndighed på Justitsministeriets område. Derudover understøtter CFCS PET i forbindelse med efterforskning af overtrædelse af straffelovens kapitel 12 og 13 i relation til cyberangreb og -spionage.

Som led i ønsket om en styrket indsats mod IT-kriminalitet i NCIS 2022-2024 er det planlagt at indstationere en forbindelsesofficer fra National Enhed for Særlig Kriminalitet (NSK) til CFCS for at styrke den fælles indsats over for virksomheder, der rammes af cyberangreb. Under NSK er Nationalt Cyber Crime Center (NC3) placeret, der blandt andet har initiativet NC3 Erhverv. NC3 Erhverv henvender sig til SMV'er, der ved at kontakte det lokale politi har mulighed for at få en af politiets IT-eksperter ud til et foredrag. Herudover varetager CFCS den koordinerende rolle for telesektoren, når den Nationale Operative Stab (NOST) under Rigspolitiet nedsættes på områder, der berører sektoren.

| INITIATIVER PÅ CYBERSIKKERHEDSOMRÅDET RELATERET TIL PRIVATE VIRKSOMHEDER | | |
|---|---|---|
| | **CFCS** | **Erhvervsstyrelsen** |
| **X** = ansvarlig myndighed \| X = bidragende myndighed | | |
| **Eksisterende initiativer igangsat før 1/1-2022** | | |
| **Trusselsvurderinger og vejledninger målrettet digital infrastruktur, der understøtter samfundsvigtige funktioner** | **X** | |
| **Virksomhedsrettede informationskampagner om cyber- og informationssikkerhed** | | **X** |
| **Virksomhedsforum for Digital Sikkerhed** | X | **X** |
| **Cybersikkerhedsrådet*** | **X** | |
| **Strategisk Samarbejdsforum for Cybersikkerhed, Bestyrelsesforeningen, Danish Hub for Cybersecurity** | **X** | X |
| **Sikkerdigital.dk*** | | **X** |
| **Etablering af den nationale cybersikkerheds-certificeringsmyndighed**** | X | X |
| **Initiativer iværksat efter 1/1-2022** | | |
| **Cyberhotline*, [B]** | X | **X** |
| **Etablering af et nationalt koordinationscenter for cybersikkerhedsindustri, - teknologi og –forskning [A]** | X | **X** |
| **Etablering af en Cybersikkerhedsenhed for SMV'er [B]** | X | **X** |
| **Pulje på 50 mio. til at styrke cybersikkerheden i SMV'er i regi af SMV:Digital** | | **X** |
| **Cybersikkerhedspagt** | X | **X** |
| **Etablering af branchespecifikke fora mhp. øget praksisnær videndeling mellem det offentlige og private aktører om hændelser og trusler [A]** | X | **X** |
| **One-stop-shop digitalt rådgivnings- og undervisningsbibliotek på CFCS' hjemmeside [A]** | **X** | |
| **Årlig konference om cybersikkerhed [A]** | **X** | X |

* I samarbejde med Digitaliseringsstyrelsen
** I samarbejde med Sikkerhedsstyrelsen (ansvarlig myndighed)
[A] Initiativ fra Delrapport om CFCS' virke i relation til rådgivning, uddannelse, forskning og videndeling (dec. 2021)
[B] Initiativ fra National Strategi for Cyber- og Informationssikkerhed (NCIS) 2022-2024

**HOVEDPOINTER**

- CFCS varetager funktionen som Danmarks nationale **it-sikkerhedsmyndighed**, er **net-sikkerhedstjeneste** og **telesikkerhedsmyndighed** og arbejder bredspektret med at opdage, analysere, varsle og modgå cyberangreb.
- Ansvaret for cybersikkerhed er, i overensstemmelse med **sektoransvarsprincippet**, fordelt på forskellige myndigheder. Samtidig er er der placeret en række tværgående opgaver ved CFCS, PET, Erhvervsstyrelsen og Digitaliseringsstyrelsen.
- CFCS har **sektoransvar for visse dele af telesektoren.**
- CFCS' opgaver rettet mod den private sektor fokuserer på virksomheder, der understøtter **samfundsvigtige funktioner**.
- I relation til den brede virksomhedsrettede indsats inden for cyber- og informations-sikkerhed er **Erhvervsstyrelsen primær myndighed**.
- CFCS og Erhvervsstyrelsen er i tæt samarbejde om de initiativer, der har til formål at **løfte cybersikkerheden hos virksomheder uden for den samfundskritiske sektor, her-under SMV'er**.
- CFCS understøtter og deltager i en række fora med fokus på videndeling med virksom-heder.

# CFCS' samarbejde med den private sektor om cybersikkerhed

Anden del af analysen evaluerer CFCS' opgavevaretagelse i forhold til den private sektor og peger på mulige tiltag, som vil kunne bidrage til at styrke indsatsen over for virksomheder. Forsvarsministeriet har hørt en række erhvervs- og brancheorganisationer om deres erfaring med og perspektiver på CFCS' arbejde i relation til den private sektor. Derudover har CFCS bidraget med erfaringer med og perspektiver på centerets virksomhedsrettede samarbejde og opgaver.

Forsvarsministeriet har samlet og sammenskrevet erfaringerne fra høringssvarene for at give et overblik over perspektiver, behov og foreslåede tiltag. I det følgende afsnit præsenteres tre identificerede hovedtendenser samt yderligere fremhævede pointer fra erhvervs- og brancheorganisationernes svar. For et detaljeret sammendrag af interessenternes høringssvar henvises til bilag 2. Herudover fremgår høringssvarene i deres fulde længde i bilag 3 til 11.

Efterfølgende præsenteres ligeledes tendenser og hovedpointer fra CFCS' egne perspektiver angående deres virksomhedsrettede indsats og erfaring med samarbejdet med den private sektor.

**Erfaringer fra den private sektor**
Nedenstående afsnit beskriver erhvervs- og brancheorganisationernes erfaringer med CFCS samlet i tre identificerede hovedtendenser: Uklarhed om roller og ansvar i relation til virksomhedsrettede opgaver; CFCS' vejledning, videndeling og dataindsamling samt CFCS' rolle i relation til telesektoren. Afsnittet præsenterer ligeledes interessenternes behov i relation til en styrket cybersikkerhedsindsats i den private sektor, samt interessenternes forslag til løsningstiltag.

## Hovedtendenser

**Tendens 1: Uklarhed om roller og ansvar i relation til virksomhedsrettede opgaver**
Af høringssvarene fremgår det, at en stor del af organisationerne anerkender CFCS' arbejde med at styrke den danske cybersikkerhed, og at virksomheder med samfundsvigtige funktioner mødes af en høj faglighed i CFCS. Høringssvarene bærer dog præg af, at der er forvirring om ansvarsfordelingen mellem myndighederne på det samlede cyberområde. Flere interessenter forholder sig eksempelvis til cyberkriminalitet og efterforskning i deres høringssvar, hvilket ikke er opgaver inden for CFCS' ansvarsområde.

Det nævnes, at det for mange virksomheder ikke står klart, hvad de kan forvente af hjælp og støtte fra CFCS. Det understreges, at der er behov for en præcisering af, hvad CFCS kan tilbyde virksomhederne, og hvem virksomhederne skal henvende sig til ved cybersikkerhedshændelser.

En enkelt interessent reflekterer over, hvorvidt sektoransvarsprincippet giver mening på cybersikkerhedsområdet, eller om den offentlige indsats burde centraliseres.

**Tendens 2: Vejledning, videndeling og dataindsamling**
Flere interessenter påpeger, at CFCS deltager aktivt i konferencer, netværk og projekter med henblik på at udbrede viden om cybertruslen. På den baggrund vurderes CFCS at spille en vigtig rolle i den offentlige debat.

Blandt høringssvarene fremgår modsatrettede perspektiver på anvendeligheden af CFCS' vejledning samt trusselsvurderinger for virksomheder. Trusselsvurderingerne karakteriseres eksempelvis som vigtige bidrag af nogle, mens andre ikke finder dem tidssvarende og fyldestgørende.

Nogle af interessenterne oplever endvidere, at processen for nedklassificering forsinker delingen af informationer til virksomhederne.

En interessent bemærker, at deres medlemmer oftest er nødsaget til at bruge mange ressourcer på at indkøbe yderligere trusselsvurderinger på det private marked. En anden interessent understreger, at det er vigtigt, at CFCS' opgaver ikke er konkurrenceforvridende.

**KLASSIFIKATION**

En klassifikationsgrad fastsættes, ændres og ophæves under hensyntagen til den skade, som bortkomst, kompromittering eller ødelæggelse vurderes at kunne medføre for statens, allierede staters, koncernens samt enkeltpersoners sikkerhed. Der er forskellige klassifikationsgrader afhængig af den skade, som videregivelse af informationen vil kunne forvolde.

Det er kun den udstedende myndighed, der kan ændre klassifikationen eller afklassificere informationsbærende materiale. Ned- og afklassificering gøres, hvis de hensyn, der betingede klassifikationsgraden, ikke længere er til stede. Ned- og afklassificering meddeles til dem, der har modtaget oplysningerne.

CFCS' klassificerede viden ses af nogle interessenter som unik samt vigtig for CFCS' arbejde og forståelse af trusselsbilledet. For andre interessenter opfattes den klassificerede information som en problematisk hindring for CFCS' videndeling med virksomheder. Der ses således en afvejning blandt organisationerne af på den ene side CFCS' adgang til efterretningsbaseret viden og på den anden side efterspørgslen på en højere grad af videndeling.

Flere interessenter peger på, at CFCS' organisationskultur er præget af at være placeret ved en efterretningstjeneste. Det anskues af flere som medvirkende til, at der er udfordringer i samarbejdet med den private sektor. En enkelt interessent vurderer, at udfordringerne ved CFCS' samarbejde med de private virksomheder ikke skyldes placeringen ved FE, men i stedet CFCS' kulturelle tilgang til samarbejdet med den private sektor.

En række interessenter påpeger, at virksomhederne er tilbageholdende med tilslutning til CFCS' netsikkerhedstjeneste og sensornetværk grundet manglende gennemsigtighed om brugen af data, samt at de finder udbyttet af tilslutningen begrænset.

En enkelt interessent bemærker, at de aktuelle sager i medierne vedrørende FE skaber mistro mod efterretningsvæsenet, hvorfor nogle virksomheder er tilbageholdende med at blive associeret med CFCS.

**CFCS' NETSIKKERHEDSTJENESTE**

CFCS' netsikkerhedstjeneste er betegnelsen for centrets samlede aktiviteter i forbindelse med at opdage, analysere og bidrage til imødegåelsen af sikkerhedshændelser hos tilsluttede myndigheder og virksomheder. Dette sker blandt andet på baggrund af data fra sensornetværket.

Virksomheder, der varetager samfundsvigtige funktioner, kan efter anmodning blive tilsluttet netsikkerhedstjenesten, hvis CFCS konkret vurderer, at tilslutningen vil kunne bidrage til et højt informationssikkerhedsniveau i samfundet. CFCS kan i særlige tilfælde påbyde virksomheder at blive tilsluttet netsikkerhedstjenesten med henblik på monitorering af netværkskommunikation.

Netsikkerhedstjenestens indsats fokuserer på de mest avancerede angreb, der oftest udføres af statsstøttede aktører, eller cyberangreb, der i øvrigt kan påvirke det danske samfund i væsentlig grad. Cyberangreb af mindre omfang skal myndigheder og virksomheder i første omgang selv håndtere

**Tendens 3: CFCS' rolle i relation til telesektoren**
Som det fremgår i første del af analysen, har CFCS sektoransvar for visse dele af telesektoren, hvilket indbefatter både tilsyn og koordination af håndteringen af særlige trusler, der kan påvirke informationssikkerheden i telesektoren.

En interessent finder, at det operative samarbejde med CFCS generelt fungerer godt. En række af erhvervs- og brancheorganisationerne nævner i deres høringssvar, at CFCS' mange roller på teleområdet er uhensigtsmæssig.

Nogle af interessenterne henviser til, at placeringen ved FE er uhensigtsmæssig for tilsynet med og ansvar i relation til telesektoren. En interessent bemærker eksempelvis, at de oplever en tilbageholdenhed blandt virksomheder i telesektoren i forhold til at tilslutte sig sensornetværket, da CFCS så vil få indblik i de virksomheder, som de grundet rollen som tilsynsmyndighed også kan sanktionere.

## Behov og tiltag

Erhvervs- og brancheorganisationerne er i deres høringssvar blevet bedt om at svare på, hvad der kan imødegå de udfordringer, der peges på i relation til CFCS' samarbejde med den private sektor og hvilke tiltag, der vil kunne styrke CFCS' virksomhedsrettede indsats.

**Forslag relateret til CFCS' opgaveløsning: Videndeling, gennemsigtighed, SMV-indsats**
Af svarene fremgår det, at en højere grad af gennemsigtighed og tillid, operativ videndeling, afklassificering af oplysninger samt en større SMV-indsats vil kunne øge samarbejdet med den private sektor.

En interessent foreslår, at man ser mod Storbritanniens arbejde med hurtig nedklassificering af oplysninger, mens en anden interessent foreslår, at udvalgte virksomheder får medarbejdere godkendt til at modtage klassificerede informationer.

I flere høringssvar er der opmærksomhed på, at CFCS' indsats er rettet mod virksomheder i samfundskritiske sektorer, hvorfor andre virksomheder i mindre grad kan drage nytte af arbejdet. Flere interessenter foreslår, at der etableres en varslingstjeneste for SMV'er (SMV-CERT).

**Forslag relateret til CFCS' organisering: Styrket civil forankring**
En række af erhvervs- og brancheorganisationerne påpeger i deres høringssvar, at CFCS' nuværende organisering og kultur ikke kan levere på den øgede åbenhed og videndeling med den private sektor, som er nødvendig.

Flere interessenter peger på, at en stærkere civil forankring af CFCS vil kunne styrke den virksomhedsrettede indsats. Flere interessenter bemærker samtidig, at det fortsat er vigtigt, at CFCS' efterretningsbaserede oplysninger kan stilles til rådighed for en potentielt ny enhed uden for FE. Hertil bemærker de fleste af interessenterne, at de dog er opmærksomme på, at det ikke er sikkert, at en enhed uden for FE vil kunne få adgang til disse data. Det påpeges ligeledes, at der bør tages højde for, hvorvidt der risikeres kompetencetab og rekrutteringsudfordringer ved en reorganisering af CFCS.

I en række af høringssvarene foreslås ligeledes en reorganisering i forhold til teleopgaverne, så tilsyn og rådgivningsfunktionen ikke er placeret ved samme myndighed.

Herudover nævner flere interessenter, at der er behov for en større analyse af hele cybersikkerhedsområdet i forhold til, hvordan den virksomhedsrettede indsats skal indrettes og forankres, end indeværende analyse har mandat til.

## CFCS' erfaringer med det virksomhedsrettede samarbejde

Dette afsnit beskriver CFCS' egen erfaring og perspektiver på samarbejdet med den private sektor og er tematisk struktureret i lighed med ovenstående gennemgang. Afsnittet præsenterer desuden forslag til at imødekomme og løse de udfordringer, der ses i forhold til samarbejdet.

### Hovedtendenser

**Tendens 1: Uklarhed om roller og ansvar i relation til virksomhedsrettede opgaver**
CFCS bemærker, at centerets opgaver rettet mod den private sektor fokuserer på virksomheder, der understøtter samfundsvigtige funktioner. CFCS oplever dog, at en lang række virksomheder jævnligt udtrykker ønske om, at CFCS også påtager sig en rolle i forhold til deres grundlæggende IT-sikkerhed og eksempelvis udarbejder specifikke trusselvurderinger for den enkelte virksomhed.

CFCS bemærker, at der er usikkerhed om CFCS' rolle, og at usikkerheden herom kan give anledning til tvivl i relation til grænsedragningen mellem CFCS og Erhvervsstyrelsen, som også løser opgaver på området.

**Tendens 2: Vejledning, videndeling og dataindsamling**
CFCS oplever, at virksomhederne ser en stor værdi i, at CFCS som en del af FE arbejder trussels- og efterretningsbaseret.

CFCS bemærker, at centeret over tid har opbygget en tæt relation til de væsentligste virksomheder i de samfundskritiske sektorer, og at virksomhederne løbende trækker på CFCS' tværsektorielle viden og erfaring samt selv deler viden og deltager i øvelser.

CFCS understreger, at centeret altid bestræber sig på at stille relevant viden til rådighed på så lavt et klassifikationsniveau som overhovedet muligt. CFCS påpeger, at der i den forbindelse tages hensyn til statens, allierede staters, koncernens og enkeltpersoners sikkerhed.

CFCS er opmærksomme på, at nogle virksomheder er forbeholdne ift. at dele data med CFCS grundet en bekymring for, at dataene deles med det øvrige FE. CFCS tager bekymringen alvorligt og henviser til, at Forsvarsministeriet har fastsat særdeles snævre rammer for, hvornår data omfattet af CFCS-lovens kapitel 4 kan deles med det øvrige FE. CFCS bemærker endvidere, at der ikke har været tilfælde på manglende efterlevelse af videregivelsesreglerne.

**Tendens 3: CFCS' rolle i relation til telesektoren**
CFCS oplever et godt og tæt samarbejde med aktørerne i telesektoren, og at telesektoren blandt andet værdsætter den efterretningsbaserede rådgivning og videndeling, som CFCS tilbyder.

CFCS bemærker, at aktører i telesektoren har fremført, at det kan være en udfordring, at CFCS både udøver rådgivningsvirksomhed inden for cybersikkerhed, herunder i telesektoren, og samtidig er tilsynsmyndighed på teleområdet. CFCS oplever ikke den beskrevne udfordring i det daglige samarbejde med telesektoren.

CFCS finder i stedet, at den nuværende myndighedsrolle på teleområdet medfører, at implementeringen og håndhævelsen af den lovgivning, som er implementeret på teleområdet i relation til informationssikkerhed, beredskab og leverandørsikkerhed, er baseret på centerets løbende indsigt i aktuelle trusler, trusselsaktører og sårbarheder i sektoren. CFCS oplever endvidere, at en række udbydere ser en fordel i at få sikkerhedsgodkendt medlemmer af topledelsen med henblik på at få et indblik i netop den viden.

CFCS vurderer, at såfremt en anden myndighed vil skulle varetage CFCS' nuværende tilsynsopgaver på teleområdet, vil det medføre, at tilsynet ikke længere vil være baseret på en efterretningsbaseret indsigt i trusler og sårbarheder mod telesektoren.

Samtidig bemærker CFCS, at en henlæggelse af tilsynsfunktionen til en anden myndighed vil bevirke, at den omfattende række af hjemler, der sikrer CFCS' adgang til leverandøraftaler, beredskabsplaner mv., samt hjemler pålæg og straf, ikke længere vil være til rådighed for CFCS.

### Behov og tiltag

CFCS finder behov for en afklaring af CFCS' rolle, og at der sker en forventningsafstemning med den private sektor om, hvordan CFCS kan, bør og må

assistere de virksomheder, som ikke understøtter samfundsvigtige funktioner.

CFCS mener, at kendskabet til centerets arbejde bør styrkes, herunder hvilken rådgivning og øvrige ydelser, som centeret kan tilbyde og til hvilken type af virksomheder. CFCS foreslår at styrke kommunikationen om, hvorfor CFCS i nogle tilfælde ikke kan dele efterretningsbaseret viden, at nuancere kommunikationen til virksomhederne, så den i endnu højere grad tager højde for virksomhedernes virkelighed samt forbedre dialogen med brancheforeningerne om forventningerne til samarbejdet mellem CFCS og virksomhederne.

Det er CFCS' faglige anbefaling, at det ikke overvejes at foretage en opsplitning af tilsyns- og rådgivningsfunktionen på teleområdet, såvel strukturelt som organisatorisk, da CFCS vurderer, at det vil medføre, at der opstår uklarhed blandt teleudbyderene såvel som hos myndighederne om, hvilke krav der er fastsat på området. CFCS finder i stedet, at udfordringer adresseres af CFCS gennem mere entydig kommunikation og vejledning. Konkret vurderer CFCS, at der er behov for yderligere kommunikation til telesektoren om den organisatoriske opdeling mellem rådgivning og tilsyn i CFCS, herunder at skabe klarhed i dialogen med televirksomhederne i forhold til, om den sker i regi af centerets rådgivnings- eller tilsynsvirksomhed.

Herudover bemærker CFCS, at der i endnu højere grad skal sikres en kommunikation om, hvad sensordata anvendes til.

**HOVEDPOINTER VEDRØRENDE CFCS' SAMARBEJDE MED PRIVATE VIRKSOMHEDER**

- Erhvervs- og brancheorganisationerne oplever, at CFCS besidder en **høj faglighed** og **stærke kompetencer**, der er med til at **styrke Danmarks cybersikkerhed.**
- Høringssvarene fra erhvervs- og brancheorganisationerne afspejler, at der er **uklarhed** omkring CFCS' ansvar over for den private sektor og **snitfladerne** mellem de statslige myndigheder på cyberområdet. CFCS bemærker ligeledes, at der kan være behov for en **forventningsafstemning** og **tydeligere kommunikation** om centrets rolle i relation til virksomheder, der ikke understøtter samfundsvigtige funktioner.
- Erhvervs- og brancheorganisationerne afvejer på forskellig vis ønsket om en **større åbenhed** på den ene side og efterspørgslen på e**fterretningsbaseret viden** på den anden side. Flere af interessenterne peger på, at en stærkere **civil forankring** af CFCS vil kunne styrke den virksomhedsrettede indsats.
- CFCS bemærker, at de altid bestræber sig på at stille relevant viden til rådighed på **så lavt et klassifikationsniveau** som overhovedet muligt, og at datadelingen mellem CFCS og det øvrige FE **er reguleret** i CFCS-loven.
- Flere af bidragene peger på et behov for en **større analyse af cyberområdet** for at kunne fastlægge en mere effektiv virksomhedsbaseret indsats på området.
- En række af erhvervs- og brancheorganisationerne nævner i deres høringssvar, at **CFCS' mange roller på teleområdet er uhensigtsmæssig**.
- CFCS påpeger, at den **nuværende myndighedsrolle** på teleområdet medfører, at implementeringen og håndhævelsen af den lovgivning, som er implementeret på teleområdet i relation til informationssikkerhed, beredskab og leverandørsikkerhed, er **baseret på centerets løbende indsigt i aktuelle trusler,** trusselsaktører og sårbarheder i sektoren.

# Forankringen af CFCS' virksomhedsrettede indsats - Fordele og ulemper

Med afsæt i analysens kommissorium belyses fordele og ulemper ved forankringen af CFCS' virksomhedsrettede opgaver ved FE i de følgende afsnit. Med afsæt i de tre hovedtendenser fra foregående afsnit kan der ligeledes opsummeres tre overordnede udfordringer for så vidt angår CFCS' virksomhedsrettede indsats: 1) Uklarhed om roller og ansvar i relation til virksomhedsrettede opgaver, 2) Vejledning, videndeling og dataindsamling, og 3) CFCS' rolle i relation til telesektoren. På baggrund af kortlægningen af CFCS' opgaver og snitflader samt de belyste erfaringer i forhold til samarbejdet med CFCS, analyseres og diskuteres først de tre hovedudfordringer. Forsvarsministeriet foreslår på den baggrund to mulige løsninger: En organisatorisk status quo eller en ny forankring af de virksomhedsrettede opgaver andet steds i Forsvarsministeriets koncern. Med henblik på en drøftelse af analysens resultater i forsvarsforligskredsen, præsenteres de primære fordele og ulemper ved de to løsningsforslag.

## Udfordringer vedrørende CFCS' virksomhedsrettede indsats

**Udfordring 1:**
**Uklarhed om roller og ansvar**

**UDFORDRING**

Høringssvarene viser, at interessenterne har en opfattelse af, at der er uklarhed om fordelingen af ansvar og opgaver i forhold til den virksomhedsrettede indsats på cybersikkerhedsområdet. Der er eksempelvis tvivl om, hvor man som virksomhed kan henvende sig, og hvilken hjælp man kan forvente fra forskellige myndigheder, hvis man rammes af en cybersikkerhedshændelse.

Kortlægningen i første del af analysen viste, at en række myndigheder har ansvaret for den virksomhedsrettede myndighedsindsats på cyberområdet. Derfor skal udfordringen, som interessenterne oplever med en uklarhed omkring ansvarsfordelingen ift. virksomhederne, også løses af alle de relevante myndigheder. I relation til CFCS' bidrag til løsningen af udfordringen kan en række indsats- og opmærksomhedspunkter fremhæves. Disse analyseres i de tre følgende afsnit.

**Behov for styrket kommunikation om CFCS' ansvar og opgaver**
Høringssvarene understreger, at der efterspørges klar viden og kommunikation om rækkevidden af CFCS' virksomhedsrettede opgaver. Der mangler i høj grad kommunikation om, at CFCS' indsats primært er rettet mod virksomheder, der understøtter samfundsvigtige funktioner, hvor andre øvrige opgaver på området eksempelvis ligger i Erhvervsstyrelsen eller hos Politiet. Misforståelsen gælder særligt i relation til CFCS' begrænsede funktion i forhold til SMV'er.

Der kan med fordel iværksættes et øget kommunikationsfokus vedrørende CFCS' rolle og ansvar i relation til private virksomheder, samt oplysning om hvor virksomheder uden samfundsvigtig funktion i stedet kan søge rådgivning og hjælp. Hvor det er statens ansvar at varetage den nationale sikkerhed, har virksomheder og myndigheder et ansvar for at varetage sikkerheden i egen organisation. Det er derfor vigtigt, at der både kommunikeres om, hvad CFCS' ansvar er, men også om det ansvar der påhviler myndigheder og virksomhederne selv som følge af sektoransvarsprincippet.

I relation til udfordringen med viden om roller og ansvar for de virksomhedsrettede opgaver på cyberområdet, skal det bemærkes, at etableringen af Cyberhotlinen forankret hos Erhvervsstyrelsen og Digitaliseringsstyrelsen forventes at imødekomme usikkerheden om rollefordelingen blandt myndigheder i forhold til den virksomhedsrettede indsats samt kan

hjælpe virksomheder til den rette hjælp.

**Eksisterende tiltag skal have tid til at få effekt**
En lang række initiativer er iværksat på cyberområdet, hvor flere er forankret i Erhvervsstyrelsen, jf. s. 13. En stor del af initiativerne imødekommer de behov og udfordringer, der italesættes i høringen af erhvervs- og brancheorganisationerne, og en styrket kommunikation om initiativernes iværksættelse vil kunne skabe større opmærksomhed om de nye tiltag og deres formål.

I nedenstående figur fremhæves de initiativer på cybersikkerhedsområdet målrettet private virksomheder fra figuren s. 13, som forventes at imødekomme en stor del af de behov og udfordringer, der påpeges i interessenthøringen.

**INITIATIVER PÅ CYBERSIKKERHEDSOMRÅDET RELATERET TIL PRIVATE VIRKSOMHEDER***

| Behov påpeget i høring af interesse- og brancheorganisationer | Nuværende og igangsatte initiativer, der forventes at imødekomme interessentbehov |
|---|---|
| Videndeling og vejledning | Trusselsvurderinger og vejledninger målrettet digital infrastruktur, der understøtter samfundsvigtige funktioner |
| | Sikkerdigital.dk |
| | One-stop-shop digitalt rådgivnings- og undervisningsbibliotek på CFCS' hjemmeside |
| Vejledning målrettet SMV'er | Virksomhedsrettede informationskampagner om cyber- og informationssikkerhed |
| Styrket videndeling<br>Facilitering af offentlig-privat samarbejde<br>Netværk | Strategisk Samarbejdsforum for Cybersikkerhed, Bestyrelsesforeningen, Danish Hub for Cybersecurity, Virksomhedsforum for Digital Sikkerhed, Cybersikkerhedsrådet |
| | Årlig konference om cybersikkerhed |
| Imødekommelse af uklarhed om rollefordeling<br>Oplysning om relevante myndigheder i forbindese med cybersikkerhedshændelser | Cyberhotline |
| Øget støtte til SMV'ere<br>SMV-CERT/SMV varslingstjeneste | Pulje på 50 mio. til at styrke cybersikkerheden i SMV'er i regi af SMV:Digital |
| | Etablering af en Cybersikkerhedsenhed for SMV'er |
| | Etablering af et nationalt koordinationscenter for cybersikkerhedsindustri, - teknologi og –forskning |
| Udveksling af data<br>Styrket videndeling | Cybersikkerhedspagt |
| Branchespecifikke netværk<br>Operationel videndeling<br>Offentlig-privat samarbejde | Etablering af branchespecifikke fora mhp. øget praksisnær videndeling mellem det offentlige og private aktører om hændelser og trusler |

* Initiativerne og kompetent myndighed beskrives i første del af analysen.

**Et område i hastig udvikling**
Cyberområdet er i konstant udvikling, hvilket medfører et behov for en løbende vurdering af initiativer og indsatser. Det er et opmærksomhedspunkt, der i høj grad er relevant i imødekommelsen af uklarheden om fordelingen af ansvar og opgaver, også henset til at der fremadrettet må forventes endnu flere snitflader på cyberområdet samt en større bevidsthed om bredden på cybersikkerhed.

Udviklingen i nye teknologier, såsom kvantecomputeren, afstedkommer øgede krav til sikkerheden. Samtidig viser eksempelvis revideringen af NIS-direktivet, at robustheden mod cyberangreb også forventes styrket i internationalt regi. Fremtidens cyber- og informationssikkerhed fordrer dermed, at organiseringen af- og tiltagene på cybersikkerhedsområdet understøtter et tilsvarende stærkt cyberforsvar. Det stiller krav til, at cybersikkerhedsområdet tilpasses i takt med udviklingen og trusselsbilledet.

**Udfordring 2:**
**Vejledning, videndeling og dataindsamling**

**UDFORDRING**

Erhvervs- og brancheorganisationerne ønsker generelt mere videndeling, rådgivning, åbenhed og hyppigere afklassificering af data fra CFCS. Samtidig er der en (modsatrettet) kritik af, at CFCS ikke må være konkurrenceforvridende i forhold til de virksomheder, der lever af at udarbejde trusselsvurderinger og rådgivning om cybersikkerhed. Herudover er flere virksomheder forbeholdende med at dele viden med en efterretningstjeneste, om end de fleste fortsat ønsker, at CFCS' arbejde tager udgangspunkt i efterretningsdata.

CFCS' arbejde med klassificeret information italesættes bredt i interessenthøringen som den største barriere i forhold til at øge delingen af viden og data mellem CFCS' og virksomhederne. I de følgende afsnit belyses både betydningen af CFCS' arbejde med efterretningsdata samt de forhold og muligheder, som gør sig gældende for CFCS' videndeling.

**Efterretningsdata og klassificeret information**
Adgangen til efterretningsdata og højt klassificerede oplysninger giver CFCS en unik indsigt i det internationale trusselsbillede og udenlandske aktører. FE vurderer, at adgangen er afgørende for, at CFCS kan levere den optimale beskyttelse af Danmark mod avancerede cyberangreb.

**FE UDTALER OM CFCS' PLACERING VED FE:**

*"Med placeringen ved FE har CFCS adgang til højt klassificerede efterretningsoplysninger, som er afgørende for at kunne levere den optimale beskyttelse af Danmark mod avancerede cyberangreb. De fleste alvorlige cyberangreb kommer fra udlandet, og FE har som udenrigsefterretningstjeneste en særlig fortrolig viden om avancerede cyberangreb, og hvem der står bag. Placeringen ved FE giver centeret adgang til tjenestens unikke viden. Viden om den slags trusler er højt klassificeret og ville ikke kunne deles med centeret, hvis det lå et andet sted. Det er i den forbindelse ofte et væsentlig hensyn, at FE's partnertjenester i udlandet kan have tillid til, at oplysninger, de deler med FE – og dermed også CFCS – ikke tilgår andre myndigheder. CFCS drager derudover også nytte af de højt specialiserede kompetencer, som FE har på området for cyber- og informationssikkerhed.*

*Selv om centret og den efterretningsmæssige del af FE tilsammen udgør én myndighed, er de gennem lovgivningen tillagt forskellige opgaver og virkemidler. Mens FE kan dele efterretningsmæssige oplysninger af betydning for cybersikkerheden uden begrænsning med CFCS, gælder det ikke den anden vej. Der er således fastsat en række begrænsninger for CFCS' udveksling af data med FE.*

*Det er vurderingen, at Danmark opnår en væsentlig fordel ved at have samlet centrale opgaver omkring cybersikkerhed i netop CFCS, samt ved at have placeret centeret som en del af FE. En anden myndighed ville med sikkerhed ikke kunne opnå samme adgang til de efterretningsmæssige oplysninger, der er afgørende for at kunne beskytte Danmark mod avancerede cyberangreb."*

Som det fremgår af FE's udtalelse, kommer alvorlige trusler især fra udenlandske og ofte statslige aktører, hvorfor adgangen til efterretningsdata er afgørende. Det var netop et af kerneargumenterne for placeringen af CFCS ved FE, da centeret blev etableret.

CFCS' efterretningsbaserede arbejdsmetode er ligeledes relevant i relation til bekymringen for, at CFCS er konkurrenceforvridende. CFCS' adgang til efterretningsdata giver en unik viden om aktører og trusselsbilledet. Da kommercielle udbydere ikke arbejder efterretningsbaseret, vil de heller ikke kunne tilbyde samme type cybersikkerhedsløsninger som CFCS. CFCS' cybersikkerhedsløsninger fungerer som et supplerende lag IT-sikkerhed. De kan ikke erstatte behovet for øvrig IT-sikkerhed og udgør dermed ikke et alternativ til private løsninger.

**Efterretningskultur og mytedannelse**

En del af udfordringen i forhold til videndeling er en opfattelse af ulige informationsudveksling parterne imellem, jf. s. 17. Begge udlægninger belyser, at der fra alle parter er en efterspørgsel på mere videndeling, samtidig med at der er uoverensstemmelse om, hvad videndeling indebærer for parterne.

Årsagen til denne uoverensstemmelse afspejles i en generel opfattelse blandt interessenterne om, at CFCS har en lukket efterretningskultur, hvorfor de er tilbageholdne med al datadeling. I høringssvarene kan der aflæses en bekymring for, at CFCS tilbageholder viden og data, som kunne styrke sikkerheden hos virksomhederne, hvis den blev gjort tilgængelig, eller at den data, CFCS indsamler gennem eksempelvis netsikkerhedstjenesten, videregives til FE til anden brug.

Der er klar lovgivning og retningslinjer for, hvordan CFCS må og skal behandle data, herunder i forhold til muligheden for at videregive data til andre myndigheder eller det øvrige FE.

**DATADELING MED DET ØVRIGE FE**

De oplysninger, som CFCS indsamler fra myndigheder og virksomheder tilsluttet netsikkerhedstjenesten, kan kun i helt særlige tilfælde udveksles med den øvrige del af FE. Sådanne udvekslinger af data, der er omfattet af CFCS-lovens kapitel 4, er reguleret af administrative retningslinjer udstedt af Forsvarsministeriet. Data omfattet af CFCS-lovens kapitel 4 udveksles således kun i et meget begrænset omfang, og i overensstemmelse med en særlig godkendelsesproces, med den øvrige del af FE.

Herved sikres det, at udveksling af oplysninger, CFCS har tilvejebragt på baggrund af indgreb i meddelelseshemmeligheden og andre indgreb omfattet af grundlovens § 72, er underlagt snævre retlige rammer.

På baggrund af CFCS' placering ved en efterretningstjeneste må der forventes en vis informationsasymmetri i samarbejdet med den private sektor, og denne kan være medvirkende til mindsket tillid og misforståelser omhandlende blandt andet videndeling og dataindsamling.

**Kommunikation og kulturændring**

Uoverensstemmelsen mellem virksomhederne og CFCS' forventninger til, hvad CFCS bør og kan dele af viden indikerer, at der først og fremmest er behov for en styrket kommunikation og afstemning parterne imellem. Kommunikationen kan med fordel aktivt skabe en bedre forståelse for CFCS' virke og lovgrundlag, herunder i forhold til samarbejdet med det øvrige FE. Herudover kan kommunikationen om klassificeret data styrkes, og CFCS bemærker eksempelvis, at de kan styrke deres kommunikation i forhold til, hvorfor de i nogle tilfælde ikke kan dele efterretningsbaseret viden.

I forlængelse af en øget kommunikationsindsats vil man aktivt kunne arbejde på at skabe en mere åben og civil kultur for den del af CFCS, der arbejder med de virksomhedsrettede opgaver. Her vil man kunne lade sig inspirere af Storbritannien, hvis nationale cybercenter også er forankret under en efterretningstjeneste. I Storbritannien har man gennem en omfattende kulturændring haft succes med at skabe en stærk gensidig tillid mellem cybercenteret og virksomheder, samtidig med at man gennem forankringen har bibeholdt adgangen til efterretningsdata.

Bedre kommunikation, større åbenhed på relevante områder (fysisk såvel som kommunikativ åbenhed) og forventningsafstemning med private virksomheder kan være med til skabe en mere åben profil og en bedre forståelse for begge parters virkeligheder, men også et mere tillidsfuldt samarbejde på trods af en fortsat informationsasymmetri grundet CFCS' placering ved FE.

**NATIONAL CYBER SECURITY CENTER I STORBRITANNIEN**

Storbritannien centraliserede i 2016 cybersikkerhedsområdet i National Cyber Security Centre (NCSC), der er placeret ved efterretningstjenesten GCHQ. NCSC arbejder bredt med cybersikkerhed og er *single point of contact* for både borgere, virksomheder og myndigheder. I tilfælde af cyberhændelser håndterer NCSC som udgangspunkt kun de hændelser, som er af national betydning. Andre hændelser skal fortsat håndteres af den myndighed, virksomhed eller borger, der rammes, ligesom at anmeldelse sker til politiet.

Placeringen af NCSC under efterretningstjenesten, GCHQ, skyldes et ønske om at samle kompetencerne ét sted med højest mulig cybereksperti se, adgang til klassificerede oplysninger og hensynet til samarbejde med andre landes efterretningstjenester. Før centraliseringen af cyberkompetencerne i NCSC oplevede man i Storbritannien, at videndeling mellem GCHQ og andre myndigheder ofte var langsommelig og bureaukratisk, men også præget af en tilbageholdenhed fra efterretningstjenesten, da der var usikkerhed i forhold til hvad og hvordan, informationen blev anvendt.

I placeringen af NCSC ved GCHQ var der stor opmærksomhed på at skabe en tillidsfuld og åben relation til både borgere, virksomheder og andre myndigheder. I NCSC har man derfor arbejdet målrettet på kommunikationsindsatsen, herunder ved at udarbejde lettilgængelige vejledninger samt skabe forståelse for centerets kompetencer, opgaver og ansvar. Herudover arbejder NCSC konkret med et koncept kaldet Industry100, hvor godkendte virksomheder kan indstationere relevante medarbejdere hos centeret. Endelig er NCSC fysisk placeret separat fra GCHQ, og man kan som virksomhed eller privat borger få adgang til centeret uden sikkerhedsgodkendelse.

**Afklassificering og deling af klassificeret viden**

Blandt høringssvarene italesættes en opfattelse af, at CFCS i højere grad burde afklassificere information med henblik på at dele denne med den private sektor. Der gælder helt specifikke regler for, hvordan information klassificeres og potentielt afklassificeres, jf. s. 16. CFCS bestræber sig på at dele viden på så lavt et klassifikationsniveau som muligt.

En anden måde at øge videndelingen med den private sektor vil være at anvende og evt. udbygge de eksisterende fora, hvor CFCS har mulighed for at dele klassificeret information med sikkerhedsgodkendte medarbejdere fra virksomhederne. CFCS' koncept Strategisk Samarbejdsforum samler eksempelvis sikkerhedsgodkendte repræsentanter fra samfundskritiske virksomheder og brancheorganisationer med henblik på at give regelmæssig indsigt i centerets klassificerede viden.

**Udfordring 3:**
**CFCS' rolle i relation til telesektoren**

**UDFORDRING**

Nogle af erhvervs- og brancheorganisationerne italesætter, at der er udfordringer i relation til CFCS' rolle over for telesektoren som både rådgivende og tilsynsmyndighed, da denne dobbeltrolle hindrer et hensigtsmæssigt og tillidsfuldt samarbejde mellem televirksomhederne og CFCS.

**Dobbeltrolle i relation til telesektoren**
Som belyst på s. 11 har CFCS, som myndighed for informationssikkerhed og beredskab på teleområdet, ansvaret for at stille sikkerhedskrav til teleudbydere, føre tilsyn på området og rådgive samfundets beredskabsaktører om teleberedskab. Denne dobbeltrolle italesættes af nogle af interessenterne som problematisk, jf. s. 17, hvor der argumenteres for, at CFCS som tilsynsmyndighed ikke bør have adgang til data om teleudbyderne, som deles med CFCS i form af deres rådgivende indsats samt gennem netsikkerhedstjenestens prober.

CFCS' opgaver på teleområdet er placeret i CFCS' afdeling for rådgivning og standarder. Sektionen, som blandt andet rådgiver telesektoren, er adskilt fra den sektion, som gennemfører tilsynsaktiviteter på teleområdet. Herudover er DCIS'en jf. s. 10 på teleområdet, placeret uden for CFCS og har primært til opgave at facilitere generel videndeling om risici og sårbarheder på teleområdet.

Nogle af interessenterne finder det endvidere uhensigtsmæssigt, at tilsynsmyndigheden er placeret hos en efterretningstjeneste og ikke ved en civil del af forvaltningen, jf. s. 17. Bekymringen relateret til de efterretningsmæssige forhold skal sandsynligvis i højere grad ses i forlængelse af den generelle bekymring om forankringen, jf. s. 16, end den er bundet op på placeringen af tilsynet specifikt.

Som det gør sig gældende for CFCS' øvrige opgaver, giver adgangen til efterretningsbaseret viden ligeledes CFCS et indblik i truslen mod telesektoren og dermed stærke forudsætninger for at rådgive med henblik på at styrke cybersikkerheden i televirksomhederne. Jf. s. 11 er det endvidere på baggrund af CFCS' viden om efterretninger, at CFCS er valgt som den myndighed, der i særlige tilfælde kan forbyde konkrete leverandøraftaler samt anvendelse af kritiske komponenter og systemer i den kritiske teleinfrastruktur.

**CFCS UDTALER OM KONSEKVENSERNE VED EN FLYTNING AF TILSYNET:**

*"En henlæggelse af tilsynsfunktionen til en anden myndighed vil bevirke, at den omfattende række af hjemler, der sikrer CFCS adgang til leverandøraftaler, beredskabsplaner mv., samt hjemler vedrørende pålæg og straf, ikke længere vil være til rådighed for CFCS. CFCS vil hermed være afskåret fra at opretholde den nuværende grad af indsigt i de enkelte teleudbyderes forhold, sikkerhedsniveau mv. Uden denne indsigt vurderer CFCS, at CFCS reelt vil være afskåret fra at varetage opgaverne fastsat i Lov om leverandørsikkerhed i den kritiske teleinfrastruktur, herunder vurderingen af sikkerheden i udrulningen af 5G.*

*Loven om leverandørsikkerhed er en overbygning til de øvrige regler på området, og en ændring af forankringen af disse opgaver vurderes at medføre en væsentlig forringelse i mulighederne for at understøtte sikkerheden i den kritiske teleinfrastruktur.*

*CFCS bemærker mere generelt, at ingen anden myndighed end CFCS har en tilsvarende efterretningsbaseret indsigt i den aktuelle cybertrussel mod telesektoren samt erfaring med tilsyn. Det kan oplyses, at CFCS har verserende sager klassificeret HEMMELIGT eller derover, hvor anvendelse af ovennævnte hjemler, kombineret med den efterretningsmæssige indsigt, har afgørende betydning for sagsoplysningen."*

**Tydeligere adskillelse mellem tilsyn og rådgivning samt øget kommunikation**
Samlingen af både rådgivning og tilsyn med efterlevelse af krav hos samme myndighed er anvendt flere steder i staten, og at CFCS har flere roller over for telesektoren er således ikke en unik model.

Usikkerheden blandt televirksomhederne om, hvornår CFCS giver rådgivning, og hvornår CFCS stiller krav som tilsynsmyndighed kræver først og fremmest en øget dialog mellem CFCS og telesektoren. CFCS kan styrke kommunikationen om, hvordan oplysningerne i netsikkerhedstjenesten benyttes, og hvorvidt disse udveksles med tilsynsenheden i CFCS. Samtidig vil en øget videndeling med televirksomhederne om baggrunden for tilsynsenhedens krav skabe transparens og indsigt i fordelene ved at have samlet både rådgivning og tilsyn hos CFCS. Bekymringen relateret til placeringen ved FE kan ligeledes forsøges imødekommet gennem en kulturændring og en øget kommunikation om, hvordan CFCS eksempelvis håndterer datadeling mm., som det er foreslået i tidligere afsnit.

Herudover kan en tydeliggørelse af den interne adskillelse mellem den rådgivende del og tilsynsdelen i CFCS bidrage til at sikre klarere linjer mellem deres funktioner samt i forhold til udvekslingen af oplysninger.

## Forsvarsministeriets forslag til den fremadrettede organisering

På baggrund af de belyste udfordringer og de forhold og muligheder, der er relevante for at imødekomme disse, præsenteres afslutningsvis fordele og ulemper ved enten en organisatorisk status quo eller ved en flytning af CFCS' virksomhedsrettede indsats til et andet sted under Forsvarsministeriets ressort. Det vurderes, at hver af de to løsninger adresserer en række af de udfordringer ved CFCS' virksomhedsrettede indsats, som påpeges i erhvervs- og branche-organisationernes høringssvar.

**Organisatorisk status quo**
Den første løsning er en organisatorisk status quo, hvor der ikke ændres ved placeringen af CFCS' virksomhedsrettede indsats ved FE, herunder i forhold til rollerne på teleområdet, men hvor indsatsen styrkes inden for eksisterende rammer.

Nedenstående figur giver et overblik over de væsentligste fordele og ulemper ved en organisatorisk status quo.

**FORDELE OG ULEMPER VED ORGANISATORISK STATUS QUO**

| Fordele | Ulemper |
|---|---|
| • Bedst mulige adgang til efterretningsdata:<br>  ▪ Giver stærkest mulige indblik i det internationale trusselsbillede og dets aktører<br>  ▪ CFCS' produkter vil adskille sig fra produkter, der udbydes på det private marked<br>• Samling af begrænsede specialiserede kompetencer<br>• Ingen yderligere fragmentering af cybersikkerhedsområdet | • Manglende videndeling fra CFCS grundet klassifikation<br>• Opfattelse af en lukket efterretningskultur:<br>  ▪ Medfører informationsasymmetri i samarbejdsrelationen<br>  ▪ Medfører mytedannelse om CFCS' arbejde<br>• Udfordringer med gensidig tillid<br>• Tilbageholdenhed i forhold til at dele data med CFCS, herunder tilslutning til netsikkerhedstjenesten |

Som det indikeres i figuren s.27, vil man ved løsningen bibeholde adgangen til efterretningsdata, som er afgørende for CFCS' arbejde med at styrke cybersikkerheden for den kritiske infrastruktur og mod avancerede cyberangreb. Herudover fragmenteres cybersikkerhedsområdet ikke yderligere og skaber større usikkerhed om rolle- og ansvarsfordeling. Til sidst er det relevant at påpege, at man beholder synergieffekten ved at have samlet de specialiserede kompetencer i en tid, hvor der er stor mangel på kvalificeret arbejdskraft på området.

Forsvarsministeriet vurderer, at flere af ulemperne kan adresseres gennem en række tiltag og indsatser. Det omfatter primært en identitets- og kulturændring, klarere kommunikation og forventningsafstemning, tydeligere intern adskillelse af rådgivnings- og tilsynsfunktionen på teleområdet, samt udvidelsen af initiativer, der muliggør deling af klassificeret information. Herudover vurderes det, at en fuld implementering af eksisterende tiltag fra blandt andet Cyberaftalen og NCIS'en, som blev præsenteret i første del af analysen, vil have positiv indvirkning på området.

På trods af adresseringen af udfordringerne, vil der forventeligt være en resterende ulempe i form af eksempelvis forbeholdenhed i forhold til deling af data med CFCS, som udtrykt i branche- og erhvervsorganisationernes høringssvar. Her henviser Forsvarsministeriet først og fremmest til den eksisterende lovgivning, der regulerer datadeling mellem CFCS og det øvrige FE. Herudover vil en afledt effekt af den styrkede kommunikation og en kulturændring forventeligt være større tillid til CFCS' datahåndtering.

**Ny forankring under Forsvarministeriet**
Som alternativ til den nuværende organisation kan den virksomhedsrettede indsats flyttes ud af CFCS (og FE) og placeres et sted i Forsvarsministeriets øvrige koncern. Alternativt kan der oprettes en ny enhed under Forsvarsministeriet til varetagelsen af CFCS' virksomhedsrettede opgaver.

Nedenstående figur giver et overblik over de væsentligste fordele og ulemper.

**FORDELE OG ULEMPER VED NY FORANKRING UNDER FORSVARSMINISTERIET**

| Fordele | Ulemper |
|---|---|
| • Mulighed for mere åben kultur og identitet<br>• Bedre forudsætning for gensidig tillid og datadeling fra virksomheder<br>• Fortsat adgang (om end mere begrænset) til efterretningsdata<br>• Bedre mulighed for videndeling | • Yderligere fragmentering af cybersikkerhedsområdet og -kompetencer<br>• Begrænset adgang til efterretningsdata<br>• Fortsat begrænset videndeling grundet klassifikation<br>• Risiko for konkurrenceforvridende opgaver<br>• Risiko for opbygning af parallelle kapaciteter og nedsat kvalitet af opgaveløsningen |

En placering af CFCS' virksomhedsrettede opgaver væk fra FE vil give bedre forudsætninger for en mere åben kultur og identitet og dermed en større gensidig tillid i samarbejdet med virksomhederne. Omvendt vurderes det, at der fortsat vil være et behov for en aktiv kommunikationsindsats og kulturændring, da størstedelen af medarbejderne fra CFCS, og dermed FE, i givet fald vil blive flyttet med opgaverne, samt at opgaverne fortsat er forankret ved Forsvarsministeriet.

Ved at placere CFCS' virksomhedsrettede opgaver et andet sted i Forsvarsministeriets struktur bibeholder man en adgang til efterretningsdata, som ikke er mulig uden for Forsvarsministeriets ressort. Adgangen vil dog være stærkt begrænset sammenlignet med den direkte adgang til alle FE's indhentningskapaciter, herunder partnersamarbejder samt efterretningsdata, som er muligt ved en forankring under FE. Samtidig vil en placering af opgaverne uden for FE ikke ændre på de forhold og regler, der gælder for deling af klassificeret viden.

Ligeledes er det relevant, at opgaverne og opgaveløsningen ikke må ændre karakter i en sådan grad, eksempelvis i forhold til den efterretningsbaserede arbejdsmetode, at opgaverne bliver konkurrenceforvridende.

Størstedelen af CFCS' opgaver er, jf. CFCS-loven, rettet mod både myndigheder og virksomheder, jf. tekstboks s. 11, hvilket kan få betydning for, hvordan den virksomhedsrettede indsats reelt kan flyttes ud af CFCS. Der er en risiko for, at man i udflytningen er nødsaget til at opbygge parallelle kapaciteter og kompetencer i den nye enhed og CFCS, for at alle opgaver fuldt ud kan løses. Samtidig vil der være en risiko for, at kvaliteten af de enkelte opgaver forringes, da hverken CFCS eller den nye enhed vil have et helhedsbillede over angreb mod myndigheder og virksomheder.

Herudover vil man fragmentere cybersikkerhedsområdet yderligere, hvilket ikke nødvendigvis vil bidrage positivt til afklaring af den usikkerhed, der foreligger om myndighedernes roller og ansvar i forhold til virksomhedsrettede opgaver. Der kan hertil være en risiko for dobbeltarbejde i forbindelse med den virksomhedsrettede indsats på cyberområdet blandt andre myndigheder. Samtidig kan der opstå problemer med rekruttering, da man spreder behovet for specialiserede kompetencer og mister de synergier, der er ved at samle ekspertisen. Det skal ligeledes bemærkes, at omfanget af de virksomhedsrettede opgaver ikke vurderes at være af en størrelse, hvor det vil være fordelagtigt at oprette en helt ny styrelse under Forsvarsministeriets koncern.

Det skal bemærkes, at hvis det besluttes at flytte én eller flere af CFCS' roller på teleområdet ud af CFCS, vil det blandt andet afskære CFCS fra fyldestgørende at leve op til centerets opgaver i regi af Lov om leverandørsikkerhed i den kritiske teleinfrastruktur.

Endvidere skal det bemærkes, at flytningen af opgaver fra CFCS med stor sandsynlighed vil kræve en lovændring af CFCS-loven, FE-loven eller evt. anden lovgivning afhængigt af den konkrete udformning af en ny enhed.

Forsvarsministeriet vurderer, at flere af ulemperne i denne løsning også vil kunne adresseres gennem en række initiativer rettet mod identitets- og kulturændring samt klarere kommunikation og forventningsafstemning. På trods af disse initiativer forventes der dog fortsat at være uadresserede ulemper – her i form af især den begrænsede adgang til efterretningsdata og dermed trusselsbilledet, risikoen for forringelse af opgaveløsningen i både en ny enhed og det resterende CFCS samt en spredning af statens begrænsede specialiserede kompetencer.

**HOVEDPOINTER VEDRØRENDE CFCS' VIRKSOMHEDSRETTEDE INDSATS**

- I relation til CFCS' virksomhedsrettede indsats kan der peges på **tre overordnede tendenser**, som udfordrer samarbejdet mellem CFCS og det private erhvervsliv: 1) **Uklarhed** om roller og ansvar i relation til virksomhedsrettede opgaver, 2) **Vejledning, videndeling og dataindsamling** og 3) CFCS' rolle i relation til **telesektoren**.

- **En række initiativer** er igangsat med National Strategi for Cyber- og Informationssikkerhed (**NCIS**) og **Delrapport om CFCS'** virke i relation til rådgivning, uddannelse, forskning og videndeling, der forventes at imødekomme en del af behov, der påpeges i høringssvarene fra branche- og erhvervsorganisationerne.

- CFCS' virksomhedsrettede indsats vil kunne styrkes ved enten at **fastholde den nuværende organisatoriske status quo** eller ved at flytte den virksomhedsrettede indsats ud af CFCS og **forankre indsatsen i Forsvarsministeriets øvrige struktur**.

- De to løsninger indeholder både fordele og ulemper, der skal afvejes ved en endelig beslutning. Forsvarsministeriet foreslår, at **analysens resultater drøftes i Forsvarsforligskredsen med henblik på at munde ud i en principbeslutning**.

## Noter

*1 Aftale om et styrket cyberforsvar. 24. juni 2021. https://fmn.dk/da/nyheder/2021/enighed-om-et-styrket-dansk-cyberforsvar/*

*2 Afsnit 1. og 2.1 i de almindelige bemærkninger til lovforslag nr. L 192 af 2. maj 2014 til lov om Center for Cybersikkerhed.*

*3 Jf. CFCS-lovens § 1, stk. 1.*

*4 Definition fra National Strategi for Cyber- og Informationssikkerhed 2022-2024*

*5 Afsnit 1., 2.1. og 3.1.2. i de almindelige bemærkninger til lovforslag nr. L 192 af 2. maj 2014 til lov om Center for Cybersikkerhed.*

*6 Afsnit 2.1. i de almindelige bemærkninger til lovforslag nr. L 215 af 27. marts 2019 om ændring af lov om Center for Cybersikkerhed, samt specielle bemærkninger til CFCS-lovens § 1, stk. 1*

*7 Jf. Kongelig resolution af 3. oktober 2011.*

*8 Jf. afsnit 2.1. og 3.1.2. i de almindelige bemærkninger til lovforslag nr. L 192 af 2. maj 2014 til lov om Center for Cybersikkerhed og afsnit 2.1. i de almindelige bemærkninger til lovforslag nr. L 215 af 27. marts 2019 om ændring af lov om Center for Cybersikkerhed.*

*9 Jf. § 2 i Forsvarsministeriets cirkulære nr. 9741 af 21. august 2019 om behandling af data i og fra Center for Cybersikkerheds netsikkerheds-tjeneste.*

*10 Jf. CFCS-lovens § 3, stk. 1. CFCS kan desuden i særlige tilfælde påbyde virksomheder, der har særlig samfundsvigtig karakter samt regioner og kommuner at blive tilsluttet, jf. stk. 4.*

*11 Jf. FE-loven § 1, stk. 3, de specielle bemærkninger til § 1, stk. 3 i lovforslag nr. L 163 af. 27. februar 2013 om lov om Forsvarets Efterretningstjeneste samt Justitsministeriets cirkulære nr. 10338 af 17. december 2014 om sikkerhedsbeskyttelse af informationer af fælles interesse for landene i NATO eller EU, andre klassificerede informationer samt informationer af sikkerhedsmæssig beskyttelsesinteresse i øvrigt.*

*12 Jf. lovbekendtgørelse nr. 153 af 1. februar 2021 om sikkerhed i net og tjenester, lov nr. 1156 af 8. juni 2021 om leverandørsikkerhed i den kritiske teleinfrastruktur og lov nr. 437 af 8. maj 2018 om sikker i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter mv.*

*13 I medfør af lov om sikkerhed i net- og informationssystemer for operatører af væsentlige internetudvekslingspunkter mv.*

*14 Jf. § 1 i lovbekendtgørelse nr. 836 af 7. august 2019 om Center for Cybersikkerhed.*

*15 Afsnit 2.1. i de almindelige bemærkninger til lovforslag nr. L 215 af 27. marts 2019 om ændring af lov om Center for Cybersikkerhed.*

*16 Jf. § 5, stk. 3, i lovbekendtgørelse nr. 153 af 1. februar 2021 om sikkerhed i net og tjenester.*

*17 Jf. Beredskabsloven kap. 5.*

*18 Jf. §§ 2 – 3 i lov om leverandørsikkerhed i den kritiske teleinfrastruktur.*

*19 De specielle bemærkninger til § 6 i lovforslag nr. L 190 af 10. marts 2021 til lov om leverandørsikkerhed i den kritiske teleinfrastruktur.*

*20 Jf. CFCS-lovens § 1, stk. 1.*

FORSVARSMINISTERIET

Holmens Kanal 9
1060 København K
DK - Denmark

Telefon + 45 7281 0000
E-mail: fmn@fmn.dk
www.fmn.dk