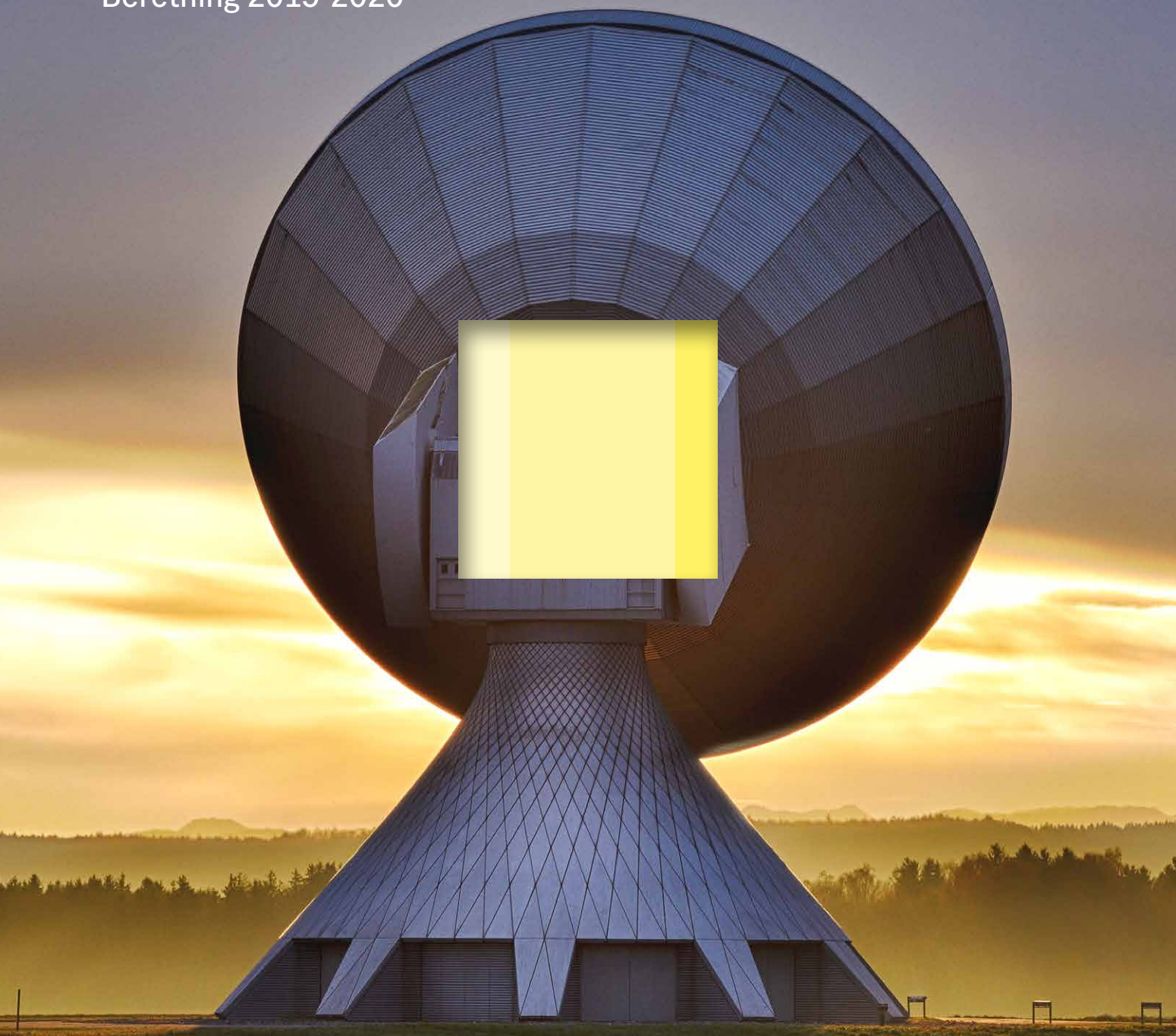
# INDBLIK

Beretning 2019-2020

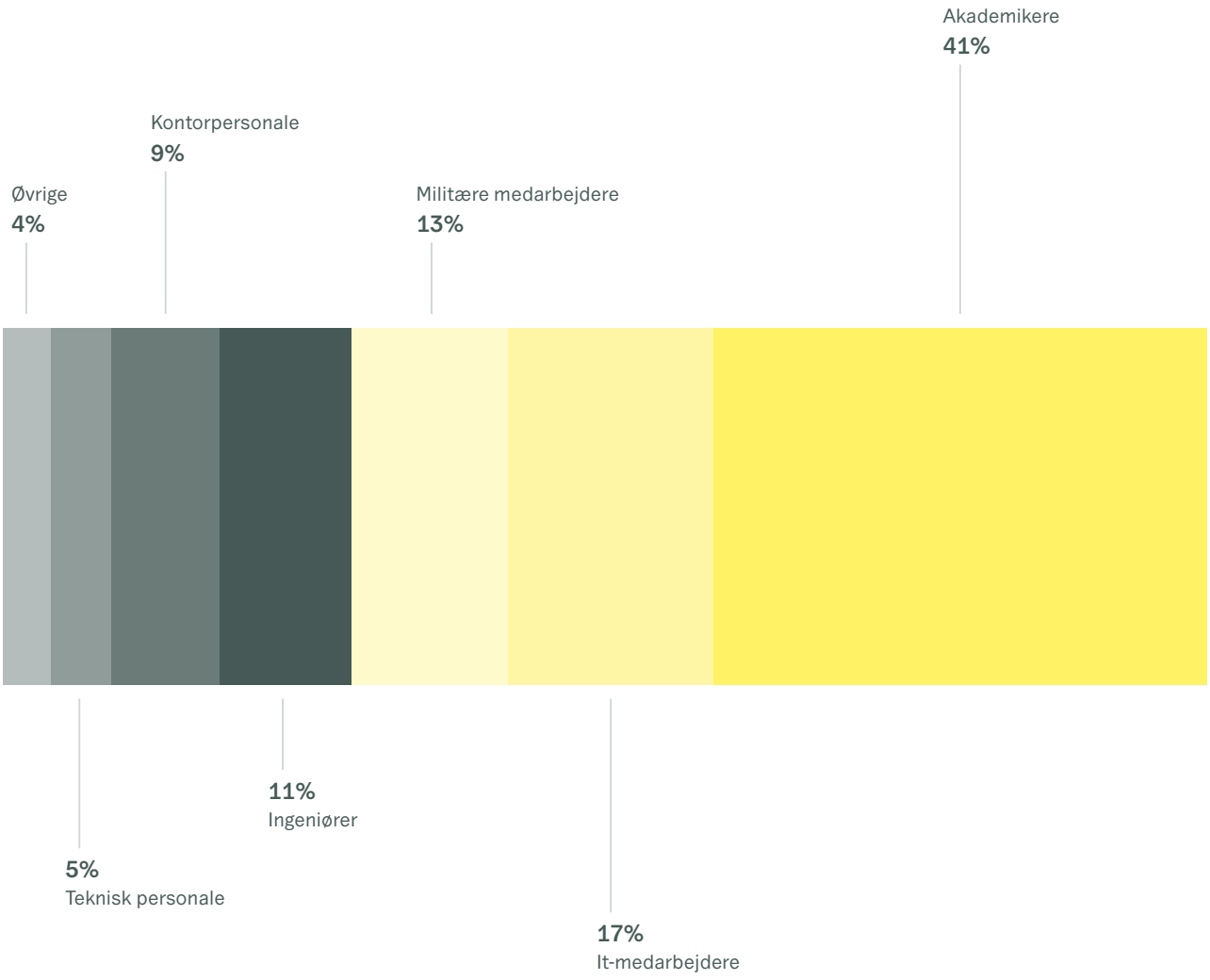


FORSVARETS
EFTERRETNINGSTJENESTE

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Telefon: 3332 5566
www.fe-ddis.dk
www.cfcs.dk

# FE'S MEDARBEJDERES BAGGRUND



FE klæder beslutnings-tagerne på, når de skal træffe beslutninger inden for udenrigs-, sikkerheds- og forsvarsområdet.

# INDHOLD

**SVEND LARSEN**

Fungerende chef
for Forsvarets
Efterretningstjeneste

# FORORD

2020 var et særligt år for FE. Vi var som resten af samfundet berørt af covid-19, og en nedlukning udgør en særlig udfordring for en tjeneste, hvor hjemmearbejde sjældent er muligt. Samtidig rettede Tilsynet med Efterretningstjenesterne kritik mod FE og mod dele af FE's indhentningskapaciteter. For en organisation som FE, hvor legalitet og compliance skal være centrale værdier, rammer en sådan kritik ekstra hårdt, og afføder umiddelbar opfølgning.

FE er en organisation, der ikke kan tillade sig at gå i stå. Heller ikke når det kommer til vores organisering. Danmark står over for et komplekst og dynamisk trusselsbillede, og det stiller store krav til vores måde at arbejde på. Derfor gennemførte vi i 2021 en organisationsændring, der skal forbedre anvendelsen af vores kapaciteter, styrke vores compliance og fremtidssikre it- og dataunderstøttelsen. Derudover skal organisationsændringen være med til at intensivere samarbejdet med Forsvaret, som er en af vores vigtigste kunder.

FE er med den nye organisering inddelt i tre operative og tre tværgående sektorer. Det er en ny måde at samarbejde på, men vi kan allerede nu se, at det har bidraget til at skabe et stærkere FE med et endnu skarpere fokus på vores kerneopgave: at beskytte Danmark og danske interesser mod trusler udefra.

FE har de seneste mange år været en højteknologisk og datadrevet arbejdsplads. Men de senere år er betydningen af teknologi og særligt den måde, vi håndterer data på, blevet helt afgørende for vores arbejde. Den teknologiske udvikling fører både nye udfordringer og muligheder med sig.

Vi er nødt til at styrke vores it- og datahåndtering, hvis vi skal have gavn af den store mængde data, vi indhenter, og vores nye organisering afspejler dette behov.

Cybertruslen er kommet for at blive, og med det seneste forsvarsforlig og reservepuljen har FE fået tilført flere midler til at imødegå den. Det betyder, at vi vil opruste yderligere på området. Vi bliver hele tiden dygtigere, men det gør vores modstandere også, og cybertruslen vil også i de kommende år være et af vores primære fokusområder.

Alt dette og meget mere kan du læse om i denne udgave af "Indblik". Vi udgiver "Indblik" for – så vidt vores særlige opgave tillader det – at give offentligheden et dækkende billede af, hvem FE er, og hvilke opgaver vi løser. Identiteten for langt de fleste af vores medarbejdere er hemmelig og skal vedblive med at være det. I år sætter vi imidlertid ansigt på nogle af de direktionsmedlemmer, som har ansvaret for centrale dele af vores arbejde.

Der er fortsat meget, vi ikke kan fortælle om, men jeg håber, at du alligevel vil føle dig klogere på vores arbejde med dette lille indblik i FE.

God læselyst og tak for interessen.

**Svend Larsen**
Fungerende chef for Forsvarets Efterretningstjeneste

# FE GØR DANMARK SIKKERT

FE klæder beslutningstagerne på, når de skal træffe beslutninger inden for udenrigs-, sikkerheds- og forsvarsområdet. Det gør vi på baggrund af efterretninger og særlig viden om forhold i udlandet, som kan have betydning for Danmark og danske interesser.

FE er Danmarks udenrigs- og militære efterretningstjeneste og arbejder – hemmeligt og åbent – for at beskytte Danmark og danske interesser i en foranderlig verden. FE's kapaciteter, viden og indsats er et afgørende fundament for Danmarks og danskernes sikkerhed.

Vi er ikke alene om at beskytte Danmark, men vi er den eneste myndighed, der har fået mandat til at udnytte helt særlige midler til at afdække, hvad andre stater og udenlandske aktører forsøger at holde hemmeligt.
Det giver mening for os at bidrage til fred, tryghed og sikkerhed for danskerne både i den analoge og i den digitale verden. Det gør vi ved at identificere, vurdere, rådgive om og i sidste ende modvirke trusler mod Danmark og danske interesser. For at løse den mission opererer vi i FE sammen – både ude og hjemme – og vi gør det dynamisk i forhold til et komplekst trusselsbillede, der konstant udvikler sig.

FE er en operativt orienteret vidensorganisation, og vi opnår meget af vores viden gennem målrettet og hemmeligt efterretningsarbejde. Vi har mange forskellige opgaver, og fælles for dem alle er det vidensgrundlag, som vores efterretningsarbejde skaber.

Vores ekstraordinære opgaver binder os sammen på tværs af den forskellighed i fag, alder, køn og etnicitet, vi har, og vi værdsætter styrken i vores mangfoldighed med dybe fagligheder og specialer.

Vi tror på værdien af en solid og ordentlig indsats i hvert eneste led i vores arbejde og på et efterretningshåndværk, hvor faglighed, troværdighed og integritet er afgørende faktorer. Og vi værner om den tillid, der ligger i de rammer, vi har fået som efterretningstjeneste og sikkerhedsmyndighed i et demokratisk samfund.

Vi bruger aktivt de muligheder, som den teknologiske udvikling giver os. Det gør vi med en bred og dyb teknologisk ekspertise, kreativitet og en praktisk evne til at integrere avancerede teknologier i vores opgaveløsning.

Vi lever dagligt med opgaver og succeser, der næsten altid vil være hemmelige, så vi kompromisløst kan beskytte vores kilder, kapaciteter og samarbejdspartnere. Men vi ønsker samtidig at være så åbne som muligt og være i dialog med det samfund, som har givet os opgaven med at passe på Danmark og danske interesser.

## FE HAR FIRE HOVEDOPGAVER:

- Vi er Danmarks udenrigs- og militære efterretningstjeneste
- Vi er Danmarks militære sikkerhedstjeneste
- Vi er Danmarks netsikkerhedstjeneste, nationale it-sikkerheds-myndighed, kompetencecenter for cybersikkerhed og myndighed for informationssikkerhed og beredskab på teleområdet
- Vi leverer defensive og offensive cybereffekter til støtte for Forsvaret

# EN EFTER-RETNINGSTJENESTES SPILLEREGLER

FE opererer på et lovgrundlag, der giver meget vide rammer for, hvordan FE kan operere i forhold til udlandet, men snævre rammer på andre områder. Det stiller store krav til FE's egenkontrol. Som intern vagthund og chef for Jura og Ledelsesstøtte sidder Esben Haugland.

### HVAD ER TILSYNETS ROLLE?

Tilsynet med Efterretningstjenesterne (TET) er et uafhængigt kontrolorgan, som fører kontrol med, at FE overholder lovens regler om oplysninger om i Danmark hjemmehørende fysiske og juridiske personer og personer, der opholder sig i Danmark. Tilsynet kan i den forbindelse kræve at få udleveret enhver oplysning fra FE og alt materiale, der er af betydning.

Tilsynet offentliggør hvert år en redegørelse om kontrollen med FE.

FE's opgave er at beskytte Danmark og danske interesser mod trusler udefra. Det gør vi på flere forskellige måder – ikke mindst ved at tilegne os viden om potentielle modstandere. For at skaffe den viden kræver det ofte, at vi benytter metoder, som normalt ville ligge uden for lovens rammer. Eller sagt med andre ord metoder, som kan være ulovlige i de lande, vi benytter dem i.

*"FE-loven giver os metodefrihed, når det kommer til forhold i udlandet. Det betyder, at vi ikke kun indsamler information gennem åbne kilder, men at vi også kan indhente gennem særlige kapaciteter, som vi eller vores samarbejdspartnere råder over. En sådan indhentning er også det, man kalder spionage. Det kan f.eks. være ved at føre kilder, ved målrettede aflytninger eller ved masseindsamling af data",* fortæller fg. juridisk chef Esben Haugland.

**ESBEN HAUGLAND**

Fungerende chef for
Jura og Ledelsesstøtte

I FE har vi vidtgående beføjelser til at indhente oplysninger om forhold i udlandet. Så meget desto vigtigere er det, at vi fuldt ud respekterer de grænser, som er opstillet for vores virke.

Esben Haugland

FE kan med andre ord skaffe viden til Danmark, som andre ikke kan eller må. Den viden er afgørende for, at Danmark kan være på forkant både udenrigs-, forsvars- og sikkerhedspolitisk, og for vores beskyttelse imod terrorisme, cyberangreb og spionage fra andre lande.

Men selv om banen er bred, er der nogle helt klare streger, som FE skal holde sig inden for.

*"FE er en udenrigsefterretningstjeneste, og derfor orienterer FE sig først og fremmest imod trusler mod Danmark og danske interesser i og fra udlandet. I FE-loven er der snævre grænser for, hvornår og hvordan FE kan tilvejebringe oplysninger om danskere og personer i Danmark. Det er helt afgørende, at vi overholder disse regler, og det er noget, som har særdeles stor bevågenhed i FE",* siger Esben Haugland.

Den store bevågenhed kommer blandt andet til udtryk gennem et højt undervisnings- og opmærksomhedsniveau om reglerne blandt FE's medarbejdere, og så understøttes rammerne af en lang række interne procedurer og egenkontroller.

FE har en tæt dialog og et nært samarbejde med PET, og i det samarbejde er der undtagelser fra reglen om, at FE ikke må indhente mod danskere.

*"Det gælder ikke mindst i forhold til terrorbekæmpelse. Her kan FE både af egen drift og efter anmodning fra PET under visse omstændigheder indhente og behandle oplysninger om danskere",* fortæller Esben Haugland.

### TILSYNETS SENESTE ÅRSREDEGØRELSE

I tilsynets årsredegørelse for 2020 fremgår det bl.a., at tilsynet ser positivt på FE's foreløbige opfølgning på de risici, som blev påpeget ved tilsynets særlige undersøgelse af FE i 2019/2020. Tilsynet vurderer samtidig, at FE arbejder dedikeret for at sikre, at de påpegede risici imødegås.

Årsredegørelsen for 2020 indeholder også nogle kritikpunkter, herunder om FE's målrettede elektroniske indhentning af oplysninger og FE's søgning i rådata. Det er ifølge årsredegørelsen tilsynets vurdering, at FE fortsat har en væsentlig udfordring i forhold til overholdelse af reglerne, når FE foretager søgning i rådata.

### Legalitetssikring og egenkontrol

FE foretager både forudgående legalitetssikring og bagudrettet egenkontrol for at sikre, at vores operationer overholder FE-loven. Vi indhenter dagligt store mængder rådata fra elektronisk kommunikation, som vores analytikere kan søge i for at finde netop de data, der skal bruges til at opbygge et efterretningsbillede. Der er et meget stort fokus på procedurerne ved søgning i rådata, og vi foretager af samme grund en tilnærmelsesvis fuldstændig egenkontrol af alle de dansk-relaterede søgninger.

Derudover arbejder vi løbende på at udbygge kontrolmekanismerne i FE's søgeværktøjer med f.eks. blokeringer og alarmer, der har til formål at sikre overholdelse af reglerne.

### Tilsynet med Efterretningstjenesterne

FE er underlagt et uvildigt tilsyn – Tilsynet med Efterretningstjenesterne (TET) – som fører kontrol med, at FE ikke uberettiget behandler oplysninger om danskere, ligesom vi løbende holder dem orienteret om vores egen kontrolvirksomhed og legalitetssikring.

I TET's årlige redegørelser har tilsynet udtrykt kritik af rådatasøgninger mod i Danmark hjemmehørende personer, som tilsynet mener er uberettigede.

*"I FE har vi vidtgående beføjelser til at indhente oplysninger om forhold i udlandet. Så meget desto vigtigere er det, at vi fuldt ud respekterer de grænser, som er opstillet for vores virke. Det er afgørende for den tillid, der skal være til en efterretningstjeneste som FE",* siger Esben Haugland.

Derfor bliver der også lyttet til kritikken.

*"Det ligger naturligvis alle i FE meget på sinde at overholde de krav, vi er underlagt, og vi har derfor også et stærkt fokus på kontrollen af de dansk-relaterede søgninger. Det er i den forbindelse vigtigt at understrege, at de uberettigede søgninger, som er registreret, skyldes menneskelige og ikke-tilsigtede fejl og ikke udtryk for, at medarbejdere i FE bevidst har søgt efter oplysninger om danskere uden gyldig grund",* fortæller Esben Haugland.

I august 2020 rettede TET kritik mod dele af FE's elektroniske indhentning, hvilket også fik en del spalteplads i medierne. Det blev på den baggrund besluttet at nedsætte en undersøgelseskommission til at undersøge de fremførte kritikpunkter, og kommissionen arbejder i skrivende stund fortsat.

*"Parallelt med kommissionens arbejde har vi i FE iværksat en række initiativer til at imødekomme de dele af tilsynets kritik, som ikke behøver at afvente kommissionsundersøgelsen. I sin seneste redegørelse skriver tilsynet, at tilsynet ser positivt på FE's foreløbige opfølgning på de fremførte kritikpunkter, og det er jeg naturligvis meget glad for. Det er et både omfattende og højt prioriteret arbejde, som vi ikke er færdige med",* afslutter Esben Haugland.

### I DANMARK HJEMMEHØRENDE FYSISKE OG JURIDISKE PERSONER

At FE's efterretningsmæssige virksomhed er rettet mod forhold i udlandet betyder, at FE som udgangspunkt ikke må foretage målrettet indhentning af oplysninger mod **"i Danmark hjemmehørende fysiske og juridiske personer"**. Der er tale om et juridisk udtryk, som dækker over danske statsborgere, udenlandske statsborgere, der har ret til ophold i Danmark og er tilmeldt folkeregistret, asylansøgere med kendt ophold i Danmark i mere end seks måneder samt virksomheder, foreninger og organisationer, der i kraft af deres hovedkontor m.v. har deres overvejende tilknytning til Danmark. FE-loven indeholder dog regler om, at FE i terrorsager under visse betingelser kan indhente oplysninger om danskere m.fl., der opholder sig i udlandet.

Ud over "i Danmark hjemmehørende fysiske og juridiske personer" må FE i sin efterretningsmæssige virksomhed heller ikke foretage målrettet indhentning mod udlændinge, der opholder sig i Danmark. Men denne beskyttelse ophører altså lige så snart, udlændingen forlader Danmark.

# ÅBNE DØRE OG VANDTÆTTE SKOTTER – ET SAMARBEJDE MED KLARE LINJER

FE og Center for Cybersikkerhed opererer på to forskellige lovgrundlag – FE-loven og CFCS-loven – som rummer forskellige muligheder og begrænsninger. Det stiller krav om vandtætte skotter mellem dele af tjenesten.

FE er ikke kun Danmarks udenrigs- og militære efterretningstjeneste. Vi er også den nationale it-sikkerhedsmyndighed og den militære og statslige varslingstjeneste for internettrusler, også kaldet netsikkerhedstjenesten. Cyberopgaven hører hjemme i Center for Cybersikkerhed (CFCS), som opererer på et andet lovgrundlag end det øvrige FE. Samtidig er CFCS' adgang til at indsamle og dele oplysninger generelt set betydeligt mere begrænset end resten af FE's. Disse grundlæggende forskelle i beføjelser, og hvordan FE og CFCS arbejder, kræver klare linjer.

FE's efterretningsmæssige virksomhed er rettet mod forhold i udlandet, og FE's indhentning er geografisk neutral. Det betyder, at indhentningen kan være meget omfattende og kan ske fra en hvilken som helst geografisk lokalitet – dansk såvel som udenlandsk – så længe formålet er at indhente oplysninger om forhold i udlandet af betydning for Danmark og danske interesser. Men det betyder f.eks. også, at FE som det meget klare udgangspunkt ikke må foretage målrettet indhentning af information mod danskere m.fl.

FE-loven og CFCS-loven adskiller sig altså helt grundlæggende fra hinanden, og selv om CFCS er en integreret del af FE, er der en udførlig og streng regulering af forholdet mellem navnlig netsikkerhedstjenesten i CFCS og det øvrige FE.

CFCS' arbejde er derimod rettet mod danske forhold – konkret at beskytte de vigtigste dele af det danske samfund mod cyberangreb. Eller som det er beskrevet i CFCS-loven, "at understøtte et højt informationssikkerhedsniveau i den samfundskritiske it-infrastruktur". Det indebærer blandt andet, at CFCS arbejder for at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos de myndigheder og virksomheder, der er tilsluttet den særlige netsikkerhedstjeneste, der er en del af CFCS. Det sker blandt andet ved at monitorere netværkskommunikation til og fra de myndigheder og virksomheder, der er tilsluttet netsikkerhedstjenestens sensornetværk. På den måde kan de hurtigt reagere, hvis der er uregelmæssigheder i kommunikationsmønstre, der kan indikere brud på it-sikkerheden.

FE-loven og CFCS-loven adskiller sig altså helt grundlæggende fra hinanden, og selv om CFCS er en integreret del af FE, er der en udførlig og streng regulering af forholdet mellem navnlig netsikkerhedstjenesten i CFCS og det øvrige FE. Derfor kan netsikkerhedstjenesten kun udveksle data med den øvrige del af FE, når der er begrundet mistanke om en sikkerhedshændelse, f.eks. når CFCS har grund til at tro, at en ondsindet aktør forsøger at hacke eller på anden måde angribe den tilsluttede myndighed m.v.

FE bruger mange ressourcer på at udføre egenkontrol for at sikre, at FE og CFCS opererer inden for rammerne. Så selv om FE samarbejder bredt på tværs af tjenesten, er det ikke ensbetydende med, at der er åbne døre mellem FE og CFCS, når det kommer til data – tværtimod.

**ANJA DALGAARD-NIELSEN**

Chef for Efterretning



# HVORDAN PÅVIRKER DE SIKKERHEDS-POLITISKE FORHOLD FE'S ARBEJDE?

Anja Dalgaard-Nielsen er chef for FE's sektor for efterretning og står dermed helt centralt i kampen mod terror og andre sikkerhedsmæssige trusler mod Danmark. I denne artikel fortæller hun om det ændrede trusselsbillede og om de krav, det stiller til FE som efterretningstjeneste.

Der er nok at tage fat på: Mod nord konkurrerer stormagterne i Arktis og gør deres interesser gældende. Mod øst fortsætter Rusland sin sikkerhedspolitiske kurs og militære adfærd og manifesterer sig som en stormagt. Kina søger at øge sin indflydelse i verdenen og ændre eksisterende betingelser for international politik til sin egen fordel. Mod syd i Afrika og Mellemøsten er jorden gødet for fortsat ustabilitet og konflikt, ikke mindst på grund af svage stater og ændrede magtforhold mellem stormagterne. Oven i dette ses en stadigt stigende cybertrussel.

Danmark er omgivet af trusler og sikkerhedspolitiske udfordringer, og det stiller store krav til FE's efterretningsarbejde. I spidsen for dette står Anja Dalgaard-Nielsen, der med en baggrund som international sikkerhedsekspert og terrorforsker er godt klædt på til at give beslutningstagerne det bedst mulige vidensgrundlag, når der skal træffes beslutninger, som har betydning for Danmarks sikkerhed.

### FE skal multitaske i en usikker verden

Siden terrorangrebet mod USA i 2001 og frem til 2014 var det entydigt største sikkerhedspolitiske fokus på terrortruslen. Men da Rusland annekterede Krim-halvøen, begyndte det sikkerhedspolitiske billede at ændre sig.

*"Vi har haft perioder i historien, hvor der ikke var tvivl om, hvilken trussel vi skulle fokusere på. Under den kolde krig var det USSR. I kølvandet på 11. september 2001 var det global militant islamisme. I dag er det ikke så entydigt, hvilket naturligvis gør FE's opgave med at modvirke trusler mod Danmark mere kompleks. Vi har altid skullet have det lange lys på og forudse truslerne, inden de opstår, men i dag skal vi i stigende grad favne meget bredt",* siger Anja Dalgaard-Nielsen.

Med trusler fra alle flanker – både fysisk og virtuelt – er det FE's opgave at klæde danske beslutningstagere bedst muligt på til at oversætte det komplekse trusselsbillede til udenrigs- og sikkerhedspolitiske prioriteter for Danmark.

Det skal ske i en verden med stor indbygget usikkerhed:

*"Jo flere stater, terrororganisationer, hackergrupper osv., der kan gøre sig gældende globalt, jo mere uforudsigeligt bliver spillet. Læg dertil faktorer som svage stater, regionale krige, spredning af våben, udviklingen af nye teknologier – der både kan anvendes konstruktivt og destruktivt – klimaforandringer og biologiske risici. Det er klart, at evnen til at forudsige begivenhedernes gang er udfordret. Det er derfor afgørende, at vi løbende tilpasser vores arbejde, så vi som minimum matcher udviklingen omkring os",* fortæller Anja Dalgaard-Nielsen.

I takt med at de sikkerhedspolitiske forhold ændrer sig, og mængden af information, misinformation og desinformation er blevet markant større, har FE's arbejdsformer også ændret sig.

*"Tværfaglighed, hurtighed, evnen til at skifte retning og tæt dialog med kunderne skal forenes med høj faglighed og tårnhøj faglig integritet. Det er sådan, vi bedst værner om Danmarks sikkerhed og klæder beslutningstagerne på til at træffe svære valg",* afslutter Anja Dalgaard-Nielsen.

# Jo flere stater, terrororganisationer, hackergrupper osv., der kan gøre sig gældende globalt, jo mere uforudsigeligt bliver spillet.

Anja Dalgaard-Nielsen

# TRUSLER MOD DANMARK OG DANSKE INTERESSER

### ARKTIS

Det anspændte forhold mellem de tre stormagter Rusland, USA og Kina vil definere udviklingen i Arktis. Det vil også påvirke Rigsfællesskabet. De tre stormagter har i vid udstrækning modstridende interesser, som de i stigende grad vil forfølge uagtet det regionale samarbejde. Rusland ser sig som den førende arktiske stat og opbygger fortsat militære kapaciteter, som kan true vestlige interesser. USA og andre vestlige lande har derfor også øget deres militære tilstedeværelse for at håndtere Ruslands rolle i Arktis. Kina vil være med til at forme rammerne i regionen, og især USA forsøger at modvirke Kinas indflydelse.

### VESTAFRIKA

Det vestlige Sahel er præget af mange problemer, herunder dårlig regeringsførelse, økonomiske kriser og militant islamisme, og de nationale myndigheder har vanskeligt ved selv at forbedre forholdene. Pirateri i Guineabugten fortsætter, og piraterne fokuserer primært på kidnapninger for at få løsepenge.

### TERRORISME

Terrortruslen er fortsat alvorlig og kommer især fra militante islamister, men også fra højreekstremister. Al-Qaida og Islamisk Stat inspirerer stadig individer og netværk til angreb i og uden for Europa. Vestlige fremmedkrigere vil fortsat udgøre en trussel. Både al-Qaida og Islamisk Stat har en vedblivende intention om at angribe Vesten, og deres regionale undergrupper udgør en trussel mod vestlige interesser i store dele af verden. Talibans magtovertagelse vil sandsynligvis øge terrortruslen fra militante islamistiske grupper i Afghanistan og regionen som helhed. Det skyldes, at terrorgrupper som al-Qaida, Islamisk Stat i Khorasan-provinsen (ISKP) og andre militante pakistanske og centralasiatiske grupper ikke længere er under pres fra afghanske sikkerhedsstyrker og amerikanske tropper i Afghanistan.

De trusler og sikkerhedspolitiske udfordringer, Danmark står overfor, er afgørende for prioriteringen af FE's indsats. Den høje cybertrussel er et grundvilkår, Ruslands politiske og militære aktiviteter er blevet en større udfordring, og terrortruslen er stadig alvorlig. Herudover betyder Kinas hastige udvikling forskydninger i den internationale magtbalance, ligesom spændingerne omkring Arktis udfordrer det regionale samarbejde.

## CYBERTRUSLEN

Staters og kriminelles cyberangreb er fortsat blandt de mest alvorlige trusler mod Danmark. Truslen fra cyberspionage og cyberkriminalitet er både rettet mod danske virksomheder og myndigheder, men kommer til udtryk på forskellige måder. Cyberspionage udføres ofte i det skjulte, og konsekvenserne kan være svære at opdage. Cyberkriminelle udnytter derimod ofte det pres, som nedbrud i it-systemer og trusler om offentlig eksponering lægger på deres ofre, til økonomisk gevinst.

## RUSLAND

Rusland underbygger sin stormagtsrolle med en voksende militær afskrækkelse og skærper konfrontationen med Vesten med offensive efterretningsoperationer, cyberspionage og påvirkning. Rusland kan træffe hurtige beslutninger i en snæver kreds, og Rusland har dyb mistillid til Vesten. Det skaber risiko for fejltagelser og utilsigtet militær eskalation, som vil kunne opstå med meget kort varsel. Rusland har over de seneste år opbygget og moderniseret sine væbnede styrker i det vestlige Rusland. Rusland er militært overlegen i Østersøregionen i den første fase af en konflikt, hvor Rusland kan indsætte sine styrker meget hurtigt. Det er usandsynligt, at Rusland med overlæg vil risikere en militær konflikt med NATO i Østersøregionen. Rusland ser dog krig med NATO som noget, der reelt kan ske, og øver sig under store strategiske øvelser på at udkæmpe en sådan konflikt.

## MELLEMØSTEN OG NORDAFRIKA

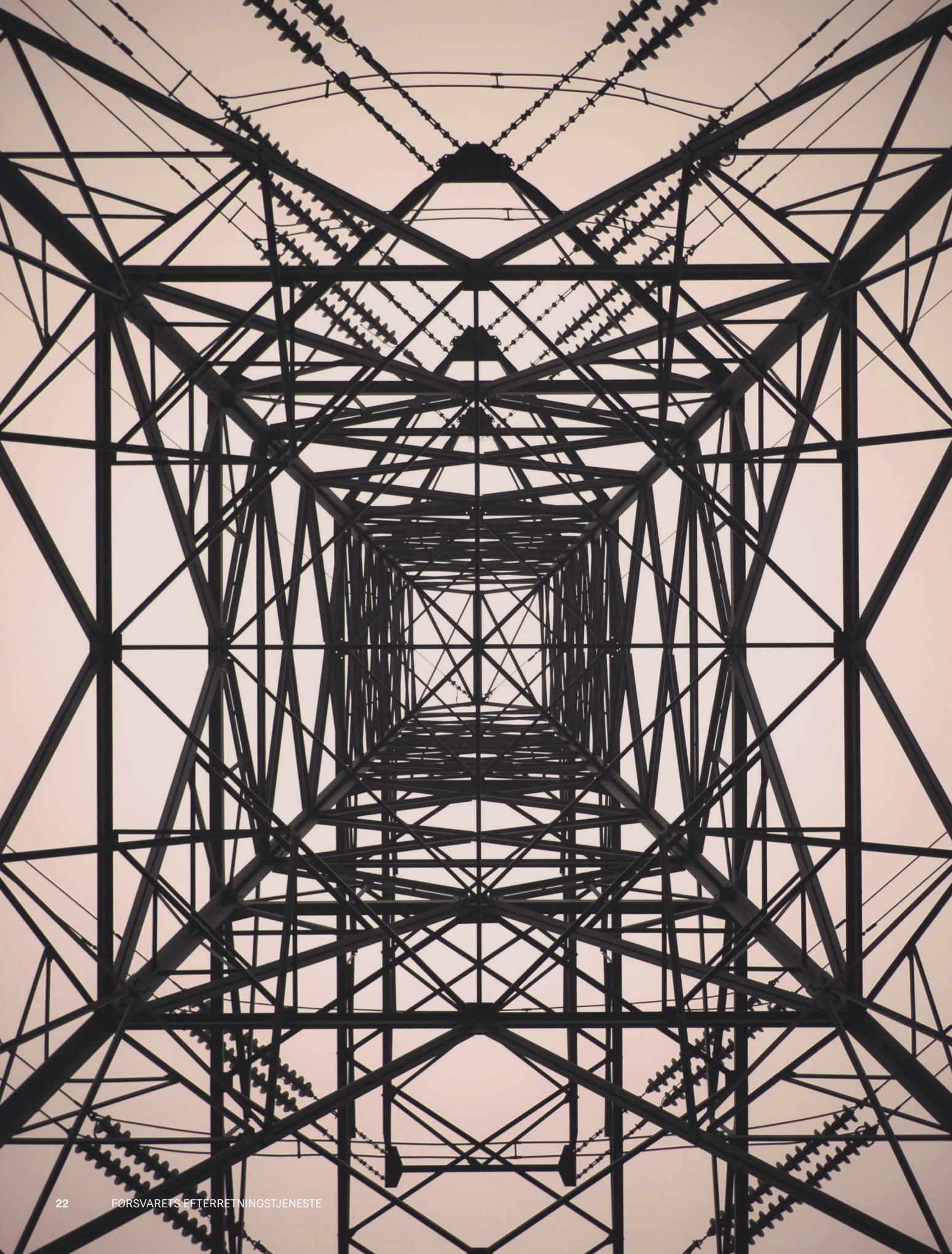
Mellemøsten og Nordafrika vil fortsat udgøre en sikkerhedspolitisk udfordring på såvel kort som langt sigt. Europa vil i højere grad stå alene med at håndtere de afledte problemer blandt andet i form af flygtninge, illegal migration og trusler fra islamistiske terrororganisationer.

## AFGHANISTAN

Taliban har erobret magten i Afghanistan. På kort sigt er risikoen for en borgerkrig aftaget, men på mellemlang sigt vil den sandsynligvis stige som følge af spændinger i Taliban, overgangen fra oprørsgruppe til regering og problemer med at håndtere de tidligere sikkerhedsstyrker. Nabolande vil muligvis søge at udnytte de dybe brudflader i landet. Talibans hårde regime og den økonomiske situation vil sandsynligvis få mange til at søge væk fra Afghanistan, til nabolandene Iran og Pakistan og nogle videre til Tyrkiet. Blandt de voksende afghanske diasporaer i disse lande vil mange migrere til Europa.

## KINA

Kinas voksende indflydelse og globale ambitioner skaber spændinger i forholdet til en række vestlige lande, herunder til Danmark. Samtidig søger Kina mere håndfast og offensivt at imødegå kritik af det, landet opfatter som sine indre anliggender. For at understøtte sine strategiske interesser bruger Kina sin økonomiske tyngde til at lægge politisk og økonomisk pres på andre lande, ligesom Kina målrettet anvender cyberspionage til at fremme sine interesser. Også Danmark rammes af disse virkemidler. Kina ser den strategiske konkurrence med USA som afgørende for landets videre udvikling og vil undgå, at USA begrænser Kinas muligheder for at manifestere sig som stormagt og få indflydelse. Kinas sikkerhedspolitiske mål er at blive den dominerende regionale stormagt i Østasien og det vestlige Stillehav. Derfor fortsætter Kina sin militære opbygning og hævder sine krav i Det Sydkinesiske Hav.



# SÅDAN FÅR FE SIN INFORMATION

FE er en all source-efterretningstjeneste, hvilket betyder, at vi beskæftiger os med alle typer af informationsindhentning. Det giver os gode muligheder for at kombinere indhentningsdisciplinerne i det, vi kalder blandede operationer.

FE er som efterretningstjeneste afhængig af informationer for at kunne identificere og analysere de trusler, der er mod Danmark og danske interesser. Derfor har FE lovgivningsmæssigt fået stillet helt særlige metoder til rådighed, som vi kan benytte i vores informationsindhentning.

Overordnet set arbejder FE med fem indhentningsdiscipliner:

### HUMINT

HUMINT står for Human Intelligence, altså efterretningsindhentning ved brug af menneskelige kilder, også kaldet fysisk indhentning. Det vil grundlæggende sige, at en person ansat i efterretningstjenesten, kaldet en føringsofficer eller indhenter, skaffer oplysninger fra andre personer, kaldet kilder. Det gør føringsofficeren typisk ved at overtale kilden til at videregive oplysninger, som det ikke var meningen, at vedkommende skulle videregive.

### SIGINT

SIGINT står for Signals Intelligence, som er elektronisk indhentning af dataoverførsler mellem computernetværk, telekommunikation osv. Den elektroniske indhentning sker f.eks. fra permanente indhentningsfaciliteter, der indhenter mod satellitter. Det kan også være indhentningsfaciliteter opstillet i udlandet, som vi kan fjernstyre fra Danmark. Kommunikationen bliver indhentet, mens den er undervejs, uden at påvirke transmissionen, og uden at de berørte parter opdager, at deres kommunikation bliver opfanget.

SIGINT kræver store it-systemer til at behandle det indhentede materiale og er teknisk komplekst. Det skyldes, at mængden af kommunikation stiger med voldsom hast, samtidig med at der hele tiden udvikles nye teknologier.

### NETVÆRKSINDHENTNING

Netværksindhentning er også kendt som Computer Network Exploitation (CNE). Det omfatter aktiv elektronisk indhentning mod computernetværk, hvilket betyder, at man eksempelvis skaffer sig adgang til – eller med andre ord hacker sig ind i – lukkede netfora, it-systemer og computere. Det er et arbejde, der kræver medarbejdere med meget stærke og meget forskellige tekniske kompetencer.

### GEOINT

GEOINT står for Geospatial Intelligence og leverer efterretninger baseret på det geografiske indhold i data fra forskellige indhentningsdiscipliner. Ud over visualisering og præsentation af data omfatter GEOINT også identifikation og analyse af bevægelses- og udviklingsmønstre i relevante tidsrum og/eller geografiske områder.

### OSINT

OSINT står for Open Source Intelligence, hvilket er indsamling af oplysninger fra åbne kilder, der typisk omfatter offentligt tilgængelig information fra internettet, trykte medier, tv m.m.

# ET INDBLIK I EN MODERNE EFTER-RETNINGSTJENESTES ARBEJDE

### BIG DATA DER BATTER

FE indhenter dagligt meget store mængder af data, der ofte er ustrukturerede, krypterede og i meget forskellige formater. Derfor er datahåndteringen en integreret del af efterretningsarbejdet. Data skal struktureres og præsenteres for analytikerne hurtigt, så de kan skabe et opdateret efterretningsbillede. Der indgår derfor også dataudviklere i vores efterretningsteams på højt prioriterede indsatsområder, som hele tiden skal have et overblik over efterretningsbehovene fra FE's analytikere.

Verden er dynamisk, og det er efterretningsarbejdet også. Som moderne efterretningstjeneste skal vi hele tiden tilpasse os et trusselsbillede, der kan ændre sig fra dag til dag.

Samarbejde og koordination er nøgleord for efterretningsarbejdet, og i FE er der et tæt samarbejde mellem vores analyse- og indhentningsenheder. Med en verden og et trusselsbillede i forandring er det afgørende, at vi løbende tilpasser den måde, vi arbejder og samarbejder på – både internt og med kunder og samarbejdspartnere.

Efterretningsbilledet kan forandre sig hurtigt og stiller hele tiden nye krav til FE's indhentning af informationer. Derfor arbejder vi i efterretningsteams sammensat af specialister på tværs af organisationen, som driver efterretningsarbejdet og optimerer indsatsen på de prioriterede områder. Det tætte samarbejde mellem eksempelvis føringsofficerer, dataudviklere og analytikere er med til at sikre, at FE skaffer de rette informationer til at dække de allerhøjest prioriterede strategiske efterretningsbehov.

Med en verden og et trusselsbillede i forandring er det afgørende, at vi løbende tilpasser den måde, vi arbejder og samarbejder på – både internt og med kunder og samarbejdspartnere.

Processen fra indhentning til færdigt produkt er ofte kompliceret og tidskrævende. Det stiller store krav til specialiseret teknisk viden inden for vidt forskellige teknologier og til samarbejdet i vores efterretningsteams. Vi skal hurtigt identificere, hvor de oplysninger, der efterspørges, er tilgængelige, og hvordan vi kan indhente dem. Når indhentningen er sikret, skal de ofte meget store datamængder håndteres, så vi kan udlede de brugbare informationer og omsætte dem til efterretninger.

### Samarbejde på tværs af landegrænser

Det er ikke kun internt, at et godt samarbejde er afgørende for at kunne levere gode og pålidelige efterretninger. Samarbejdet med efterretningstjenester i andre lande bidrager til en mere komplet forståelse af det komplekse globale trusselsbillede.

Den hastige teknologiske udvikling og digitalisering har medført, at fremmede stater og terrornetværk har nemmere ved at operere på tværs af landegrænser. For at kunne imødegå sådanne grænseoverskridende trusler kræves et godt samarbejde mellem efterretningstjenesterne.

Samarbejdet med partnertjenester kan både være bilateralt og multilateralt. Samarbejderne kan omhandle indhentningsmetoder, teknologier og kapaciteter, og de kan omhandle deling af efterretninger om specifikke trusler. Partnersamarbejde kan også have en karakter og dybde, så det ender i fælles operationer. Partnersamarbejdet er helt centralt for FE's evne til at forebygge og modvirke trusler mod Danmark og danske interesser.

FE's partnersamarbejde er opbygget over årtier og er baseret på troværdighed, tillid og fortrolighed. Det gælder både i forhold til de udvekslede oplysninger og metoder og i forhold til eksistensen af selve samarbejdsrelationen. Vi kan altså hverken be- eller afkræfte eksistensen af et partnersamarbejde, heller ikke over for øvrige partnere. Hvis partnere får indtryk af, at vi ikke kan opretholde den fulde fortrolighed, vil relationen kunne tage skade. Ikke kun i forhold til den partner, der oplever manglende diskretion, men også i forhold til øvrige partnere. Og det vil ultimativt påvirke vores evne til at modvirke trusler.

FE's samarbejde med udenlandske samarbejdspartnere foregår naturligvis i overensstemmelse med dansk ret og relevante internationale konventioner.

# VORES KUNDER OG PRODUKTER

Vores arbejde er hemmeligt for de fleste – men ikke for alle. Formålet med vores arbejde er nemlig at levere efterretninger til vores kunder, så de kan træffe beslutninger om Danmarks sikkerhed på et så oplyst grundlag som muligt.

### HVAD ER EN VARSLING?

En varsling kan både være konkrete informationer om et møde, et angreb eller en reaktion, og det kan også være i form af tidlig identifikation af nye tendenser eller forskydninger i globale magtforhold.

Når Rusland f.eks. bygger Nagurskoye-basen i Arktis, der sætter landet i stand til at sende kampfly mod grønlandsk territorium med kort eller slet intet varsel, er det vigtigt, at vi i Danmark kender til det arbejde, i god tid før at basen er operativ. Derfor har FE gennem flere år varslet om opbygningen.

FE's kunder og deres behov er styrende for vores efterretningsarbejde. De efterretningsmæssige produkter, vi leverer, er det mest synlige resultat af vores efterretningsarbejde. Vi leverer dagligt produkter til vores kunder i form af rapporter og briefinger, og hertil kommer en operativ indsats, som kun vil være synlig for få kunder.

Produkterne udarbejdes ud fra vores oplysninger om en række landes og regioners politiske, økonomiske og militære forhold og om vigtige trusler og udfordringer som f.eks. terror og cyberangreb. Det gør os i stand til at informere og varsle om forskellige staters og andre aktørers hensigter, kapaciteter og adfærd. Vi deler vores viden med regeringen, så Danmark som suveræn stat kan føre sin udenrigs-, sikkerheds- og forsvarspolitik på grundlag af selvstændige, nationale efterretningsmæssige vurderinger. Center for Cybersikkerhed deler desuden løbende trusselsvurderinger og rådgivningsprodukter med offentligheden.

## FE'S VIGTIGSTE KUNDER

- Udenrigsministeriet
- Forsvarsministeriet
- Forsvaret
- Den kritiske infrastruktur
- PET

En stor del af FE's produkter varsler om specifikke angreb, f.eks. af betydning for udsendte styrker. Særligt i forhold til terror- og cybertrusler er FE's opgave ikke kun at varsle, men også at bidrage til at modvirke angreb mod Danmark og danske interesser. Det kræver, at vores efterretningsprodukter er relevante, rettidige og fagligt solide.

### Dialog og samarbejde

Det er vigtigt, at vi løbende holder en tæt dialog med vores kunder, så vi kan sikre, at vi leverer de relevante produkter, og at de bliver forstået rigtigt. Kundernes behov bliver omsat til specifikke, prioriterede efterretningsbehov, som derefter bliver nedbrudt til konkrete emner for indhentning. På den baggrund beslutter FE, hvilke indhentningskapaciteter der skal bringes i spil for at tilvejebringe oplysningerne, og herefter går det komplekse operative og analytiske arbejde i gang. Vi holder løbende kundemøder, hvor vi drøfter samarbejdet og prioriteringen af de efterretningsmæssige fokusområder, så vi hele tiden kan sikre, at vi er i stand til at imødekomme vores kunders ønsker og behov for pålidelige og rettidige efterretninger.

### IKKE-KLASSIFICEREDE PRODUKTER

FE udgiver hvert år en efterretningsmæssig risikovurdering, der giver et ikke-klassificeret billede af de vigtigste trusler og andre forhold i udlandet af betydning for Danmarks sikkerhed.

FE leverer også to typer ikke-klassificerede trusselsvurderinger. Den ene type udarbejdes som en del af Folketingets grundlag for beslutninger om indsættelse af danske militære bidrag i forbindelse med internationale operationer. Den anden type handler om cybertruslen mod Danmark generelt og specifikt mod blandt andet samfundsvigtige sektorer.

Se FE's og CFCS's offentliggjorte produkter på hjemmesiderne: **www.fe-ddis.dk** og **www.cfcs.dk**

# FE HJÆLPER FORSVARET MED AT BESKYTTE DANMARK

Som Danmarks militære sikkerheds-tjeneste er det FE's opgave at rådgive Forsvaret om potentielle trusler og skabe de bedste forudsætninger for at beskytte Danmark.

Forsvaret beskytter os mod trusler udefra og bidrager til en mere stabil og sikker verden. En af FE's opgaver er at varsle Forsvaret mod de trusler, der kan påvirke udførelsen af Forsvarets opgaver. I spidsen for FE's sektor for støtte til Forsvaret står oberst Kim Simonsen, som selv har en lang karriere i Forsvaret bag sig.

*"FE støtter Forsvaret ved at analysere og rådgive om de trusler, Forsvaret potentielt kan møde – både i de lande, vi er udsendt i, og også når de skal beskytte rigsfællesskabet. Vi rådgiver om konkrete trusler og udfordringer og også om den militærteknologiske udvikling",* siger Kim Simonsen.

**KIM SIMONSEN**

Chef for Støtte til Forsvaret

Ligesom vi holder øje med udviklingen i andre lande, holder de også øje med os. Forsvaret vil altid være et mål for spionage og cyberspionage, så det er klart, at det fylder i vores efterretningsmæssige støtte.

Kim Simonsen

Når Forsvaret skal rådgive politikerne om militære indsatser, er det afgørende, at politikerne altid har et opdateret billede af, hvilke ressourcer og muligheder en fjendtlig aktør har, og hvordan trusselsbilledet ser ud. Og selv om Danmark ikke er i direkte krig, er der stadig mange trusler mod Forsvaret.

*"Ligesom vi holder øje med udviklingen i andre lande, holder de også øje med os. Forsvaret vil altid være et mål for spionage og cyberspionage, så det er klart, at det fylder i vores efterretningsmæssige støtte. Herudover er det vigtigt, at Forsvaret altid har et opdateret billede af mulige modstanderes kapaciteter og udvikling, så de kan være på forkant med truslen. Og så er vi selvsagt også særligt opmærksomme på konkrete trusler og sikkerhedsrisici i de lande, vores styrker udsendes til",* siger Kim Simonsen.

FE's støtte tilpasser sig hele tiden Forsvarets behov og ændrer sig derfor løbende. Men særligt på ét område har støtten ændret sig markant, nemlig i det kolde nord.

*"De seneste år er aktiviteten i Arktis begyndt at fylde mere, også i vores støtte til Forsvaret. Vi ser særligt et Rusland, der i stigende grad gør sig gældende, og derfor skal Forsvaret være klædt rigtigt på til de udfordringer, en eventuel militær eskalation kan udgøre for rigsfællesskabet",* siger Kim Simonsen.

Trusler mod Forsvaret kommer ikke kun udefra – de kan også komme indefra. Som ansvarlig for den militære sikkerhed er det blandt andet FE's opgave at sikkerhedsgodkende alle, der er ansat under Forsvarsministeriets område.

*"Vi er opmærksomme på, om der er personer, der vil bruge deres ansættelse i Forsvaret til at tilegne sig militære kompetencer til et andet formål end at passe på Danmark og danske interesser – og som dermed kan udgøre en intern trussel. Det er en vigtig del af vores arbejde med sikkerhedsgodkendelser"*, siger Kim Simonsen.

Den kommende tid forventer Kim Simonsen dog, at det særligt er stormagtsspændinger og avanceret teknologi, der kommer til at fylde i FE's støtte til Forsvaret:

*"Som jeg ser det, er der tre væsentlige risici, som vi vil have øget fokus på i vores støtte til Forsvaret: Det er truslen fra spionage, det er andre landes udvikling og brug af avancerede teknologier, og så er det, hvordan vi i NATO-sammenhæng håndterer den trussel, lande som Rusland kan udgøre".*

# EFTERRETNINGSMÆSSIG STØTTE TIL MILITÆRE OPERATIONER


Når Folketinget beslutter, at Danmark skal deltage i militære operationer, ligger der grundige overvejelser bag. Det er vigtigt, at beslutningstagerne har et solidt indblik i, hvilke risici der kan være, og hvor stor effekten af indsatsen kan forventes at blive.

En af FE's opgaver er at yde efterretningsmæssig støtte til den politiske og militære beslutningsproces. Det sker blandt andet ved, at FE udarbejder analyser og trusselsvurderinger på baggrund af indhentede oplysninger og på den måde danner et billede af de trusler og udfordringer, de udsendte tropper kan komme til at stå overfor.

Når Forsvaret er i et missionsområde, støtter FE med rådgivning og efterretninger, der kan have betydning for operationen. Det kan f.eks. være efterretninger om fjendtligtsindede personers og gruppers hensigter, placering af enheder, aktiviteter og kapaciteter.

I 2019 og 2020 støttede FE de militære operationer i Afghanistan, Syrien, Irak og Mali såvel som de danske bidrag til NATO's enhanced Forward Presence i Estland. Herudover har FE leveret støtte til Danmarks deltagelse i en fransk hangarskibsgruppe og til Flyvevåbnets afvisningsberedskab med F-16 samt overvågning af dansk nærområde.

# KONSTANTE TRUSLER MOD FORSVARET

Spionage, indbrud, terroranslag, phishing, sabotage – truslerne mod Forsvaret er mange, også når de ikke er i direkte kamp.

En af FE's kerneopgaver er at beskytte Forsvaret mod interne og eksterne trusler. Det er ikke kun Forsvarets medarbejdere, truslerne rettes mod, men i lige så høj grad våben, køretøjer og it- og kommunikationsudstyr. Derfor skal den samlede sikkerhedsindsats dække bredt og følge med et trusselsbillede i konstant forandring.

En vigtig del af indsatsen består i forebyggende arbejde. Det kan blandt andet være rådgivning og briefinger til Forsvarets medarbejdere både i Danmark og i forbindelse med internationale operationer. En anden væsentlig del af arbejdet er kontraefterretning, der har til formål at opdage, advare mod og modvirke trusler rettet specifikt mod Forsvaret og dets medarbejdere. De mest markante trusler mod Forsvaret er spionage og terrorisme, men trusler kan også være sabotage, påvirkningskampagner eller anden kriminalitet.

### Spionagens mange ansigter

FE vurderer løbende spionagetruslen mod Forsvaret, som kommer i flere former: både højteknologisk ved brug af moderne teknologi og – som de fleste nok forbinder med spionage – gennem hemmelige spioner, lokkeduer, manipulation og afpresning.

I forbindelse med leveringen af nye F-35-kampfly fik en række personer med kendskab til flyene i flere lande flirtende Tinder-beskeder fra en kvindelig kamppilot. Kvindens Tinder-profil var sådan set rigtig nok, det var bare ikke hende selv, der skrev beskederne. Profilen var nemlig blevet hacket, og gennem den hackede profil lykkedes det fremmede aktører at indhente oplysninger om de nye kampfly. Eksemplet understreger, at spionagetruslen er rykket med ned i lommen og inden for hjemmets trygge rammer.

FE rådgiver løbende Forsvarets udsendte enheder om spionagetrusler. Det gælder f.eks., når der udsendes fly til en NATO-mission i Baltikum, når der sendes skibe til indsatsen i Hormuzstrædet, og når Hæren støtter kampen mod terror i Mali i det nordvestlige Afrika. Truslen ændrer konstant karakter afhængigt af indsatsområdet, udenrigspolitiske interesser og Forsvarets engagement i f.eks. Rigsfællesskabet og internationale missioner. Så selv om Danmark er et lille land, er Forsvaret en særdeles vigtig aktør og styrende for fjendtlige aktørers interesser og efterretningsbehov.

### Trusler fra flere sider

Terrortruslen er stadig aktuel. Både mod Danmark og danske interesser generelt og også mod Forsvaret specifikt, hvor truslerne kan komme både udefra og indefra. FE støtter kontinuerligt og aktivt Forsvaret mod denne trussel, og en del af FE's opgaver er blandt andet at være opmærksom på bekymrende eller unormal adfærd, afdække hensigten og træffe de nødvendige foranstaltninger.

Medarbejdere og veteraner i Forsvaret afspejler på mange måder den gængse danske befolkning, men på ét væsentligt punkt adskiller de sig fra den almindelige civile borger – nemlig i deres kampfærdigheder. Derfor er FE meget opmærksom på eventuelle ekstremistiske eller radikaliserede miljøer i Forsvaret og den sikkerhedsrisiko, det kan udgøre.

Et andet fokusområde er, når ansatte i Forsvaret rejser til lande eller områder, hvor spionagetruslen er særligt udtalt. Hvis man har tilknytning til Forsvaret og rejser til sådanne lande, kan man blive udsat for hændelser, man ofte hverken opdager eller kan kontrollere. Man kan f.eks. risikere at komme i en situation, hvor man udsættes for afpresning og dermed bliver en potentiel trussel mod Forsvaret. Derfor rådgiver FE Forsvarets ansatte om, hvordan de håndterer denne risiko forud for udsendelser og rejser.

Det er med andre ord ikke nok kun at være opmærksom på de udefrakommende trusler. Det er lige så vigtigt at sikre, at der ikke opstår trusler indefra, og FE støtter også Forsvaret med det arbejde.

De mest markante trusler mod Forsvaret er spionage og terrorisme, men det kan også være sabotage, påvirkningskampagner eller anden kriminalitet.

# MILITÆRE CYBEROPERATIONER

Med den teknologiske udvikling følger både nye muligheder og udfordringer – også når det kommer til militære operationer. I dag kan dele af kampen udspille sig bag en computerskærm i skjul for fjenden.

### BESKYTTELSE AF FORSVARETS NETVÆRK

Formålet med defensive militære cyberoperationer er at beskytte Forsvarets digitale infrastruktur mod cyberangreb, også når Forsvarets enheder er indsat i operationer.

Når danske soldater er udsendt, er det i sagens natur vigtigt, at fjendtlige enheder ikke kan lytte med på den interne kommunikation eller få adgang til oplysninger på anden vis. For at sørge for dette kan FE etablere netværksovervågning i området med henblik på at opdage og modvirke forsøg på indbrud i enhedens netværk. Derudover kan FE udsende eksperthold til et missionsområde, f.eks. som støtte i en efterforskning af et forsøg på indbrud i den udsendte enheds netværk.

Sideløbende med at en bred international koalition gennemførte en omfattende militær indsats mod Islamisk Stat, samledes teams af it-specialister i al hemmelighed i operationscentre tusindvis af kilometer væk og førte en mere hemmelig og stille krig mod terroristerne.

Indsatsen havde til formål at ramme Islamisk Stats store medie- og propagandaorganisation. I al stilhed hackede it-specialister sig ind i Islamisk Stats medieorganisation og kunne på den måde påvirke organisationens muligheder for at kommunikere, sprede propaganda og gennemføre finansielle transaktioner – et område, hvor Islamisk Stat ellers stod meget stærkt.

Dette kunne være et eksempel på nogle af de nye offensive handlemuligheder, der følger af den teknologiske udvikling. En udvikling, der dog også stiller stadigt stigende krav til beskyttelsen af egne kapaciteter.

### Etablering af en militær Computer Network Operations-kapacitet

Computer Network Operations – forkortet CNO – dækker over defensive og offensive cyberoperationer. CNO er lettere forsimplet den kapacitet, Forsvaret bruger til at beskytte og forsvare egne netværk, gengælde angreb eller til at angribe en fjendes netværk og systemer. Et af formålene kan f.eks. være at få adgang til informationer, fremmede stater eller terrororganisationer gerne vil holde hemmelige, hvilket i sagens natur sjældent er en nem opgave. Det kræver dygtige specialister at opnå adgang til sådan information, og den styrke har FE oparbejdet over de senere år.

I forbindelse med den politiske aftale på forsvarsområdet fra 2013-2017 blev det besluttet at etablere en militær CNO-kapacitet i FE, der blandt andet skal støtte Forvaret ved at gennemføre militære cyberoperationer. Hvis der skal udføres militære cyberoperationer, kræver det et konkret politisk mandat – præcis som ved andre militære operationer.

Den militære CNO-kapacitet i FE planlægger og koordinerer den militære cyberstøtte til Forsvaret og gennemfører både defensive og offensive militære cyberoperationer. Dermed råder Danmark over et attraktivt militært værktøj og sikkerhedspolitisk instrument, der kan anvendes selvstændigt eller i sammenhæng med andre konventionelle militære indsatser.

### Defensive militære cyberoperationer

FE kan med CNO-kapaciteten også støtte Forsvarets militære enheder med at sikre deres it-systemer og netværk. Det kan eksempelvis ske gennem sårbarhedsanalyser af netværket og penetrationstests, hvor man simulerer et hackerangreb for at evaluere sikkerheden. Men støtten kan også foregå direkte til soldaterne med information om konkrete cybertrusler og præventive tiltag til at imødegå dem. FE bidrog med en sådan støtte til Forsvaret i forbindelse med det danske bidrag til operation AGENOR i Hormuzstrædet og NATO's fremskudte tilstedeværelse i Baltikum, enhanced Forward Presence.

### Offensive militære cyberoperationer

Offensive militære cyberoperationer kan støtte Forsvaret ved at angribe en modstanders digitale infrastruktur. Et sådan cyberangreb kan både gennemføres som en selvstændig militær operation og som led i en større militær indsats.

Beslutninger om at anvende FE's CNO-kapacitet til at gennemføre et cyberangreb til støtte for en militær operation træffes på samme måde som beslutninger om indsættelse af andre militære kapaciteter. Det kræver med andre ord en Folketingsbeslutning, når FE skal gennemføre et cyberangreb. Indsatsen er underlagt de samme vilkår, som er gældende for magtanvendelse i resten af Forsvaret, og skal ske i overensstemmelse med nationale og internationale regler på området.

#### CYBERANGREB

Når Forsvaret og FE planlægger et cyberangreb, skal risikoen for utilsigtede følgeskader vurderes og afvejes på samme måde, som når Forsvaret indsætter andre mere traditionelle militære kapaciteter. Et cyberangreb til støtte for en militær operation vil være designet til den konkrete opgave ud fra den ønskede militære effekt og de rammer, der er opstillet.

Et cyberangreb går ud på at ramme en modstander gennem dennes digitale infrastruktur. Afhængigt af hvad Forsvaret ønsker at opnå, kan virkningen af et cyberangreb være midlertidig eller varig og medføre begrænset eller omfattende skade. Derfor kan modstanderen i nogle tilfælde ikke undgå at opdage, at et cyberangreb har været gennemført, mens det i andre tilfælde kan være meget svært at opdage.

### Offensive militære cyberoperationer i NATO-regi

NATO råder ikke selv over kapacitet til at gennemføre offensive militære cyberoperationer. Hvis behovet opstår, vil NATO derfor skulle trække på lande, der er i stand til og villige til at gennemføre militære cyberangreb til støtte for en operation i NATO-regi.

Danmark, USA, Storbritannien, Nederlandene og Estland var de første lande, der erklærede sig villige til at stille nationale offensive cyberkapaciteter til rådighed for NATO. Det skete på NATO-topmødet i juli 2018. Efterfølgende har flere nationer meldt sig til, og kredsen af lande er siden udvidet med Frankrig, Litauen, Norge, Spanien, Tyrkiet og Tyskland.

Hvis NATO henvender sig til Danmark med en anmodning om støtte i form af cyberangreb, vil den danske beslutningsproces være den samme som ved en beslutning om indsættelse af kapaciteten i national dansk sammenhæng. Kapaciteten, der bliver indsat til støtte, forbliver desuden under dansk kontrol i forbindelse med både planlægning og selve udførelsen.

**CARMINE GIOIA**

Chef for Data, It og
Avanceret Teknologi



# HVAD BETYDER DE TEKNOLOGISKE MULIGHEDER OG UDFORDRINGER FOR VORES ARBEJDE?

De hastigt voksende datamængder stiller store krav til datahåndtering. For selv om mere data betyder flere informationer, er de enorme datamængder også en udfordring for en efterretningstjeneste.

Når man taler data, er det de tre v'er, der gør sig gældende – volume, variety og velocity, eller sagt på dansk mængde, variation og hastighed. En efterretningstjeneste lever af informationer, men ser man ind i fremtiden, bliver de voksende datamængder, den øgede anvendelse af kryptering og den rivende udvikling inden for digitale kommunikationsformer de helt store udfordringer for verdens efterretningstjenester.

Nye teknologiske trends som kunstig intelligens, maskinlæring og kvantecomputere skal i fremtiden være med til at imødegå disse udfordringer i FE. I spidsen for det arbejde står chef for FE's sektor for Data, It og Avanceret Teknologi, Carmine Gioia.

*"Når datamængderne vokser, bliver behovet for filtrering større. Med højere hastigheder stiger behovet for computerkraft, og når forskelligheden i data bliver større, stiger behovet for avancerede teknologier til at håndtere informationsflowet. Indhentning og databehandling bliver mere kompleks og kan ikke alene løses med flere computere og større lager. Det kræver løbende udvikling og "state of the art"-metoder til indhentning, udvælgelse og filtrering, når vi skal sikre, at vores analytikere får lige præcis de relevante informationer og helst præsenteret i forståelig form",* siger Carmine Gioia.

Det stiller enorme krav til indhentning og datahåndtering at følge med den teknologiske udvikling, specielt da efterspørgslen på efterretninger stiger, og tidskravet er en stadigt vigtigere faktor. Dette gælder især cyberområdet, men også inden for kontraterror og kontraefterretning er FE oppe mod aktører, der hurtigt flytter sig med hensyn til modus og teknologi.

### Skjulte mønstre

Teknologier som "smart devices", IoT og 5G gør, at mængden af data hele tiden vokser, hvilket giver efterretningstjenester mulighed for at indhente mere data. Det medfører dog også, at der er tilsvarende mere data, der skal håndteres, selv om det ofte kun er en lille del af kommunikationen, der er relevant.

Men de store datamængder kan også åbne nye muligheder. Med de rigtige redskaber bliver det muligt at se hidtil skjulte mønstre i strømmen af information. Det betyder f.eks., at information om målpersoners aktivitet kan findes i data, der tidligere er blevet sorteret fra.

*"Forudsætningen for store datamængder er, at vores indhentning er tidssvarende. Det muliggør nemlig, at vi kan udnytte de muligheder, der følger med de store datamængder. Vi kan give vores analytikere nye typer data eller præsentere dem i nye formater, der kan give en ny dimension i vores analyser",* siger Carmine Gioia.

### Kunstig intelligens (AI) og maskinlæring

Den hurtige udvikling inden for kunstig intelligens og maskinlæring de seneste år har øget værdien af data betydeligt i stort set alle sektorer. Det gælder også i FE, hvor en fokuseret indsats på disse områder allerede har ført til en øget værdi af de data, vi indhenter.

Vi har de seneste år arbejdet intensivt med kunstig intelligens og især opgaven med at opbygge den nødvendige forståelse for og strukturering af data, som er den helt afgørende forudsætning for at få succes med kunstig intelligens. Dette fokus har ført til, at kunstig intelligens i dag er integreret i vores dataløsninger.

### Finde genvejene

Udfordringen med de voksende datamængder ser kun ud til at blive større. I internettets tidlige dage var kommunikationen ren tekst, men i dag sendes billeder og videostrømme i stadigt højere opløsning – og meget ofte krypteret. Det er datatyper, der både fylder mere, og som kræver mere computerkraft og kryptoanalysekapacitet at omsætte til et format, analytikerne kan arbejde med.

FE's datacenter rummer ét af Danmarks største storage-systemer til håndtering af datamængderne. Men det er ikke nok blot at installere mere hardware. Smartere databehandling er i den grad i højsædet.

*"Det er sådan set ikke nyt. Lige siden begyndelsen på computerteknologien har der været dette kapløb mellem kapacitet og den voksende mængde information. Derfor har det også altid været en hæderkronet disciplin at finde genvejene til at løse store problemer med små ressourcer",* siger Carmine Gioia.

Ligesom Alan Turings generelle computer kom i brug for at afkode krypteret kommunikation under Anden Verdenskrig, så står tilsvarende udfordringer på spring. Med behovet for store datamængder og yderligere udvikling af teknologierne opstår der et endnu større behov for at løse udfordringerne.

*"Vi kommer ikke uden om, at moderne efterretningsarbejde kun kan lade sig gøre med avanceret databehandling. Det er én af de vigtigste forudsætninger for vores arbejde. Det vil ikke ændre sig",* konkluderer Carmine Gioia.

Vi kommer ikke uden om, at moderne efterretningsarbejde kun kan lade sig gøre med avanceret databehandling. Det er én af de vigtigste forudsætninger for vores arbejde.

Carmine Gioia

# ER KUNSTIG INTELLIGENS DE NYE SPIONER?

## Kunstig intelligens fylder mere og mere, men kan efterretningsarbejdet overlades helt til maskiner?

Når der er blevet spået om fremtiden, har der været store forventninger til den teknologiske udvikling. Selv om den faktiske udvikling endnu ikke helt har indfriet alle spådomme, er kunstig intelligens efterhånden en integreret del af hverdagen. Din smartphone kan genkende ansigter på billeder, din streamingtjeneste hjælper dig med anbefalinger, og din bil er måske selvkørende.

For bare 15 år siden kunne det være svært at få en computer til at kende forskel på en hund og en kat, mens du i dag kan styre dit hjem fra din smartphone og bruge dit ansigt til at betale med. Vi sætter mere og mere vores lid til teknologien og de mange muligheder, kunstig intelligens åbner for i hverdagen. Det gælder også i en efterretningsverden.

Hvor efterretninger før i tiden var mere eller mindre håndholdte, er teknologien i dag en vigtig faktor. I takt med at datamængden vokser, er behovet for teknologisk hjælp nemlig også steget. En efterretningstjeneste modtager enorme mængder data i alle afskygninger, og kunstig intelligens er et afgørende værktøj til at samle brikkerne og sortere i data, før en analytiker bliver præsenteret for dem. De opgaver, et menneske skulle bruge timer på, løser teknologien på få sekunder. Det gør det muligt at behandle data på ekstremt mange parametre i mange modeller og opstille sammenhænge og mønstre, der ellers havde været svære at få øje på. Og hastighed er afgørende i en efterretningsverden.

Ikke nok med at datamængden er stor, den indhentede mængde data er ofte også ustruktureret, krypteret og i mange forskellige formater. Samtidig kan kravene til dataudstilling være vidt forskellige, alt efter om der eksempelvis arbejdes med politisk-strategiske mål eller kontraterror, hvilket øger kompleksiteten.

Er kunstig intelligens så de nye spioner? Kunstig intelligens er et vigtigt og centralt element i efterretningsarbejdet, men hovedsageligt som anretter af den store databuffet, analytikerne til dagligt bliver præsenteret for. Frem for at det hele er blandet sammen i én stor skål, hjælper teknologien med at dele indholdet op, så analytikeren nøje kan vælge, hvilke informationer der er værd at se nærmere på. Det kritiske blik og den menneskelige erfaring skal fortsat i spil, før informationerne kan omsættes til meningsfulde og brugbare efterretninger.

I sidste ende vil der altså altid sidde et menneske og foretage den endelige analyse. Det ligger i efterretningstjenestens DNA, at resultater og konklusioner ikke bare dobbelttjekkes, men kontrolleres i mange led, inden de bliver til et færdigt produkt. Kunstig intelligens kan hjælpe analytikeren, men analytikeren skal også kunne tjekke resultatet og ikke mindst bruge sin faglige viden til at sætte algoritmens output ind i den rigtige kontekst. Men der er ikke tvivl om, at kunstig intelligens er en værdifuld spion-assistent, der vil spille en stadigt større rolle i fremtidens efterretninger.

For bare 15 år siden kunne det være svært at få en computer til at kende forskel på en hund og en kat, mens du i dag kan styre dit hjem fra din smartphone og bruge dit ansigt til at betale med.

Cybersikkerhed er vigtigere end nogensinde

# DEN DIGITALE TRUSSEL

Center for Cybersikkerhed har siden 2012 arbejdet for et sikkert digitalt Danmark – et arbejde, der kun er blevet mere krævende med årene. Fra centerets start til november 2021 har Thomas Lund-Sørensen stået i spidsen for det arbejde.

Truslen fra cyberkriminalitet og cyberspionage mod Danmark er igen i år på det højest mulige niveau. Det viser Center for Cybersikkerheds (CFCS') trusselsvurderinger, som udgives hvert år. Cybertruslen er eksploderet, siden CFCS blev oprettet for 10 år siden, og det er en trussel, vi som samfund skal tage meget alvorligt.

*"For 10 år siden var trusselsbilledet mere enkelt. Dengang var der enkelte velkendte efterretningstjenester, der brugte digitale værktøjer til spionage, og nogle få kriminelle, der gik efter private borgere".*

*"Det har ændret sig væsentligt. Nu står vi over for professionelle og meget dygtige hackere, der udnytter huller i vores netværk til kriminalitet. Borgere kan stadig blive ramt, men i dag går de kriminelle især efter virksomheder, som vi f.eks. så det med Demant og ISS, der blev angrebet med enorme milliontab til følge",* fortæller Thomas Lund-Sørensen, chef for CFCS.

**THOMAS LUND-SØRENSEN**

Chef for Center for Cybersikkerhed, 2012-2021

Udviklingen er sket i takt med den stigende digitalisering – en udvikling, der rummer mange fordele, men som også gør os mere sårbare, fordi den giver kriminelle eller statsstøttede hackere bedre arbejdsbetingelser. Har de først held til at bryde ind i et system, får de adgang til data i langt højere grad end tidligere. Derfor skal digitalisering og sikkerhed gå hånd i hånd.

Selv om nogle virksomheder kan være mere udsatte end andre, er cybertruslen alvorlig for alle størrelser og typer af virksomheder:

*"Hvor sikker du er som virksomhed, afhænger af dit trusselsbillede. En stor højteknologisk virksomhed eller en offentlig myndighed skal forholde sig til, at de altid er i angriberens sigtekorn. Spørgsmålet her er ikke, om man bliver forsøgt hacket, men hvornår. Men også små og mellemstore virksomheder er udsatte",* siger Thomas Lund-Sørensen.

De seneste års mange ransomwareangreb mod både store og små virksomheder peger på, at der fortsat er lavthængende frugter at plukke i forhold til at implementere helt grundlæggende sikkerhedstiltag. Vi kan løfte det sikkerhedsmæssige bundniveau med relativt enkle midler og stor effekt. De kriminelle går nemlig efter størst muligt udbytte med mindst mulig omkostning. Bliver det for besværligt det ene sted, går de hurtigt videre til det næste.

Nye teknologier som kunstig intelligens og kvantecomputere giver os nye muligheder for at beskytte vores data. Men selv om den udvikling umiddelbart kan synes positiv, har den også en dyster side.

*"Udfordringen er, at de teknologier også kan bruges til at identificere hullerne i vores systemer. Om det tipper i den ene eller anden retning er svært at sige. Mit bud er, at truslen og vores forsvar kommer til at følges ad. Men er vi bagud om to år, kommer vi ikke til at kunne indhente det om ti. Så der er behov for en konstant og også styrket indsats allerede nu",* fortæller Thomas Lund-Sørensen.

Der er altså ingen tvivl om, at cybertruslen skal tages meget alvorligt, og som led i udmøntningen af en cyberpulje på 500 mio. kr. er det politisk besluttet, at CFCS skal gennemføre en række tiltag, der skal styrke Danmarks cyberforsvar. Der er lagt op til at styrke robustheden i samfundet, blandt andet gennem bedre støtte til samfundsvigtige virksomheder og myndigheder samt bedre beskyttelse af vores kritiske infrastruktur. CFCS står altså over for en stor opgave med at sikre, at den digitale fremtid og de muligheder, den bringer med sig, ikke kommer til at stå i skyggen af cybertruslen.

Hvor sikker du er som virksomhed, afhænger af dit trusselsbillede. En stor højteknologisk virksomhed eller en offentlig myndighed skal forholde sig til, at de altid er i angriberens sigtekorn.

Thomas Lund-Sørensen

# SOLARWINDS: SKJULT BAGDØR GAV HACKERNE ADGANG TIL TUSINDVIS AF NETVÆRK

En harmløs test og en god portion tålmodighed var opskriften, da det lykkedes en gruppe hackere at angribe SolarWinds' Orion-software. Et angreb, der blev et wake-up call for mange virksomheder.

I oktober 2019 tilføjede en hacker som en test et par linjer programkode til softwarefirmaet SolarWinds' software. Kodelinjerne var i sig selv harmløse, men testen bekræftede hackerne i, at de havde fået mulighed for at udføre et af de mest opsigtsvækkende hackerangreb i nyere tid.

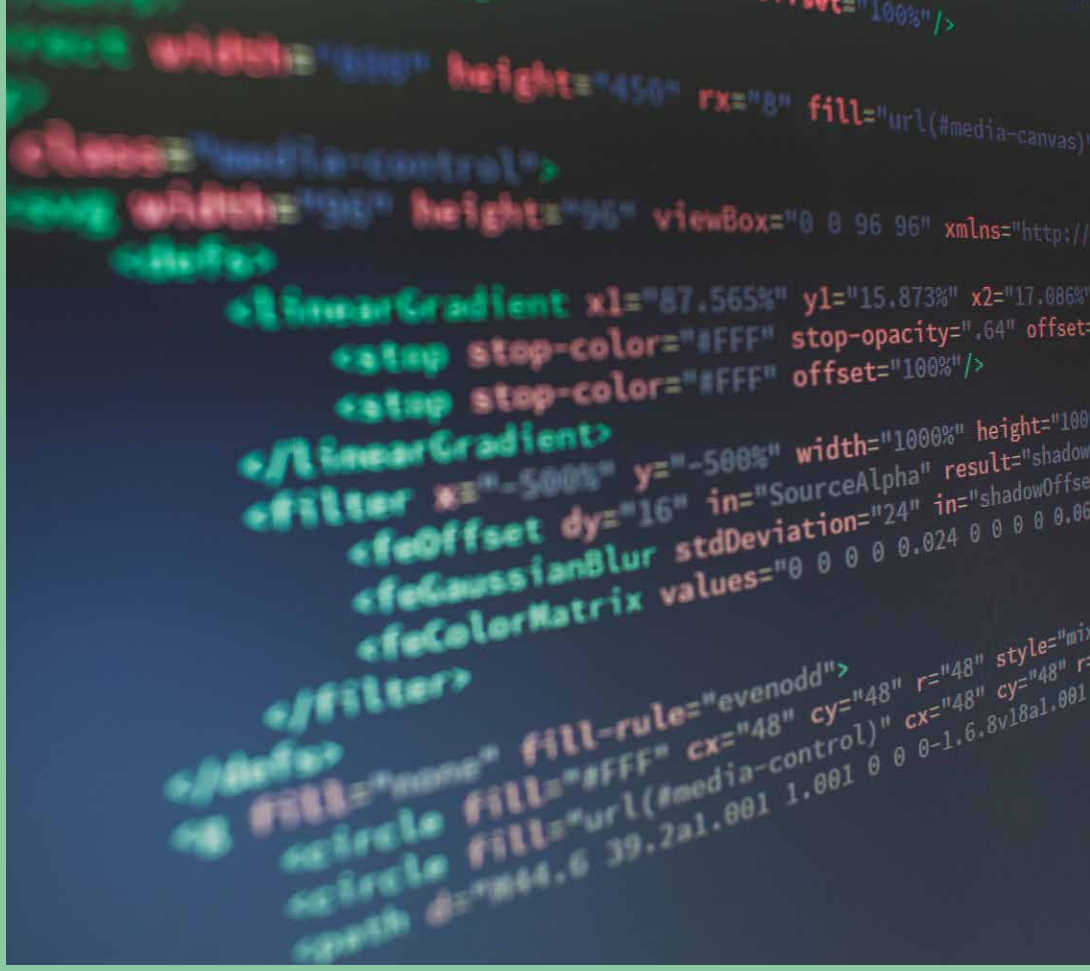
SolarWinds' Orion-software bliver brugt af tusindvis af organisationer til at styre deres it-infrastruktur. Seks måneder efter hackernes harmløse test begyndte tusindvis af systemadministratorer over hele verden at downloade en rutinemæssig opdatering til SolarWinds Orion-software. Ingen af dem vidste, at hackerne igen havde udnyttet deres adgang til at ændre i softwaren. Og denne gang var koden ikke harmløs.

Ved at placere en bagdør, dvs. en skadelig kode, i softwaren fik hackerne mulighed for at få en fod inden for hos op mod 18.000 organisationer i hele verden, som i god tro havde installeret opdateringen med bagdøren.

*"SolarWinds-sagen er den berømte undtagelse, som bekræfter reglen. At holde sine systemer opdateret til seneste version er stadig det gyldne råd til en bedre cybersikkerhed. Men sagen understreger en anden vigtig pointe: Enhver virksomheds cybersikkerhed påvirkes også af sikkerhedsniveauet hos underleverandørerne. Og det svageste led bestemmer niveauet,"* siger Thomas Lund-Sørensen.

### Udvalgte ofre

Fra marts til juni 2020, mens verden var optaget af covid-19-pandemien, var hackerne kræsne. I modsætning til NotPetya-angrebet fra 2017, der på samme måde skete ved at infiltrere en underleverandør, var SolarWinds-hackerne kun interesserede i at ramme nogle få særligt udvalgte ofre ud af de tusindvis af organisationer, som de havde fået adgang til.



På dette tidspunkt havde ingen bemærket hackernes bagdør. I juni 2020 trak hackerne følehornene til sig. Efter alt at dømme var det her, de hos nogle udvalgte SolarWinds-kunder gik et skridt videre med en ny og mere avanceret bagdør. Den tredje fase af angrebet ser ud til at være foregået ved hjælp af værktøjer, der blev udviklet til lige netop dette angreb. Hos de udvalgte ofre arbejdede hackerne aktivt for at få adgang til mere følsomme systemer i modsætning til mange andre angreb, der foregår helt eller delvist automatiseret. Således viste data fra blandt andet CFCS' sensornetværk, at hackerne nogle få steder undersøgte, om den ramte virksomhed var et mål, der var interessant for dem.

### Varslede danske ofre

Hackerne gik fortrinsvis efter amerikanske myndigheder og virksomheder inden for udvalgte brancher, heriblandt it-sikkerhedsfirmaet FireEye. Det var her, at man i december 2020 bemærkede noget usædvanligt på firmaets netværk. Det førte til en intern undersøgelse, der endte med at afsløre det spektakulære angreb. Søndag den 13. december 2020 offentliggjorde FireEye en rapport om bagdøren, som blev døbt SUNBURST. Sammen med det amerikanske center for cybersikkerhed, CISA, delte FireEye de "fingeraftryk", som kunne bruges til at finde frem til, om man var én af de organisationer, som hackerne havde kompromitteret.

*"Vi var forhåndsorienteret om, at der ville komme en alvorlig sag, så vi var klar, da de amerikanske myndigheder besluttede at dele deres oplysninger. Vi kunne således hurtigt søge efter danske ofre i vores sensornetværk og varsle de organisationer, som kunne være ramt, ud fra de data, vi indledningsvist havde adgang til",* fortæller Thomas Lund-Sørensen.

Meget tyder på, at hackerne først og fremmest var interesserede i amerikanske myndigheder. Men angrebet vidner om, at beslutsomme og tålmodige hackere med mange ressourcer i ryggen kan tiltvinge sig langvarig adgang i al ubemærkethed.

CFCS bistod en håndfuld danske organisationer, som var tilsluttet sensornetværket, med at undersøge, om de var blandt dem, hvor hackerne havde udnyttet bagdøren til at trænge dybere ind i systemerne for at udføre spionage. CFCS var desuden i kontakt med et større antal danske organisationer, der benyttede SolarWinds' software, og hvor flere af dem kunne udgøre potentielle spionagemål.

### Spor tabt i mørket

For mange af de tusindvis af SolarWinds-kunder verden over var hackernes tålmodighed en udfordring. Angrebet var foregået over så lang tid, at mange ikke kunne se langt nok tilbage i logfilerne til at udelukke, at de var blevet kompromitteret i angrebets anden og tredje fase. Det var også tilfældet hos så godt som alle de danske ofre, som ikke var tilsluttet CFCS' sensornetværk.

CFCS kunne se, at der kun var få ramte blandt de virksomheder, som var tilsluttet sensornetværket. Hos mange af de andre SolarWinds-kunder gik logfilerne kun få måneder tilbage, hvis de overhovedet eksisterede. Kunderne kunne derfor ikke vide, om de var blandt ofrene. Logning er altså en forudsætning for efterfølgende at kunne se, om man er alvorligt ramt eller ej.

CFCS har ikke set tegn på, at hackerne gik hele vejen til den tredje fase mod organisationer i Danmark. Meget tyder på, at hackerne først og fremmest var interesserede i amerikanske myndigheder. Men angrebet vidner om, at beslutsomme og tålmodige hackere med mange ressourcer i ryggen kan tiltvinge sig langvarig adgang i al ubemærkethed.

SolarWinds-sagen understreger vigtigheden af at have basale elementer som rettigheder, passwords, logning og opdateringer på plads.

# EN HELT ALMINDELIG ONSDAG I SITUATIONS-CENTERET

I Center for Cybersikkerheds Situationscenter sidder et vagthold og holder øje med alarmer i døgndrift året rundt. Alarmerne kommer ind fra de sensorer, der monitorerer mistænkelig internettrafik hos myndigheder og virksomheder, der er koblet på sensornetværket.

### SITUATIONSCENTERET

Center for Cybersikkerheds (CFCS) Situationscenter er én af de vigtigste indgange til centeret. Det er her, alarmerne kommer ind fra de sensorer, der holder øje med mistænkelig internettrafik hos myndigheder og virksomheder. Samtidig står Situationscenteret for en del af kommunikationen med tilsvarende funktioner i andre lande. Situationscenteret kommunikerer også med de danske myndigheder og virksomheder, der underretter CFCS om sikkerhedshændelser.

Situationscenteret er døgnbemandet året rundt. Det betyder også, at Situationscenteret er det sted, der kontinuerligt opretholder et situationsbillede i CFCS.

Klokken er 6:45, og i Center for Cybersikkerheds (CFCS') Situationscenter er "Nemo" og "Rusty" ved at gøre klar til at overdrage vagten til dagholdet. Mens det meste af Danmark lå og sov, har de holdt øje med de alarmer, der er kommet ind fra CFCS' sensornetværk.

*"I nat har der været mange alarmer, men andre gange sidder vi og behandler de IoC'er, vi får ind,"* fortæller "Nemo". IoC'er, forkortelsen for Indicators of Compromise, er de tekniske "fingeraftryk", som it-sikkerhedsfolk bruger til at opdage, om der f.eks. kommer malware eller trafik gennem netværket fra en server, der er kontrolleret af en kendt hackergruppe. Det kan være IP-adresser, som CFCS, sikkerhedsfirmaer og andre indsamler og deler.

Selv om de to cyberanalytikere er trætte efter en 12 timers vagt, så giver vagterne også en del frihed.

*"Det er meget fedt med tre vagter om ugen, og så har man fri. Lige nu kører vi med to uger med nattevagt og så to uger med dagvagt, og vi har altid mindst tre dage til at gå fra nat til dag. Jeg har lige købt mørklægningsgardiner, så det bliver lækkert. Så er det bare fuglene i vores baggård, der kvidrer,"* fortæller "Nemo".

### Commander's update

6:55 møder "0b1" og "GNUru" ind. "0b1" er vagtleder på dagholdet, og den første opgave er at få en mundtlig overlevering fra "Rusty", der har haft ansvaret for at føre logbogen i løbet af natten.

De lidt specielle kaldenavne, som alle cyberanalytikerne i Situationscenteret har, stammer fra uddannelsen, hvor holdet døbte hinanden ved afstemning, forklarer "Nemo" og "0b1". *"Der var endda én, der lavede en hjemmeside, så folk kunne stemme,"* fortæller "Rusty".

Klokken er 8:04, da "0b1" er ved at lægge sidste hånd på punkterne til morgenens interne briefing.

*"Der var lige en sag om en telefon, vi skulle få ind. Der skal indhentes en samtykkeerklæring, og vi skal bruge koden til telefonen. Og så skal ejeren være indforstået med, at den måske bliver destrueret efterfølgende. Så nu må vi se",* forklarer "0b1".

Opgaven som vagtholdsleder kører normalt på skift, men lige i øjeblikket er "0b1" det faste holdepunkt på dagholdet.

8:37 er alle i færd med at gøre klar til konferencen med de øvrige afdelinger i CFCS. Alle kender rutinen. Lyden bliver slået fra på tv'et, der kører i baggrunden med nyhederne, og præsentationen med punkterne i dagens briefing bliver kaldt frem på projektoren.

*"God morgen her til dagens 'Commander's Update Brief',"* siger "0b1" og begynder at gennemgå situationsbilledet på telefonkonferencen. Her gennemgås ny udvikling på igangværende sager samt udvalgte overskrifter fra dagens trusselsbillede. Alle afdelinger byder også ind på skift med dagens vigtige møder og andet, der kan være vigtigt at få delt med de andre.

Klokken 9:00 er dagens faste punkt afsluttet, men der går ikke mange minutter, før telefonerne begynder at kime. Om morgenen er det især kolleger fra andre afdelinger, der ringer for at følge op på sager eller spørge Situationscenteret til råds.

### Brunsviger og alarmer

Klokken er 13:05. "Note" spiser et stykke hjemmebagt brunsviger med den ene hånd, mens den anden rutineret klikker sig igennem det system, der viser alarmerne fra CFCS' sensornetværk. Han fokuserer på en kritisk alarm, der kommer fra en sensor hos et dansk ministerium. Den er udløst af usædvanlig trafik fra en udenlandsk IP-adresse, der står på en liste over mulige mistænkelige IP-adresser. "Note" opretter en rapport på sagen og klipper data fra sit analyseværktøj over i rapporten.

Han har fået sit kaldenavn "Note", fordi han på cyberanalytikeruddannelsen altid havde komplette noter, der dækkede al den information, der stod på de PowerPoint-præsentationer, deltagerne ellers ikke kunne få udleveret. Evnen til at tage hurtige noter kan ses, når han hastigt indtaster feltkoder, screenshots og får skrevet en konklusion. I dette tilfælde: Falsk positiv. Klokken 13:10 er "Note" allerede videre til den næste alarm.

> Min opgave er at skærme de andre, så de kan fokusere på vores kerneopgaver. Så jeg svarer på mails, telefoner og chefer, der har brug for noget.
>
> "0b1"

### Svindelsider

16:21 stiger aktiviteten yderligere. I takt med at arbejdsdagen slutter for mange af dem, Situationscenteret kommunikerer med, tikker opdateringer og opgaver ind. Som vagtholdsleder er det "0b1", der tager telefonen.

*"Min opgave er at skærme de andre, så de kan fokusere på vores kerneopgaver. Så jeg svarer på mails, telefoner og chefer, der har brug for noget,"* forklarer "0b1".

"Note" er i gang med én af kerneopgaverne og tjekker potentielle phishing-sider ved hjælp af et værktøj, som analytikerne i Situationscenteret selv har udviklet. Det holder øje med nye sider, der registreres, og henter automatisk screenshots og anden information, som hjælper "Note" med at vurdere, om siderne er suspekte. En af siderne ser ud til at være en side for et tysk pizzeria, en anden side er lige nu tom, men domænenavnet kunne tyde på, at den vil blive kørt i stilling til netbank-phishing.

Klokken 17:59 er der faldet ro på igen, og det meste af dagholdet er gået. "0b1" er i færd med at opdatere logbogen og forberede overleveringen til natholdet. 18:23 møder "Wiz" og "Snap" fra natholdet og så begynder overleveringen af dagens begivenheder. En af de presserende opgaver er en underleverandør til et projekt hos Forsvaret, som muligvis har været udsat for et forsøg på et brute force-angreb.

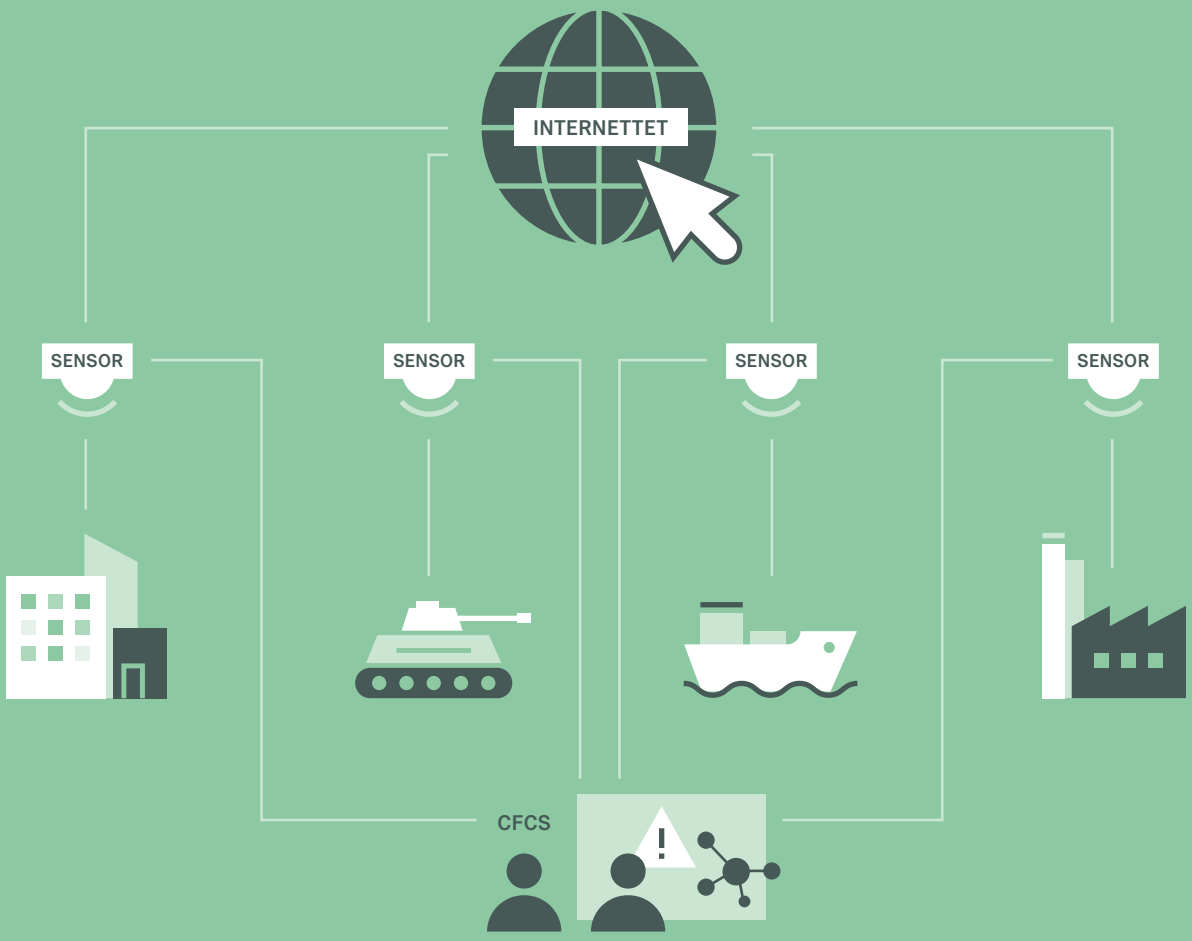
*"Vi har haft kontakt med dem, men hvis I får samtykkeerklæringen ind fra dem, må I meget gerne lægge den på sagen,"* siger "0b1", som slutter overleveringen med en praktisk instruks: "*Og i andre opgaver så skal vi huske at tømme opvaskemaskinen".*

### CYBERANALYTIKER

Uddannelsen som junior cyberanalytiker er et særligt forløb, som CFCS har kørt to gange. Et tredje hold skal uddannes i foråret 2022. Uddannelsen er beregnet til dem, der måske ikke har en formel uddannelse inden for it, men har interesse og evner, der kan gøre dem til gode analytikere.

Flere af de junioranalytikere, der er startet i Situationscenteret efter uddannelsen, er skiftet til andre afdelinger i CFCS, der også kan bruge talenterne. Derfor er der behov for løbende at finde nye kandidater og uddanne dem.

Selve uddannelsen er et tremåneders forløb med løn. Derefter bliver langt de fleste ansat i CFCS, men enkelte er blevet ansat hos private virksomheder eller i andre myndigheder i tilsvarende funktioner. I CFCS bliver junioranalytikerne oplært i de forskellige systemer og procedurer.




## CENTER FOR CYBERSIKKERHEDS SENSORNETVÆRK

CFCS' netsikkerhedstjeneste driver et sensornetværk, som kan opdage cyberangreb og forsøg på cyberangreb. Det nuværende sensornetværk er et egenudviklet system, som består af hardwareenheder placeret på internetforbindelsen i for eksempel flere ministerier og offentlige myndigheder.

Sensornetværket indeholder en række regler, der bruges til at genkende forsøg på cyberangreb. Det kan være IP-adresser eller internetdomæner, der bliver brugt af en hackergruppe, eller det kan være digitale fingeraftryk af filer, der indeholder malware. Når der registreres potentielt skadelig trafik, der passer på en regel, modtager CFCS' Situationscenter en alarm.

CFCS har set forsøg på cyberspionage, som er foregået over flere måneder, før de blev opdaget. Derfor opbevarer sensorerne trafikdata og pakkedata op til 13 måneder, så det er muligt at gå tilbage og se, hvad der skete, da angrebet begyndte.

# EN RET ALMINDELIG ARBEJDSPLADS MED EN UALMINDELIGT VIGTIG OPGAVE

En stor del af vores hverdag er hemmelig, og vores opgaver er lidt ud over det sædvanlige. Men vi er også en almindelig arbejdsplads, og medarbejderne er vores allervigtigste aktiv.

At arbejde i FE er ganske særligt og helt almindeligt på samme tid. Vi arbejder med hemmelige opgaver, og det præger vores hverdag og den måde, vi arbejder på. Vi har fået mandat til at udnytte helt særlige midler til at afdække, hvad andre stater og udenlandske aktører forsøger at holde hemmeligt – og derfor løser vi opgaver, du ikke finder mage til andre steder. Men vi er også helt almindelige mennesker, der bringer vores forskellige baggrunde og uddannelser i spil i en hverdag, der til tider er lidt ud over det sædvanlige.

**FE har brug for din viden**

FE er en vidensorganisation, og vores medarbejdere er afgørende for, at vi kan løse vores opgaver og levere den viden, der skal til for at modvirke trusler. Viden er både vores vigtigste vare og vores stærkeste kort, når vi skal holde Danmark sikkert.

FE er en all source-efterretningstjeneste. Det betyder, at vi beskæftiger os med alle indhentningsdiscipliner og tilsvarende analysearbejde. Derfor er vi en fagligt meget alsidig organisation, hvor vores medarbejdere også har meget forskellige baggrunde. Vi har blandt andet ingeniører, it-medarbejdere, selvlærte hackere, sprogofficerer, jurister, antropologer, historikere og militært ansatte. Pladsen til forskellighed gennemsyrer hverdagen i FE, og på gangene møder du alt fra jakkesæt og stiletter til hættetrøjer og sneakers. Og selv om det ikke er så ofte, som mange måske ville tro, er der også kollegaer i uniform.

Vi tror på, at det netop er vores forskelligheder, der gør os stærke, og vi værdsætter styrken i vores mangfoldighed med dybe fagligheder og specialer. Men én ting har alle FE-medarbejdere til fælles uanset baggrund og funktion: Vi arbejder for at beskytte Danmark og danske interesser. Det er dét, der samler os, og dét, der gør FE til en helt særlig arbejdsplads.

### Når stoltheden må bæres i stilhed

Opgaverne i FE vil ofte være hemmelige, så vi kan beskytte vores kilder, kapaciteter og samarbejdspartnere. Det betyder, at vores største succeser forbliver hemmelige, men det betyder også, at der er et stærkt kollegafællesskab, hvor der er plads til at vende både stort og småt – og ikke mindst til at fejre succeser. Hvor vi udadtil kan virke meget lukkede, bliver mange nye kollegaer overraskede over den store åbenhed indadtil.

*"Jeg var overrasket over, hvor åbne, søde og hjælpsomme alle medarbejdere har været. Det er ikke det billede, man får udefra med hemmelighedsboblen, der omkranser FE"*, siger en ny medarbejder i FE.

Åbenhed indadtil styrker kollegarelationerne og dermed også samarbejdet på tværs. Som medarbejder i FE er der gode muligheder for at blive ekspert inden for dit felt, men det er en forudsætning, at du kan arbejde sammen med andre faggrupper. Specialisering og samarbejde er nemlig helt afgørende for, at vi kan levere effektivt efterretningsarbejde i høj kvalitet til vores kunder og samarbejdspartnere.

### Hvis du overvejer at søge job i FE

Søger du job hos FE, vil du ikke altid kende jobbet til fulde, før du begynder hos os. Vores særlige arbejdsvilkår gør nemlig, at vi ofte først kan fortælle om alle dine arbejdsopgaver, når du er ansat og har været igennem vores sikkerhedskurser.

Allerede når du søger jobbet, vil din omgangskreds måske finde det interessant. Derfor anbefaler vi, at du, for at beskytte dig selv, er diskret om, at du har søgt job hos FE. Det gælder både, når du møder folk ansigt til ansigt og på de sociale medier. Her i "Indblik" sætter vi navn og ansigt på nogle af FE's direktionsmedlemmer, men for langt de fleste andre ansatte gælder, at de er – og skal være – anonyme.

Diskretion om jobbet er et grundvilkår, når du arbejder i en efterretningstjeneste, men dybden i din diskretion vil selvfølgelig afhænge af din funktion i tjenesten. Der er meget sikkerhed forbundet med at arbejde i FE – både for at passe på vores viden og arbejdsmetoder og også for at holde FE's kapaciteter hemmelige. Det store fokus på sikkerhed er med til at skabe en anderledes arbejdssituation, og det skal du have overvejet, inden du søger job i FE.

### Den første tid i det hemmeliges tjeneste

Det er både spændende og anderledes at blive ansat i en efterretningstjeneste, og i den første tid vil der være mange nye ting, du skal lære – uanset hvilken baggrund du kommer med. Derfor har vi sammensat et helt særligt introduktionsforløb, hvor du som nyansat blandt andet bliver uddannet i, hvordan du forholder dig til de sider af arbejdet, der har med sikkerhed at gøre. Derudover får du indblik i efterretningskredsløbet og andre funktioner end den, du selv arbejder i. Det er med til at give dig de rette forudsætninger for at samarbejde på tværs af tjenesten. Efterretningsarbejde er nemlig en holdindsats, og gode samarbejdsevner er afgørende, når du arbejder i FE.

*"Jeg synes, at FE er kendetegnet ved åbenhed, læringsvillighed, stor professionalisme og utrolig glæde ved nye medarbejdere – jeg har følt mig rigtig velkommen"*, fortæller en ny medarbejder i FE.

Vi har primært til huse i Københavnsområdet – i historiske bygninger på Kastellet, i Holsteinsgade på Østerbro og på Sandagergård på Amager. Herudover har vi et mindre antal kollegaer i Hjørring-området.

Vi arbejder på at samle de tre lokationer i København i et nybygget domicil på Svanemøllens Kaserne.

Hold øje med nye jobopslag på **www.fe-ddis.dk** og på vores LinkedIn-profiler

# NYT FÆLLES HOVEDSÆDE TIL FE

FE har i mange år udført efterretningsarbejdet fra forskellige adresser. I dag arbejder de fleste af vores medarbejdere i Forsvarets bygninger på Kastellet i København, på Sandagergård på Amager eller i kontorlokaler på Østerbro. Men inden for en overskuelig fremtid forventes alle vores medarbejdere – på nær vores medarbejdere i Hjørring – at blive samlet på én fælles lokation i København. Herfra skal fremtidens efterretningstjeneste drives fra et moderne og topsikret domicil. Byggeriet er i skrivende stund i planlægningsfasen, så det er endnu ikke endeligt afklaret, hvornår det vil stå færdigt.

Det nye hovedsæde skal ligge på Svanemøllens Kaserne, hvor Forsvaret i dag blandt andet allerede huser Forsvarsakademiet. Selve kaserneanlægget udgør et helt unikt militært område, og med sin bynære placering, sine smukke gamle bygninger og grønne udearealer har det en helt særlig stemning og atmosfære, der i fremtiden vil komme FE's medarbejdere til gode. Hele området er under forvandling og vil i de kommende år blive moderniseret og udbygget med en række nye funktioner. Planlægningen af projektet er i gang, og når de nødvendige godkendelser er på plads, forventes byggeriet at kunne starte i løbet af de næste par år. Kaserneområdet forbliver militært, og FE's nye domicil får en yderst attraktiv placering i kasernens vestlige hjørne.

Ved at samle FE på én fælles lokation styrkes muligheden for tværfagligt samarbejde – og derved højnes niveauet for efterretningsarbejdet. Det nye bygningsanlæg vil desuden medvirke til at højne tjenestens sikkerhed, så FE er rustet til at imødegå fremtidige trusler.

Selve domicilet vil indeholde omfattende sikkerhedsfaciliteter og en række særfunktioner knyttet til efterretningstjenestens særlige behov. Rammerne vil være moderne og fremtidssikrede og skal blandt andet medvirke til at binde organisationen sammen og understøtte effektive arbejdsgange og et godt arbejdsmiljø.

### Det faglige miljø

I udformningen af det nye domicil er det centralt, at FE's medarbejdere får gode muligheder for fordybelse og for tæt kontakt, sparring og videndeling med kolleger. Tjenestens arbejdsopgaver kræver en høj grad af tværfaglig koordination, og de fysiske rammer skal understøtte et stærkt fagligt miljø og en fælles kultur på tværs af organisationen, hvor der er gode muligheder for at mødes både fagligt og socialt.

FE's organisering ændres løbende og justeres i takt med, at opgaverne ændrer sig, ny teknologi implementeres, og nye arbejdsprocedurer og -mønstre skal indarbejdes. Det nye domicil vil derfor være udformet med en indbygget fleksibilitet, der sikrer, at de fysiske rammer let kan justeres, så efterretningsarbejdet kan udføres på bedste vis mange år frem i tiden.

### Fysisk sikkerhed

FE arbejder med højt klassificerede informationer, herunder med materiale fra samarbejdspartnere og kunder, der har tiltro til, at FE beskytter deres materiale. Sikring og overvågning af det nye domicil har derfor høj prioritet – både i den kommende anlægsfase, i det færdige byggeri og ikke mindst i driften af det.

# PASSER DU IND I FE?

Vi stiller hverken krav om militær baggrund eller spionerfaring, hvis du skal arbejde i FE. Til gengæld skal du være blandt de bedste inden for dit felt og motiveres af at styrke Danmarks sikkerhed. Her kan du se eksempler på nogle af de medarbejdertyper, der arbejder i FE.

### DEN ELEKTRONISKE INDHENTER

Elektronisk indhentning (SIGINT) er en kompleks efterretningsdisciplin, der kræver mange forskellige kompetencer. Den elektroniske indhenter har typisk en teknisk baggrund, f.eks. som ingeniør, datalog, matematiker eller it-tekniker. Det er fagspecialister med et solidt kendskab til digital kommunikation, som blandt andet står for at udvikle og vedligeholde FE's tekniske indhentningskapaciteter. Det kan også være kryptologer, der kan bryde krypteret kommunikation. Den elektroniske indhenter er typisk god til at spotte teknologiske trends.

### NETVÆRKSINDHENTEREN OG -BESKYTTEREN

I FE er der flere måder at arbejde med it-netværk på, men det overordnede formål er det samme: at skaffe efterretninger og beskytte netværk. Både netværksindhenteren og -beskytteren har et dybt kendskab til internettets struktur, computere, programmer og applikationer. Netværksindhenteren skaber adgang til de informationer, vi skal bruge for at løse vores efterretningsmæssige opgave. Den uddannelsesmæssige baggrund og de personlige spidskompetencer er forskellige, men alle har stor samarbejds- og læringsevne, kreativitet og teknisk snilde.

### FØRINGSOFFICEREN

Føringsofficeren, også kaldet indhenteren, skaffer oplysninger fra personer, som videregiver oplysninger af følsom karakter. En føringsofficer skal være dygtig til at få alle typer af mennesker i tale, til at håndtere stress og uforudsete situationer og i det hele taget kunne acceptere en vis form for risiko. I FE's uddannelse til føringsofficer indgår blandt andet skydning, kørsel og udvidet førstehjælp. Føringsofficerer kan have mange forskellige baggrunde, og mange har en videregående uddannelse, men det afgørende er de personlige kvalifikationer.

### DATAUDVIKLEREN

FE indhenter store mængder data, som i deres rå form sjældent gør nytte. Dataudviklerne sørger for at ensrette og systematisere data, så FE's analytikere hurtigt kan finde de relevante data. Dataudviklerne i FE har både berøring med indhentning og analyse og med udvikling og drift, så de skal både være dygtige softwareudviklere, kunne samarbejde med et bredt udsnit af FE's øvrige medarbejdergrupper og have et godt indblik i efterretningsbehovene. Dataudviklernes opgaver spænder fra overførsel af data til datamodellering, inklusive anvendelse af kunstig intelligens og machine learning, samt udvikling af brugergrænseflader. Dataudvikleren har typisk en it-uddannelse, en naturvidenskabelig baggrund eller er ingeniør.

### DEN AVANCEREDE IT-MEDARBEJDER

It er essentielt for alt arbejde i FE. Derfor har FE it-medarbejdere, der både har avancerede it-kundskaber og kan se organisationens efterretningsmæssige behov og tænke dem ind i teknologiske muligheder. FE har både it-specialister og it-generalister, men udviklingen kræver, at den avancerede it-medarbejder er alsidig og hurtigt kan tilpasse sig den teknologiske udvikling. Nogle af FE's it-medarbejdere varetager den daglige drift af FE's kerne-it og sikrer, at organisationens systemer arbejder sammen, er stabile og opdaterede. Andre arbejder med avancerede systemer, som er direkte relateret til FE's indhentning, analyse og rapportering. Den avancerede it-medarbejder kan have mange forskellige uddannelsesmæssige baggrunde, men er ofte ingeniør, datamatiker eller har en anden teknisk baggrund.

### SIGINT-ANALYTIKEREN

SIGINT-analytikeren har veludviklede it-kundskaber og kan typisk et eller flere fremmedsprog på højeste niveau. SIGINT-analytikeren arbejder med alle typer elektronisk indhentet data og har stor indsigt i indhentningens muligheder. SIGINT-analytikeren skal være i stand til at overskue mange forskellige typer komplekse data, som skal fremsøges, udvælges og analyseres i en række forskelligartede systemer. SIGINT-analytikeren har typisk en lang videregående sproglig og/eller samfundsvidenskabelig uddannelse og har ofte boet i eller arbejdet med et bestemt område gennem længere tid.

### ALL SOURCE-ANALYTIKEREN

På baggrund af analyser af materiale fra alle FE's indhentningsdiscipliner udfærdiger all source-analytikeren produkter til FE's kunder og partnere. All source-analytikerens arbejdsområde er defineret geografisk eller emnemæssigt. All source-analytikeren skal både have et dybt fagligt kendskab til sit område og indsigt i indhentningens muligheder. All source-analytikeren har typisk en samfundsvidenskabelig eller humanistisk akademisk uddannelse.

### MILITÆRANALYTIKEREN

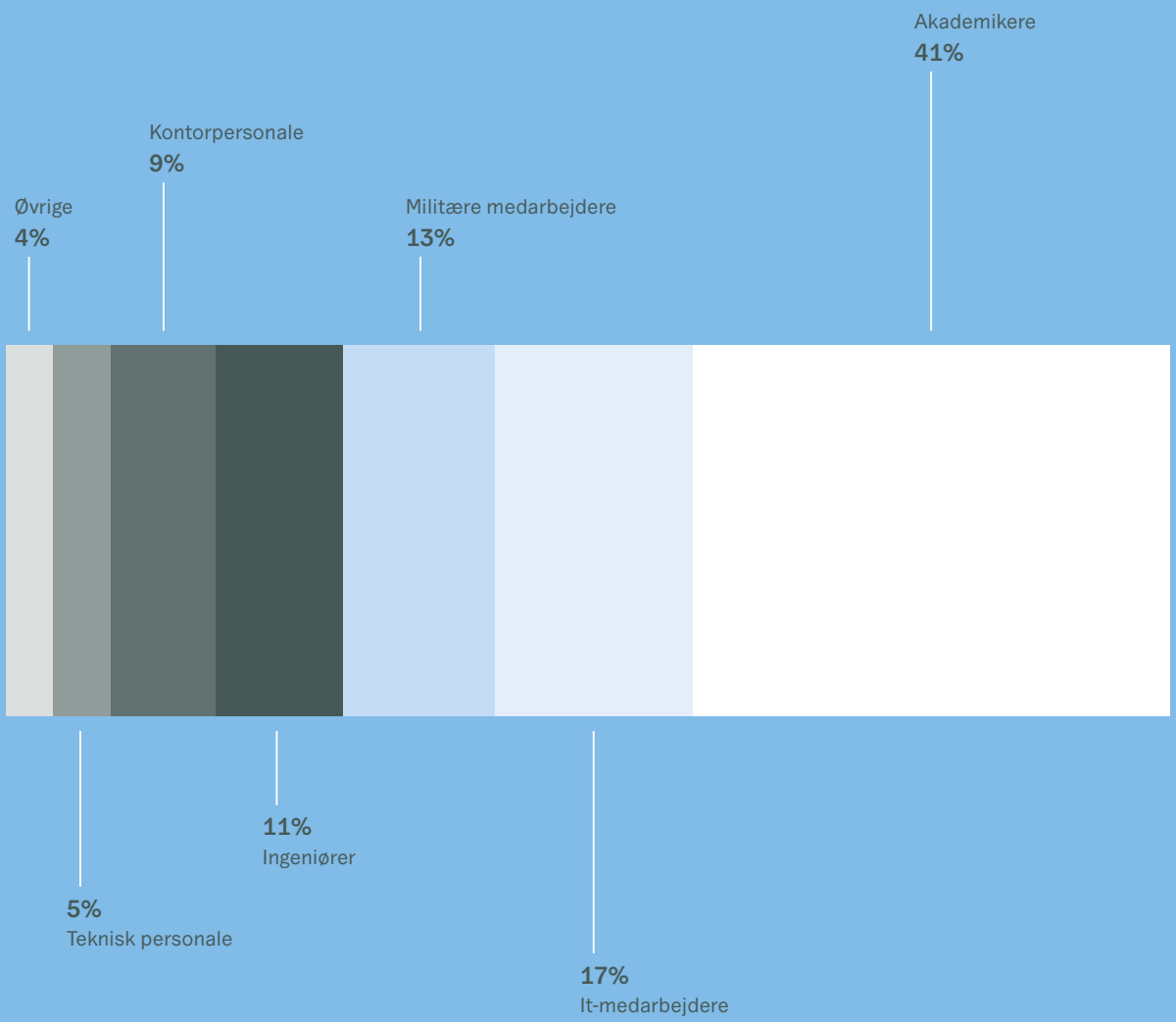
Den militære all source-analytiker arbejder sammen med de civile all source-analytikere samt analytikere, der er specialiseret inden for FE's indhentningsdiscipliner. Militæranalytikeren bidrager med sine militære kompetencer og står typisk for de dele af analysen, som er rene militære vurderinger. Militæranalytikeren skal kunne overskue store og komplicerede mængder af data og have en solid og bred erfaring og faglighed inden for sit værns militære fagområder eller på tværs af værnene. Militæranalytikeren kan udsendes sammen med Forsvaret for at levere direkte efterretningsstøtte til de udsendte enheder.

### DEN OFFENSIVE OPERATIONSPLANLÆGGER

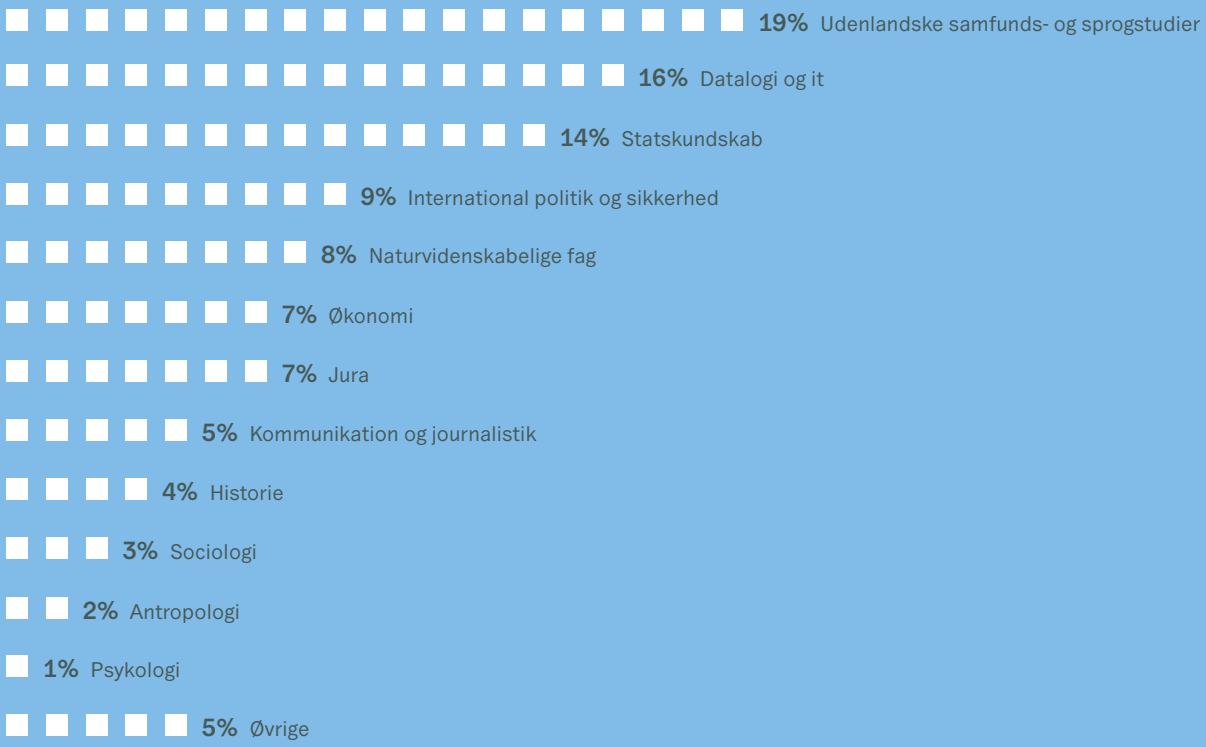
Den offensive operationsplanlægger er omdrejningspunktet, når FE støtter Forsvaret med offensive militære cyberoperationer. Den offensive operationsplanlægger analyserer og udvælger relevante cyberrelaterede mål, som vil kunne angribes for at opnå den ønskede effekt. Opgaven indeholder både indhentning og analyse og har et stærkt operativt fokus. Den offensive operationsplanlægger besidder typisk en høj grad af kreativitet, veludviklet samarbejdsevne og god teknisk forståelse. Den offensive operationsplanlægger har oftest en akademisk og/eller militær baggrund.

# MEDARBEJDERFORDELING

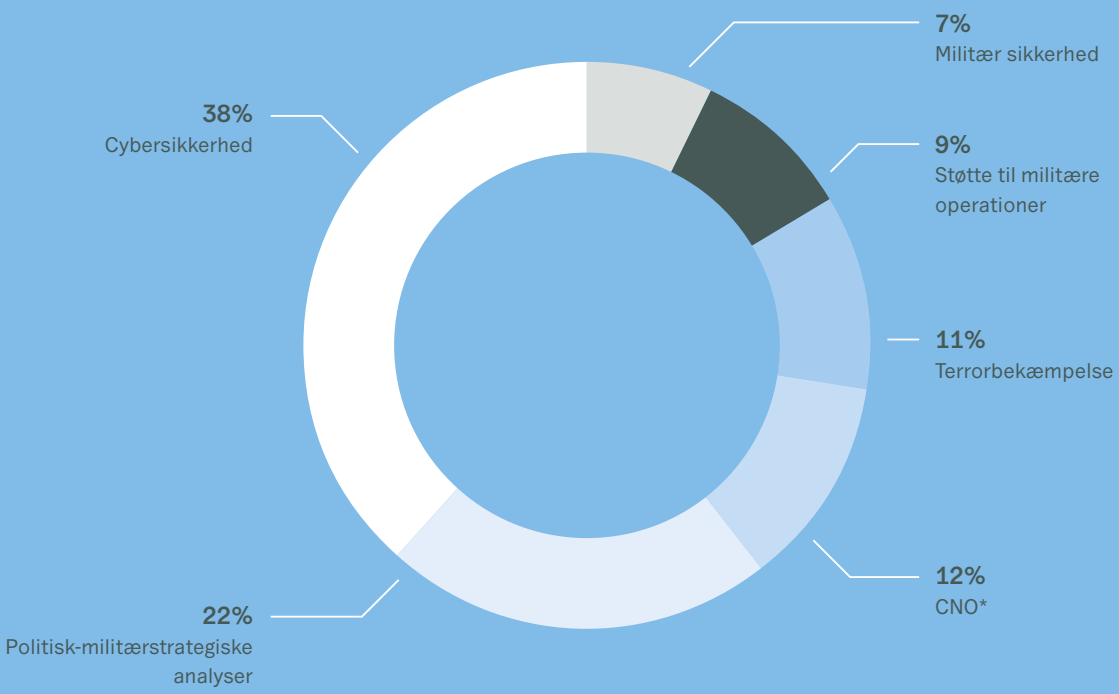
## FE'S MEDARBEJDERES BAGGRUND



## FE'S CIVILE AKADEMIKERE UNDER KONTORCHEFNIVEAU




## MEDARBEJDERE FORDELT PÅ FE'S OVERORDNEDE FOKUSOMRÅDER




* Når ressourcerne ikke anvendes til CNO, indgår de i løsningen af FE's øvrige opgaver.

# ORGANISATION

FE er organiseret i seks sektorer – tre operative og tre tværgående.

## OPERATIVE SEKTORER

De tre operative sektorer beskæftiger sig direkte med FE's kerneopgaver: at forebygge og modvirke trusler mod Danmark og danske interesser.

### Efterretning

Sektoren for efterretning samler størstedelen af FE's efterretningsmæssige kompetencer og har tre hovedopgaver: vidensopbygning, varsling og modvirkningsindsats. Sektoren indhenter med sine forskellige kapaciteter data og informationer, som bearbejdes og omdannes til analyser og viden. Meget af denne viden danner grundlag for de varslinger, som FE løbende leverer til sine kunder.

### Center for Cybersikkerhed

Center for Cybersikkerhed medvirker blandt andet til at styrke cybersikkerheden i de samfundsvigtige sektorer. Det sker f.eks. gennem rådgivning og monitorering af myndigheder og virksomheders netværkskommunikation for at imødegå de mest avancerede cyberangreb. Centeret er desuden myndighed for informationssikkerhed og beredskab på teleområdet.

### Støtte til Forsvaret

Sektoren har ansvaret for at støtte Forsvaret og NATO, og har blandt andet ansvaret for den militære sikkerhed inden for Forsvarsministeriets område, at yde efterretningsmæssig støtte til militære operationer og at støtte Forsvaret med både offensive og defensive cyberoperationer (Computer Network Operations, CNO) i forbindelse med militære operationer.

## TVÆRGÅENDE SEKTORER

De tværgående sektorer understøtter FE's operative sektorer i deres arbejde.

### Jura og Ledelsesstøtte

Jura og Ledelsesstøtte har ansvaret for de juridiske opgaver i FE, bistår direktionen, koordinerer betjeningen af Forsvarsministeriet, håndterer presse og kommunikation og varetager forbindelsen til FE's udenlandske samarbejdspartnere.

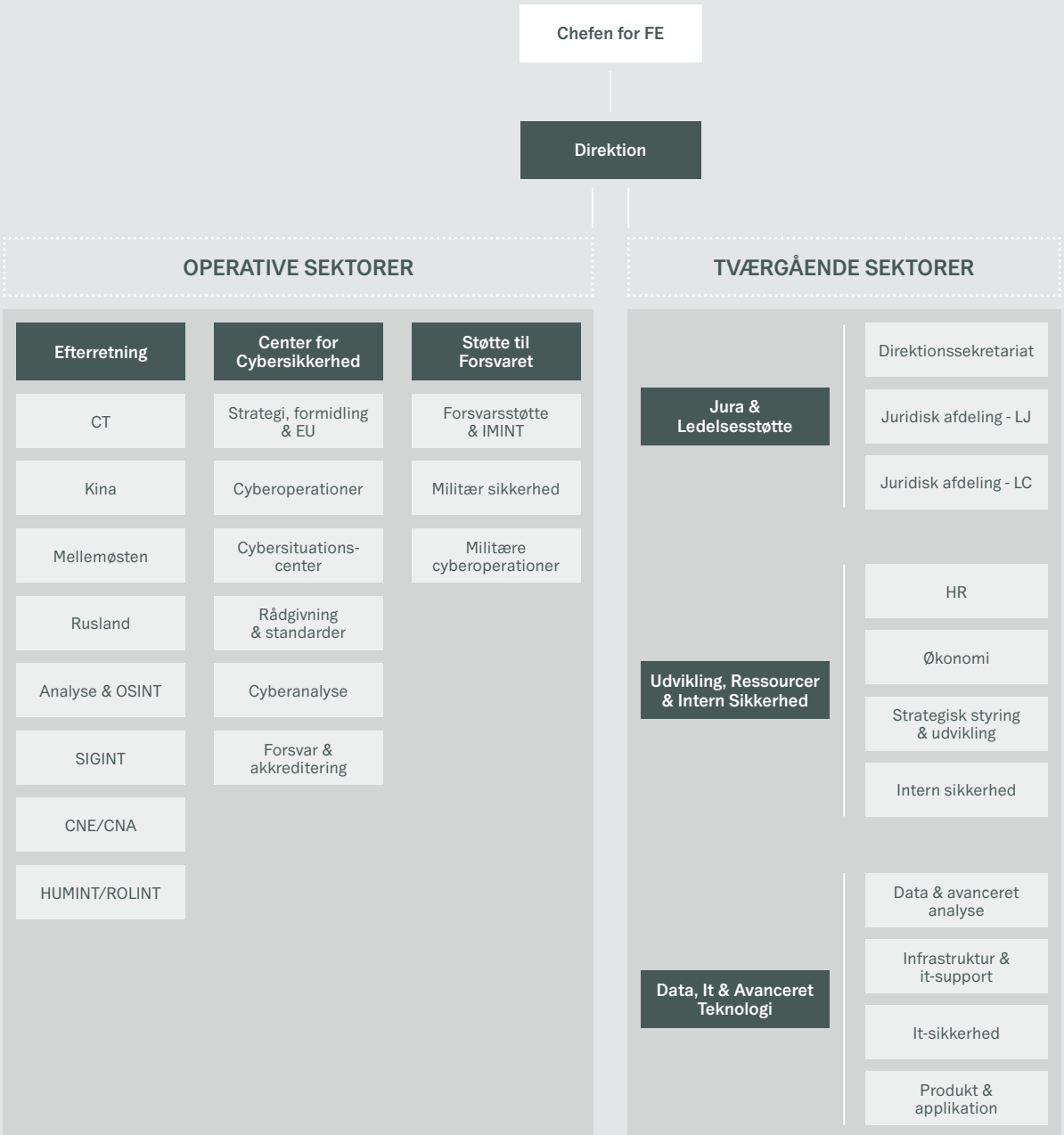
### Udvikling, Ressourcer og Intern Sikkerhed

Sektoren understøtter hele FE og samler en række centrale stabsfunktioner. Sektoren har ansvaret for HR, økonomi og FE's udviklingsopgaver. Herudover har stabssektoren ansvaret for FE's interne sikkerhed.

### Data, It og Avanceret Teknologi

Sektoren for data, it og avanceret teknologi har ansvaret for at udvikle og vedligeholde FE's data- og teknologinfrastruktur. Herudover står sektoren for drift og udvikling af it-systemer og applikationer samt den interne it-sikkerhed.

## ORGANISATIONSDIAGRAM



# FE'S ØKONOMISKE RAMME

FE fik i 2021 en samlet bevilling på 1.045,1 mio. kr. Ved det seneste forsvarsforlig fik FE tildelt yderligere midler (34 mio. kr. i 2018 stigende til 230 mio. kr. i 2023, når forliget er fuldt implementeret). De tildelte midler vil primært skulle styrke FE's evne til at imødegå cybertrusler, men der er også afsat midler til at imødegå påvirkningsoperationer mod Danmark fra fremmede stater og til at sikre FE's fortsatte teknologiske udvikling. Præcis hvordan pengene bruges, kan vi ikke offentliggøre. Det vil nemlig løfte sløret for vores kapaciteter og dermed gøre os og Danmark mere sårbare over for fremmede staters efterretningstjenester.

I juni 2021 blev forligsreserven på 500 mio. kr. udmøntet. FE fik tildelt en væsentlig del af reserven i resten af perioden, dvs. fra 2021 til og med 2023. Disse midler skal hovedsageligt bruges til at styrke det danske cyberforsvar.

FE's årlige bevilling forventes med udgangen af forligsperioden at være på ca. 1,1 mia. kr. Dertil kommer et væsentligt beløb fra forligsreserven, der ikke er endeligt udmeldt i skrivende stund.

**INDBLIK**
Forsvarets Efterretningstjenestes
beretning 2019-2020

**Udgivelse**
December 2021

**Foto**
Side 6, 11, 16, 29, 36, 43, Trine Bukh
Side 1, 9, 52, pexels.com
Side 22, 32, 40, 46, unsplash.com

**Design og layout**
e-Types

**Tryk**
Dystan og Rosenberg

**Papir**
Indhold: Scandia 2000 White 130g
Omslag: Scandia 2000 White 300g


Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Telefon: 3332 5566
www.fe-ddis.dk
www.cfcs.dk