

INDBLIK

Beretning 2021-2022



**FORSVARETS
EFTERRETNINGSTJENESTE**



FE er ikke alene om at beskytte Danmark, men vi er de eneste med mandat til at udnytte helt særlige midler for at afdække andre stater og udenlandske aktørers hemmeligheder.

INDHOLD

4	Forord
6	FE gør Danmark sikkert
	■ EN ÆNDRET SIKKERHEDSPOLITISK DAGSORDEN
8	Krigen har fornyet vores fokus på truslen fra Rusland
12	Trusler mod Danmark og danske interesser
14	Sådan får FE sin viden
16	Mød Martin, Ruslandsanalytiker i FE
	■ STYRKET STØTTE TIL FORSVARET
18	FE's kontraspionage i Danmark er igen blevet højaktuel
20	FE hjalp danske soldater i Mali på 4.000 kilometers afstand
24	Mød Ellen, dataanalytiker i FE
	■ EFTERRETNINGER SOM IT-DISCIPLIN
26	Teknologi er drivkraft for forandring i FE
29	Data- og it-stillinger i FE
30	Mød Rasmus, data scientist i FE
	■ CYBERSIKKERHED
32	Vi beskytter den kritiske infrastruktur mod cyberangreb
36	Cybersikkerhed og nye teknologier
40	Mød Marcus, malwareanalytiker i CFCS
	■ VIDE RAMMER FORPLIGTER
42	Åbenhed i en hemmelig tjeneste
45	Én tjeneste – to lovgrundlag
46	Mød Marie, jurist i FE
	■ VORES HEMMELIGE HVERDAG
49	En ret almindelig arbejdsplads med en ualmindelig vigtig opgave
52	FE har også brug for dig
54	Medarbejderfordeling
56	FE's nye hovedsæde
58	Sådan bliver du ansat i FE
59	Vokseværk kræver nytænkning af FE's rekruttering
60	Cyberdemon og Unipwnie – den ondeste og sødeste CTF
62	Mød Claus, underviser i FE
64	Organisation
66	FE's økonomiske ramme



SVEND LARSEN

Fungerende chef
for Forsvarets
Efterretningstjeneste

FORORD

■ Denne udgave af FE's beretning dækker 2021 og 2022. I den periode er der naturligvis særligt én begivenhed, der springer i øjnene og har haft betydning ikke bare for FE, men for verden som sådan – nemlig Ruslands invasion af Ukraine i februar 2022.

Det er FE's kerneopgave at klæde beslutningstagere i Danmark på til at træffe vigtige og svære udenrigs- og sikkerhedspolitiske beslutninger, men krigen i Ukraine har alligevel været en helt speciel situation, hvor vi i særlig grad har kunnet bringe vores kompetencer i spil. Krigen har også været en unik mulighed for os i FE til at lære og udvikle nye metoder.

Som lille nation har Danmark alle dage haft brug for gode venner og alliancepartnere, og det gælder også for FE. Krigen i Ukraine har i særlig grad illustreret værdien af tæt samarbejde mellem lande med samme værdigrundlag. I FE har vi gennem mange år haft et meget stærkt samarbejde med en række partnerlande – et samarbejde som vi har styrket yderligere efter den russiske invasion. Det er vi glade for, da det er med til at gøre Danmark endnu mere sikkert.

Men FE må og skal også selv holde sig opdateret uafhængig af omverdenen. Det gælder blandt andet i forhold til den teknologiske udvikling, hvor f.eks. kunstig intelligens, machine learning og kvanteteknologi i disse år markant flytter grænserne for, hvad der er muligt.

Ukraines tilgang til brugen af bl.a. droner og satellitbilleder har gjort værdien af en effektiv udnyttelse af data og ny teknologi meget tydelig. Som moderne efterretningstjeneste er FE allerede i dag en højteknologisk og datadrevet arbejdsplads, og vi ansætter hver eneste måned mange nye medarbejdere, der skal være med til at udvikle os yderligere.

FE vokser således markant i disse år, navnlig med nye kollegaer som skal løfte vores arbejde med avancerede teknologier og datahåndtering. Vi forventer, at den udvikling kommer til at fortsætte. Verden er blevet mere usikker, trusselsbilledet er det mest komplekse i årtier, og det er Danmark og FE nødt til at forholde sig til.

Vi kan meget i FE. Også meget, som vi ikke kan fortælle om. Sådan er vilkårene for en efterretningstjeneste, hvor diskretion er både en æressag og en nødvendighed. Vi holder på vores hemmeligheder, men på de områder, hvor vi kan fortælle mere, vil vi gerne være så åbne om vores arbejde, som det er muligt.

Her i INDBLIK kan du derfor læse om nogle af de helt særlige opgaver, som vi løser, samt møde en række af vores medarbejdere og få et indblik i, hvorfor de arbejder i FE.

Vi håber, at du har lyst til at læse med.

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-sikkerhedsmyndighed, kompetencecenter for cybersikkerhed og myndighed for informationssikkerhed og beredskab på teleområdet
- Vi leverer defensive og offensive cybereffekter til støtte for Forsvaret

■ KRIGEN HAR FORNYET VORES FOKUS PÅ TRUSLEN FRA RUSLAND

Krigen i Ukraine har ændret den sikkerhedspolitiske situation i Europa. For FE har krigen betydet et skærpet fokus på truslen fra Rusland – på kort og langt sigt. FE's chef for efterretning, Anja Dalgaard-Nielsen, fortæller om krigens betydning for FE's arbejde.

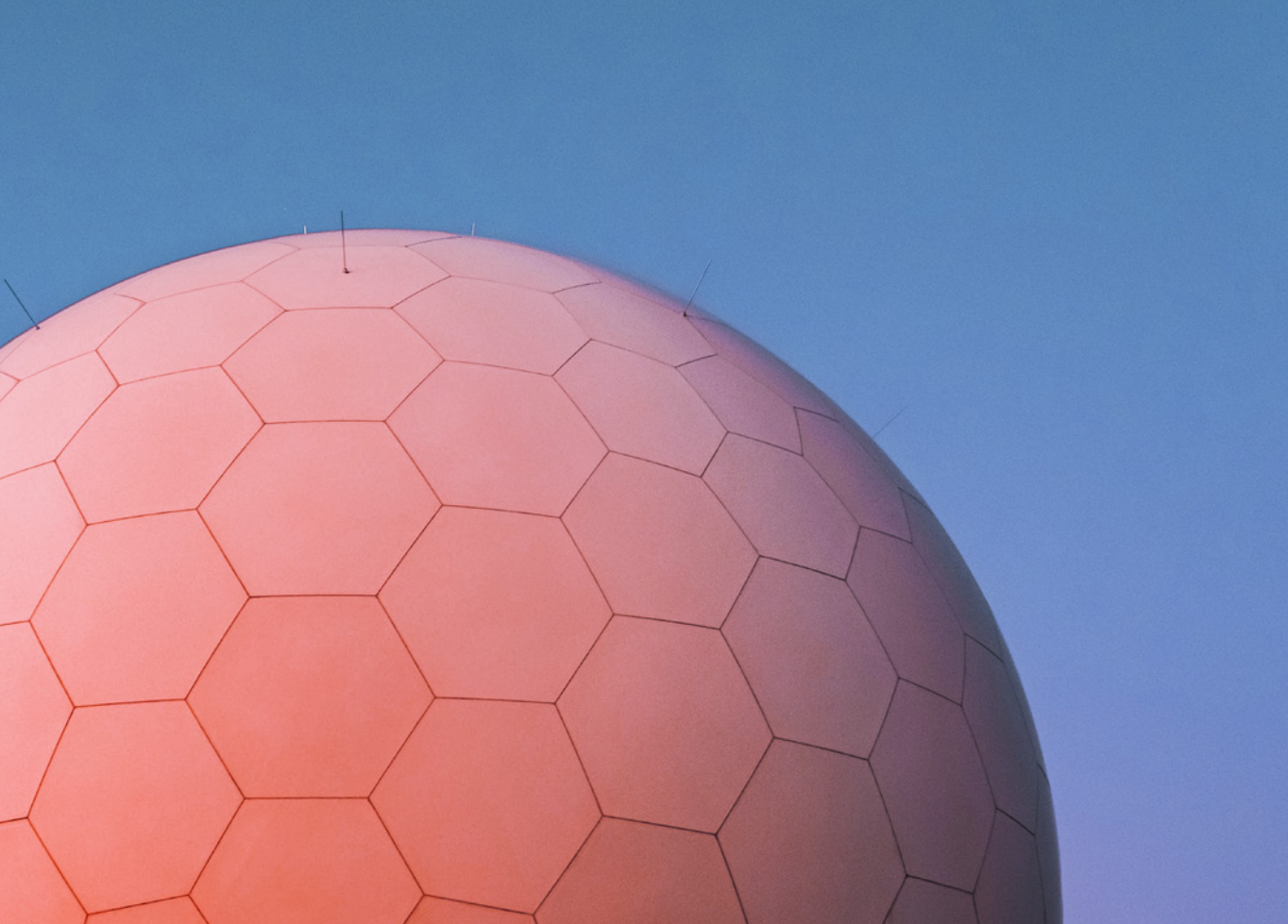
Da det russiske militær natten til den 24. februar 2022 indledte en invasion af Ukraine, var det kulminationen på lang tids oprustning, store troppebevægelser og klargøring til krig. Vestlige efterretningstjenester havde kort forinden vurderet, at der var en stor sandsynlighed for, at præsident Putin ville tage skridtet videre og gøre alvor af oprustningen og give sine generaler ordre til at begynde invasionen.

I FE blev Ruslands angreb den foreløbige kulmination på mange ugers intenst arbejde med at følge og forudsæ udviklingen i de russiske planer.



**ANJA DALGAARD-
NIELSEN**

Chef for Efterretning



"Der var naturligvis stor efterspørgsel på vores viden og vurderinger af situationen, og vi skulle arbejde hurtigere og tættere på vores kunder for at levere den nødvendige viden. Det var travlt og udfordrende, men også, til trods for de tragiske omstændigheder, meningsfyldt, fordi det blev meget nærværende og konkret, hvad FE arbejder for – nemlig at levere viden, som giver et solidt grundlag for danske myndigheders arbejde med at fremme sikkerhed og stabilitet i Europa og i Danmarks nærområde", forklarer Anja Dalgaard-Nielsen.

Langsigtet strategi og akut krisehåndtering

Den langstrakte krig i Ukraine har bl.a. betydet, at FE har skærpet sit fokus på truslen fra Rusland endnu mere, samtidig med at den sikkerhedspolitiske situation generelt i verden også er blevet mere kompleks.

"Vi har på den ene side skullet arbejde meget strategisk og langsigtet med Rusland og på den anden side skaffe viden om Ruslands militære kapaciteter nu og her. Det er et meget stort spænd, og det kræver meget af

os at kunne det hele. Når man har med store statslige aktører at gøre, er man efterretningsmæssigt oppe imod nogle sværere modstandere end for eksempel på terrorisme-rådet, som var det store fokus i en årrække. Nu skal vi kunne det hele på samme tid", siger Anja Dalgaard-Nielsen.

For at være et skridt foran udviklingen arbejder FE hele tiden strategisk med, hvilken teknologi og hvilke kapaciteter der er nødvendige for evnen til at imødegå trusler, leve op til kundebehov og følge med de teknologiske udfordringer. Det sker i et samspil med bl.a. PET og Forsvaret.

"På tværs af myndigheder, fagligheder og domæner rykker vi sammen i bussen. Det kræver situationen. Vi skal i dybden have viden om bl.a. Rusland og kunne gennemføre lange, tålmodige indsatser, men vi skal også kunne håndtere pludseligt opståede kriser på eksempelvis det afrikanske kontinent. Vi skal trække på den viden, vi kan skabe sammen", siger Anja Dalgaard-Nielsen.

Gamle discipliner og nye teknologier

Som såkaldt all source-efterretningstjeneste benytter FE sig af alle typer af indhentningsdiscipliner. Selv om teknologier som kunstig intelligens og machine learning er blevet afgørende for en moderne efterretningstjeneste, er der fortsat brug for menneskelig indhentning af efterretninger (HUMINT).

FE fik således en del opmærksomhed med et stillingsopslag i 2022, hvor der blev søgt efter nye føringsofficerer for at styrke FE's fysiske indhentning med menneskelige kilder.

"Vi fik i tusindvis af ansøgninger og har aldrig før haft så mange ansøgere til stillingen som føringsofficer eller til nogen anden stilling for den sags skyld. Vi vokser, fordi opgaverne vokser, og vi har brug for medarbejdere med forskellige baggrunde til vores efterretningsarbejde. Det gælder både den fysiske indhentning og også til vores mere tekniske stillinger, hvor vi forventer at skulle styrke vores hacker- og AI-kapacitet signifikant", siger Anja Dalgaard-Nielsen.

En af de hurtigst voksende discipliner er Open Source Intelligence (OSINT), hvor mere eller mindre åbent tilgængelige kilder bidrager til at tegne et samlet billede af situationen.

"Vi kommer også til at styrke vores Open Source-arbejde. Mængden af åbent tilgængelige data stiger eksponentielt, og OSINT kan være den billigste og mindst risikable vej til svar på nogle af vores efterretningsbehov. OSINT kan også supplere den viden, vi har fra andre indhentningskapaciteter. Vi er en all source-tjeneste. Når vi er bedst, vælger vi den billigste og mindst risikable vej til målet, og vi trækker på det hele, når situationen kræver det", fortæller Anja Dalgaard-Nielsen.

Samarbejde fremmer forståelsen

Ruslands krig i Ukraine har været med til at forstærke behovet for godt efterretningsarbejde. Samtidig har den understreget betydningen af et godt internationalt samarbejde – ikke bare på politisk og militært niveau, men også efterretningstjenester imellem.

"Vi kan selv meget, men vi kan ikke dække alt. Multilateralt bidrager vi til NATO og EU. Sammen med partnere, vi deler værdier med, udvikler vi fælles kapaciteter og arbejdsdeler. Som småstat i en stor verden er vi nødt til det. På samme måde som vi har et tæt samarbejde med PET om at afværge terrorangreb, spionage og andre trusler i Danmark. Vi lægger vægt på at dele den viden, vi kan," afslutter Anja Dalgaard-Nielsen.



Vi har på den ene side skullet arbejde meget strategisk og langsigtet med Rusland og på den anden side skaffe viden om Ruslands militære kapaciteter nu og her.

Anja Dalgaard-Nielsen

■ TRUSLER MOD DANMARK OG DANSKE INTERESSER

FE's indsats afspejler i høj grad de trusler og sikkerhedspolitiske udfordringer, Danmark står overfor. Ruslands fortsatte invasion af Ukraine er derfor naturligvis et stort fokusområde i FE, samtidig med at truslen fra cyberangreb fortsat er meget høj. Dertil kommer bl.a. terrortruslen, spændinger i Arktis og ustabilitet i Mellemøsten og Afrika.

■ RUSLAND

Rusland udgør en langvarig sikkerhedspolitisk trussel mod Vesten, uanset at Ruslands væbnede styrker sandsynligvis i en årrække vil være bundet i krigen i Ukraine. Rusland har med invasionen af Ukraine og i sin offentlige kommunikation gjort det klart, at landet ønsker at gennemtvinge en grundlæggende ændring af den sikkerhedspolitiske orden i Europa og modarbejde en regelbaseret verdensorden.

Rusland har fortsat en betydelig militær kapacitet i Arktis og Østersøregionen. Ruslands militære aktiviteter i Arktis vil sandsynligvis få en mere uforudsigelig karakter med en til tider truende adfærd. Dette vil i nogen udstrækning også kunne gøre sig gældende i Østersøregionen, hvor Rusland i lyset af NATO-udvidelsen ønsker at signalere militær styrke.

■ HYBRIDE MIDLER

Mange stater har evnen og viljen til at bruge hybride virkemidler for at opnå strategiske og udenrigspolitiske målsætninger. Hybride virkemidler omfatter en kombination af militære og ikke-militære virkemidler, der bidrager til at sløre både aktørerne og deres hensigter. Rusland bruger hybride midler mod vestlige lande med henblik på at underminere sammenhængskraft og sammenhold over for Rusland.

Rusland har en stor kapacitet til at gennemføre påvirkningsoperationer og andre destabiliserende aktiviteter såsom sabotage mod kritisk infrastruktur i vestlige lande, herunder trafikknudepunkter, energi, tele- og it-infrastruktur. Rusland bruger imidlertid ikke alle sine rådige hybride virkemidler i samme udstrækning. Sabotage og attentater er helt særlige og også risikofyldte aktiviteter for Rusland, hvorimod påvirkningsaktiviteter og offensiv og truende retorik er mere udbredt.

■ SPIONAGE

Spionagetruslen mod Danmark er fortsat aktuel og sammensat med bredt fokus på militære såvel som civile mål. Navnlige Rusland og Kina, som udgør de to mest alvorlige spionagetrusler mod Kongeriget Danmark, spionerer for at opnå viden om forsvars-, sikkerheds- og udenrigspolitik samt om dansk viden og teknologi. Særligt Rusland har desuden fokus på danske militære kapaciteter.

■ CYBERTRUSLEN

Danmark står over for en alvorlig cybertrussel fra både statslige- og ikke-statslige aktører. Statsstøttede hackere forbereder sig sandsynligvis, så de kan udføre destruktive cyberangreb, imens særligt de pro-russiske cyberaktivister og cyberkriminelle er aktive mod mål i Vesten og Danmark.

■ TERROR

Den største terrortrussel mod Danmark og danske interesser i udlandet kommer fortsat fra militante islamister, primært fra Islamisk Stat og al-Qaida. De to globale terrororganisationer har sandsynligvis ikke kapacitet til selv at udføre et større angreb i Europa, men opfordrer i deres propaganda jævnligt sympatisører til at udføre angreb. Islamisk Stat og al-Qaida har bl.a. flere gange i løbet af 2023 opfordret til hævnangreb for afbrændinger af koraner i Danmark og Sverige. Begge grupper udnytter endvidere konflikten mellem Israel og Hamas i deres propaganda. Herudover fører både Islamisk Stat og al-Qaida lokale oprørskampe mod magthavere og militære styrker i mange af verdens konfliktområder.

■ ARKTIS

Rusland vil fortsat forsøge at holde de sikkerhedspolitiske spændinger ude af Arktis, men Ruslands tilgang til regionen kan ændre sig i en mere konfrontatorisk retning. Kina ønsker at sikre sig større indflydelse på regionen og adgang til naturressourcer og sejl-ruter i Arktis. Kinas adgang til Arktis vil blive hjulpet af Ruslands isolation, som tvinger landet til at give Kina mere "plads" i Arktis for at sikre sig nødvendig støtte.

■ KINA

Relationen mellem Kina og USA vil på mange områder blive definerende for verdens udvikling. Kinas diplomatiske støtte og nære forhold til Rusland øger imidlertid modsætningerne mellem Kina og vestlige lande. Samtidig spidser situationen omkring Taiwan til, og Kina øger sin militære tilstedeværelse omkring øen, hvilket medfører risiko for eskalation. Kinas status som verdens største handelsnation giver landet stor indflydelse globalt. Kina bruger sin indflydelse til at ændre den etablerede regelbaserede verdensorden. I Kina strammer præsident Xi Jinping og kommunistpartiet grebet om myndigheder, civilsamfund og virksomheder, og den tiltagende autoritære linje vækker modstand i Vesten. Samtidig er Kina en uomgængelig aktør i håndteringen af globale problemer, herunder klimaforandringer.

■ REGIONALE KONFLIKTER, USTABILITET OG MIGRATION

Regionale konflikter, ustabilitet, klimaforandringer og dybe strukturelle problemer i Mellemøsten og Afrika skaber grobund for irregulære migrationsstrømme og stigende migrationspres på Europa. Regeringer i de lande, som EU gerne vil have til at begrænse tilstrømningen, vil søge at udnytte situationen til at lægge diplomatisk og politisk pres på Europa. Migrantstrømme er også et blandt flere hybride virkemidler.

■ PIRATERI

Regionale konflikter kan endvidere true sikkerheden for international skibsfart, herunder danske handelskibe. Pirateriet i Guineabugten fortsætter på lavt niveau med ganske få angreb på den kommercielle skibsfart. På trods af de få angreb har piraterne vist, at de er i stand til at angribe mål i stadig større afstand fra fastlandet.

Læs mere om truslerne mod Danmark og danske interesser i UDSYN, som er FE's årlige risikovurdering. Du kan finde UDSYN på fe-ddis.dk.



■ SÅDAN FÅR FE SIN VIDEN

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 værktøjer og metoder til rådighed, som vi kan benytte i vores informationsindhentning.

Efter FE-loven må FE for eksempel foretage masseindhentning af datakommunikation, så længe den ikke er rettet mod dansk data trafik. FE-loven indeholder bl.a. regler om, hvornår indhentning kræver retskendelse, og hvordan indhentet data skal behandles, herunder hvad det må bruges til, og hvornår det skal slettes. Tilsynet med Efterretningstjenesterne kontrollerer løbende FE's overholdelse af FE-loven.

FE arbejder med flere indhentningsdiscipliner:



SIGINT

SIGINT står for Signals Intelligence, som er elektronisk indhentning af dataoverførsler mellem computernetværk, telekommunikation osv. Den elektroniske indhentning sker for eksempel 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. FE indhenter via SIGINT store mængder data med udgangspunkt i FE-loven, der giver mulighed for at indhente data om forhold i udlandet. For at bringe de informationer i spil, der findes i disse data foretager FE søgninger i materialet. FE-loven regulerer, hvilke søgninger der må foretages. Søgningerne er underlagt løbende kontrol af Tilsynet med Efterretningstjenesterne.



CNE

CNE står for Computer Network Exploitation. 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.



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.



KRYPTO

Kryptoanalyse handler om at skaffe adgang til information, som er blevet forsøgt beskyttet med kryptering eller lignende metoder. I dag bliver data i stigende grad krypteret. Derfor er det ofte nødvendigt at kunne dekryptere trafikken, hvis den skal kunne bruges. Disciplinen handler derfor om at forstå og analysere protokoller og kryptosystemer ved at se på den underliggende kryptografi og softwaren omkring. Det er derfor både stærke IT-faglige kompetencer samt dyb matematisk forståelse der er fundamentet i disciplinen.



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.



IMINT

IMINT står for Imagery Intelligence og er en indhentningsdisciplin, hvor billeder, primært fra satellitter, fly og droner, analyseres for at udlede information af efterretningsmæssig værdi. IMINT er en delmængde af det samlede GEOINT-begreb.



OSINT

OSINT står for Open Source Intelligence, hvilket er indsamling af oplysninger fra åbne eller delvist åbne kilder, der typisk omfatter offentligt tilgængelig information fra f.eks. internettet, trykte medier, tv m.m. OSINT kan f.eks. omfatte monitorering af medier eller sociale medier og dybdegående undersøgelser af bestemte aktører eller enheder. Oplysninger skaffet gennem OSINT kan for eksempel bidrage til opbygning af efterretningsbilleder, understøtte SIGINT'en og danne grundlag for CNE- eller HUMINT-operationer.

”EN HVERDAG TÆT PÅ KRIGEN”



For at beskytte vores medarbejderes identitet, optræder de her under et alias

Krigen i Ukraine har fyldt i verden, i medierne og i FE de seneste to år. Mød Martin, som er en af de medarbejdere, der i sit arbejde har krigen helt tæt på. Han holder sammen med sit team øje med de russiske landmilitære styrker i Ukraine, Belarus og Rusland.

Hvad er din baggrund?

Jeg har været ansat i Forsvaret siden midt 90'erne og har primært gjort tjeneste i hæren og været udsendt til adskillige brændpunkter rundt omkring i verden. Jeg blev kontaktet af en tidligere kollega, som var overbevist om, at jeg kunne skabe merværdi i FE, hvis jeg var interesseret i at lægge uniformen. Efter mange år med udsendelser og lange perioder væk fra familien, samt mulighed for at arbejde et spændende sted som FE, krævede det ikke mange overvejelser at søge, og heldigvis fik jeg jobbet.

Hvordan har din tid i FE været?

Jeg blev ansat for ca. ti år siden som analytiker. Arbejdsopgaverne er grundlæggende de samme i dag, som da jeg startede, men verden og sikkerhedssituationen har ændret sig, og arbejdspresset er naturligvis højere i dag end før Ruslands invasion af Ukraine.

Som arbejdsplads er FE fyldt med alle typer af mennesker og personligheder. Men fælles for alle mine kollegaer er, at de har samme mindset med fokus på opgaven.

Hvad består dit arbejde af?

Min primære opgave som analytiker er at udarbejde militære analyser og faglige vurderinger, og at yde rådgivning om aktuelle og fremtidige militære trusler mod Danmark og rigsfællesskabet.

Det kræver bl.a. stor viden om Ruslands væbnede styrkers militære kapaciteter, militære doktriner, organisation og teknologier. De analytiske opgaver er meget forskellige og varierer også i forhold til tidsmæssigt sigte. Nogle opgaver bidrager til langsigtede strategiske analyser, andre understøtter kortsigtede, konkrete behov hos modtagere af FE's efterretningsprodukter.

Hvordan var det at arbejde i din stilling, da Rusland gjorde klar til at invadere Ukraine?

I den sidste tid op til invasionen og i det første lange stykke tid efter havde jeg ikke mange fridage. Min afdeling er heldigvis kommet igennem de fleste strabadser med skindet på næsen, men det har været hårdt i perioder. Det har været en særlig oplevelse at være en del af, og den viden, som jeg havde tilegnet mig over årene, har været med til at underbygge FE's vurderinger krigen igennem.

Hvordan er det ikke at kunne fortælle om sit arbejde til venner og familie?

Det er helt klart en udfordring i sociale sammenhænge ikke at kunne fortælle om mit arbejde. Jeg har dog fundet ud af, at hvis man selv er meget spørgende, så kan man nemt dreje samtalen over på andres job eller et andet emne. Min familie og mine venner ved godt, hvor jeg arbejder, men de ved ikke, hvad jeg laver. Derudover ved de også godt, at jeg ikke kan tale om mit arbejde.



Min primære opgave som analytiker er at udarbejde militære analyser, faglige vurderinger og yde rådgivning om aktuelle og fremtidige militære trusler.

FE'S KONTRA- SPIONAGE I DANMARK ER IGEN BLEVET HØJAKTUEL

Som militær sikkerhedstjeneste i Danmark er det bl.a. FE's opgave at beskytte Forsvaret og vores allierede mod spionage og andre trusler under ophold i Danmark. Det er en opgave der igen er blevet højaktuel i forbindelse med krigen i Ukraine. Ikke mindst når vi modtager og hjælper allierede med at komme sikkert igennem Danmark.

April 2022. Ud af morgentågen anløber det 264 meter lange fragtskib ARC Endurance Esbjerg Havn. Lastrummet er fyldt med militært udstyr fra den amerikanske hær. 44 helikoptere og over 300 pansrede køretøjer er blandt det udstyr, som nu skal transporteres fra Esbjerg videre til en planlagt NATO-militærøvelse i Polen.

Danmark er blevet anmodet om støtte til at sikre indskibningen af det amerikanske materiel til Europa. En opgave, der også er kendt som Host Nation Support (HNS), som er en betegnelse for den logistiske støtte, Danmark yder som værtsland, når allierede styrker og

deres materiel ankommer til Danmark for eventuelt at blive transporteret videre til en slutdestination i Danmarks nærområde.

Mistænkelig adfærd og nysgerrige turister

For FE lyder opgaven at beskytte den militære kortege mod spionage. Det er en opgave, der løses i samarbejde med Forsvaret og andre myndigheder. Kontraetterrettingsarbejdet er en del af FE's opgave som militær sikkerhedstjeneste i Danmark. FE leder og kontrollerer den militære sikkerhedstjeneste og er national sikkerhedsmyndighed inden for Forsvarsministeriets ressortområde.



Det er FE, der har myndighedsopgaven og mandatet, når det drejer sig om Forsvarets og allieredes sikkerhed på dansk jord.

FE'S OPGAVER PÅ DANSK JORD

FE er Danmarks udenrigs- og militære efterretningstjeneste rettet mod forhold i udlandet jf. FE-loven.

Men FE leder og kontrollerer også den militære sikkerhedstjeneste og er national sikkerhedsmyndighed inden for Forsvarsministeriets ressortområde. Det vil sige, at det er FE, der har myndighedsopgaven og mandatet, når det drejer sig om Forsvarets sikkerhed – også på dansk jord. Det sker ofte i samarbejde med andre myndigheder som PET, politiet, Forsvaret og Hjemmeværnet.

Det vil sige, at det er FE, der har myndighedsopgaven og mandatet, når det drejer sig om Forsvarets og allieredes sikkerhed på dansk jord. Mistænkelig adfærd i forbindelse med konkrete opgaver som den i Esbjerg bliver meldt ind til FE, der undersøger den nærmere.

Det kan for eksempel være udenlandske lejebiler med mistænkelig adfærd, nærgående droneflyvning eller lidt for nysgerrige turister, der filmer kortegen fra en motorvejsbro. Ofte er der naturlige og uskyldige forklaringer, men i en tid med krig i Europa har Danmarks modstandere interesse i eller et decideret efterretningsbehov for at vide, hvordan Danmark yder Host Nation Support, og hvilke NATO-kapaciteter der flyttes rundt i Europa.

Eksempelvis blev et udenlandsk køretøj flere gange observeret omkring et militært område, som var oprettet i forbindelse med en HNS-opgave. Personerne i køretøjet blev set fotografere og observere amerikansk militært materiel på området.

FE registrerede køretøjet og kunne konstatere, at det var kommet til Danmark tidligt om morgenen og forlod Danmark igen allerede samme dag inden frokost. Personerne i køretøjet var sandsynligvis kun rejst til Danmark – kortvarigt – for at se på amerikansk militært

materiel i et par timer. Disse oplysninger indgår i FE's videre arbejde med at afdække spionage mod Danmark og vores allierede.

Ukraine-krigen og styrket støtte til Forsvaret

Krigen i Ukraine har skærpet betydningen af FE's rolle i forbindelse med Host Nation Support. For hvis situationen mellem Vesten og Rusland eskalerer til en krigslignende tilstand, vil Rusland have en interesse i at forstyrre eller sabotere transporten af allierede styrker og deres materiel til frontlinjen.

Med den aktuelle situation forventes behovet for HNS-aktiviteter i Danmark at stige yderligere. Derfor er der allerede nu et øget behov for FE's kontraetterretningsstøtte.

Det er FE's opgave at varsle Forsvaret om de trusler, der kan forstyrre eller forhindre Forsvarets opgaveløsning. Det gælder både i Danmark, og når Forsvaret er på missioner i udlandet. Med et forværret og mere komplekst trusselsbillede er opgaven for FE også vokset. Det gælder ikke mindst den teknologiske udvikling, som har gjort truslen fra spionage og cyberspionage mod Forsvaret større, samtidig med at den også giver FE nye muligheder i arbejdet med kontrapionage.

Det militære udstyr om bord på ARC Endurance nåede sikkert frem til destinationen i Polen takket være et godt samarbejde mellem myndighederne i Danmark og partnere i udlandet.

EKSEMPLER PÅ FE'S STØTTE TIL FORSVARET

- Forebyggende indsatser i form af awareness og rådgivning om konkrete spionagetrusler mod Forsvaret
- Varsel om interne og eksterne trusler i Forsvaret
- Understøttelse af Forsvaret i udlandet mod fjendtlige trusler
- Offensive og defensive militære cyberoperationer til støtte for Forsvaret



■ FE HJALP DANSKE SOLDATER I MALI PÅ 4.000 KILOMETERS AFSTAND

To gange har FE hjulpet Forsvaret med at bekæmpe terrorister i Mali. Dette er fortællingen om den seneste, om et stærkt samarbejde med Forsvaret, om kreativ brug af FE's særlige kompetencer og om cyberspace som kampplads.

Langt fra den fysiske kampplads sidder et af FE's operative team på en lokalitet i Danmark. I måneder har teamet minutøst planlagt, hvordan truslen fra terrorister kan bekæmpes til støtte for det danske forsvar i Mali.

Året er 2021, og Danmark er en del af Operation Barkhane, den fransklede internationale indsats mod terrorisme i Sahel-regionen. Det danske forsvar bidrager med specialstyrker og har anmodet FE om hjælp til at imødegå trusler, som udspringer i eller gennem cyberspace. FE's offensive cyberstøtte er blevet godkendt af Folketinget, så FE kan indgå selvstændigt eller til støtte for den danske militære indsats med formålet at imødegå terrorgruppernes evne til at forberede, understøtte og gennemføre terroroperationer.

Chefen for FE's operative team fortæller:

"Hvor specialstyrkerne var folkene på jorden, var vi øjet i skyen. FE's bidrag til operationen gik i hovedtræk ud på at bekæmpe terroristerne i cyberspace og forringe deres mulighed for at operere og angribe danske soldater eller koalitionsstyrker. Cyberspace giver nye muligheder for at bekæmpe trusler og støtte Forsvarets opgaveløsning – også selv om vi befinder os tusindvis af kilometer væk fra den fysiske kampplads. Vi er i berøring med modstanderen på nye måder og hele tiden, hvilket kræver tæt integration mellem de operative og analytiske behov – og et tæt samarbejde med Forsvaret".

FE har særlige kompetencer

Operationer i cyberspace, hvor det handler om at ramme en modstander, kræver stor nøjagtighed, grundig forberedelse og hemmeligholdelse med henblik på at understøtte operationens formål og støtte Forsvarets udsendte bidrag bedst muligt. Derfor er FE's operative teams sammensat af medarbejdere med forskellige faglige kompetencer for at sikre, at alle dele af operationen bliver gennemført præcist, effektivt og forsvarligt, således at FE's cyberangreb rammer dem, de er tiltænkt, og ikke går ud over andre. Det handler bl.a. om at kunne analysere enorme mængder data, som skal bruges i realtid og har betydning for soldaternes indsats på landjorden.

OPERATION BARKHANE

Den fransklede Operation Barkhane har til formål at bekæmpe terrorisme i Sahelregionen i Afrika og var tidligere massivt til stede i Mali.

I 2019-2020 bidrog Danmark med helikopterstøtte til Operation Barkhane, mens Folketinget i maj 2021 besluttede at udsende nye militære bidrag til den europæiske specialoperationsstyrke Task Force Takuba i Mali. Bidraget blev deployeret efter invitation fra Malis regering, men måtte hjemtages igen kort efter på grund af nye udmeldinger fra det maliske overgangsstyre.



Men det handler også om at udvikle operative og gennemtestede løsninger, som giver værdi for Forsvaret og Danmarks sikkerhed. Endelig er der behov for en høj grad af hemmeligholdelse, så modstanderen ikke kan få kendskab til FE's metoder og kapaciteter. Her har FE særlige kompetencer, som også under Operation Barkhane viste sig afgørende for succes.

Operationen ændrer karakter

Kort efter at de danske styrker ankommer til Mali for anden gang, beslutter militærregimet, at Danmark ikke er velkommen. Det er en fredag eftermiddag i januar 2022. Og operationen, som FE gennem måneder har forberedt, ændrer hurtigt karakter. Nu venter et intenst døgn med minutiøs planlægning for at få de danske specialstyrker sikkert hjem til Danmark.

"Heldigvis fik vi lynhurtigt lagt en ny plan med Forsvaret og justeret vores operative aktiviteter. Det gjorde, at vi også kunne støtte Forsvaret i hjemtagelsen af de danske soldater" forklarer en af medarbejderne, der var med til indsatsen.

Indsatsen i Operation Barkhane viste, at vi er kommet langt med at integrere Forsvarets og FE's aktiviteter i både den fysiske verden og i cyberspace til gavn for dansk sikkerhed. Det er vigtige erfaringer, som vi kan bruge i fremtidige operationer. Endelig understregede Operation Barkhane, at FE sikkert, effektivt og troværdigt kan operere i og gennem en central del af fremtidens kampplads – nemlig cyberspace.



Cyberspace giver nye muligheder for at bekæmpe trusler og støtte Forsvarets opgaveløsning – også selvom vi befinder os tusindvis af kilometer væk fra den fysiske kampplads.

”JEG FINDER NÅLEN I HØSTAKKEN”



For at beskytte vores medarbejderes identitet, optræder de her under et alias

På lang afstand af krig og konflikt kan FE støtte Forsvarets udsendte soldater på landjorden med effektive cyberindsatser. Mød en af de medarbejdere i FE, der med analyser af store datamængder gør det muligt.

Hvad er din baggrund og hvordan endte du i FE?

Jeg blev uddannet ingeniør fra DTU for en håndfuld år siden og fik efter studiet arbejde i en privat virksomhed, men efter noget tid gik det op for mig, at mit arbejde grundlæggende bestod i at hjælpe store virksomheder med at tjene flere penge. Jeg ville gerne arbejde et sted, hvor jeg følte, at jeg gjorde en reel forskel, så da en god ven, der arbejdede i FE, viste mig stillingsopslaget som dataanalytiker, søgte jeg jobbet. Det er fedt at være kommet ind i en operativ afdeling, hvor det er tydeligt for mig, at jeg bruger min tid og energi på noget vigtigt, som gør en forskel ude i den virkelige verden.

Hvad består dit arbejde i?

Som dataanalytiker er det min opgave at finde sammenhænge i de store komplekse datamængder, som man ikke kan gennemskue med det blotte øje. Det gør jeg ved at bearbejde, analysere og visualisere data på baggrund af de informationer, vi henter ind i forbindelse med vores operationer. Jeg bidrager dermed til at finde ”nålen i høstakken” til gavn for mine kollegaer, FE’s ledelse og ikke mindst vores kunder.

Hvordan ser en typisk arbejdsdag ud som dataanalytiker i FE?

Der er dage, hvor jeg har hovedet dybt begravet i data, fordi et komplekst problem skal løses, og så er der dage, hvor jeg nærmest ikke sidder på min plads, fordi jeg samarbejder med kollegaer på tværs af FE. Jeg arbejder ikke kun med data, men er også med til at udvikle operative muligheder. Jeg synes, at det er en stor styrke i afdelingen, at alle får rum til at bidrage på tværs af de projekter, de har interesse for, så man over tid bygger en masse forskellige kompetencer og erfaringer op.

Hvornår kan du mærke, at dit arbejde gør en forskel?

Når vores kunder giver feedback og udtrykker stor tilfredshed med vores indsats, kan jeg mærke, at vi gør en forskel. Det er selvfølgelig en begrænset gruppe,

som har stor indsigt i, hvad vi laver, og derfor er vi også gode til internt i afdelingen at fejre sejrene, og markere, når vi har lavet et godt stykke arbejde.

Ved din familie og venner godt, hvor du arbejder, og hvad du laver?

Min nærmeste familie ved godt, at jeg arbejder i FE. Det har jeg besluttet, fordi det gør det nemmere at forklare, hvorfor der er spørgsmål, jeg ikke kan svare på. De ved dog ikke, hvad jeg laver, ud over at jeg er ansat som dataanalytiker. I nogle sociale sammenhænge kan det være underligt ikke at kunne tale om mit arbejde, men min familie kender jo omstændighederne og er gode til at spørge mere generelt frem for at spørge ind til specifikke opgaver.

Hvordan er det at sidde ved en computer, mens dit arbejde har direkte effekt på ”slagmarken”?

Det er afgørende for en effektiv og forsvarlig opgaveløsning, at vi ikke lader os afkoble fra den virkelighed, vi sidder med, og at vi kender målområdet og modstanderen indgående. Vi taler også meget om, at det, vi gør, har betydning og påvirker noget eller nogen ude i verden. Vi er der for hinanden og er gode til løbende at vende situationen.

Hvad skal man kunne for at få job i din afdeling?

Vi er en afdeling med meget forskellige faglige kompetencer, og vi er stærke på grund af vores tværfaglighed og villighed til at lære fra os og af hinanden. Det er i højere grad ens indstilling og analytiske evner, der spiller ind. Man skal kunne tænke operativt. Men det er selvfølgelig en fordel at have interesse for moderne informations- og kommunikationsteknologier eller programmering. Det vigtigste er, at man er nysgerrig og i stand til og har lyst til at fordybe sig i nye og ukendte områder.



Det, vi gør, har betydning og påvirker noget eller nogen ude i verden.

TEKNOLOGI ER DRIVKRAFT FOR FORANDRING I FE

Den teknologiske udvikling går ekstremt hurtigt, og FE skal som efterretningstjeneste ikke blot følge med udviklingen, men også gerne være flere skridt foran. Derfor har vi et konstant fokus på at udvikle og anvende nye teknologier og tiltrække medarbejdere med de rette kompetencer.

Trusler mod Danmark og danske interesser kommer i mange forskellige former og størrelser. For FE er det en kerneopgave at have kendskab til truslerne og ikke mindst evnen til at imødegå dem. For at løse opgaverne skal FE være blandt landets førende inden for udvikling og anvendelse af ny teknologi, fortæller Carmine Gioia, der som chef for FE's Innovation og Teknologier er ansvarlig for at integrere de nyeste teknologier i FE.

"FE er en højteknologisk organisation og arbejdsplads, og vores fremtidige opgaveløsning afhænger i høj grad af, hvordan vi formår at anvende nye teknologier. Derfor har vi etableret et innovationsmiljø, som skal udvikle avancerede løsninger til brug i hele FE. Ambitionen er, at avanceret teknologi skal være fundamentet for hele vore forretningsmodel og gøre os dygtigere og mere effektive til at indhente, analysere og formidle information til offentligheden og til vores kunder. Det har potentiale til at give os et helt afgørende forspring i kampen mod dem, der på den ene eller anden måde ønsker at ramme Danmark eller danske interesser", siger han.

FE indhenter og bearbejder alle typer af information. Det kræver, at den teknologiske udvikling i FE spænder bredt og implementeres i alt fra signal-indhentning, cybersikkerhed og kryptografi over kvantecomputere, kunstig intelligens og machine learning til supercomputere.

CARMINE GIOIA

Chef for Innovation
og Teknologier



SAMARBEJDE MED DTU

I juni 2023 indgik FE en aftale med DTU om et teknologisamarbejde.

Med aftalen ønsker FE at gøre større brug af de førende forskningsmiljøer i Danmark til at løse opgaver, der er med til at holde Danmark sikkert.

Aftalen betyder, at der sættes gang i et samarbejde om bl.a. at udvikle konkrete forskningsprojekter af strategisk vigtighed for FE.

Det er første gang, at FE på denne måde gør direkte brug af forskningsmiljøet i Danmark til at løse konkrete opgaver.

"Når alle disse discipliner og systemer kombineres på en sikker og compliant måde, bidrager det i høj grad til Danmarks sikkerhed. Som ansat i FE keder man sig aldrig, for kravene til, at vi udvikler os og forbliver konkurrencedygtige, er høje. Det er derfor, at vi i de her år tilfører betydelige ressourcer til vores arbejde med at forstå og anvende ny teknologi. Det er også baggrunden for, at vi som noget nyt begynder at indgå strategiske samarbejder med blandt andet større virksomheder og universiteter. For det er utænkeligt, at vi kan udvikle al den nødvendige teknologi alene," siger Carmine Gioia.

Behov for tech-talenter

Når man har en ambition om at være blandt de førende arbejdspladser i Danmark inden for de nyeste teknologier, medfører det en naturlig tiltrækningskraft på innovative og nysgerrige medarbejdere med højt specialiserede kompetencer. Det samme gælder samarbejdet med aktører uden for FE, mener Carmine Gioia.

"Jeg er sikker på, at det bliver nemmere at rekruttere, når vi styrker vores samarbejde med både offentlige og private virksomheder. I FE har vi generelt virkelig spændende opgaver, som giver mening i et bredere samfundsperspektiv. For at være relevant for de dygtigste tech-talenter skal vi derudover også være med helt fremme i den teknologiske udvikling, så vi kan tilbyde de stærkeste specialister de udfordringer og muligheder, de efterspørger, og som de i øvrigt ikke finder andre steder. Her er både vores samarbejder med partnertjenester i andre lande og med de dygtigste forskningsmiljøer i Danmark helt centrale".

FE har senest indgået et forskningssamarbejde med DTU – Danmarks Tekniske Universitet – om at udvikle nye kapaciteter af strategisk vigtighed for FE's arbejde. Hovedformålet med aftalen er at levere innovation, som kan anvendes direkte i FE's opgaveløsning, men aftalen forventes også at vække interesse i teknologimiljøet og kunne tiltrække forskere og andre eksperter med særlige kompetencer inden for eksempelvis kunstig intelligens og kvanteteknologi.

EKSEMPLER PÅ NYE TEKNOLOGIER

- **AI/ML**
Kunstig intelligens har i mange år været et fokusområde for FEDer er særligt fokus på Computer Vision, Graph AI og Natural Language Processing (NLP). AI-produktionssystemer er en helt afgørende komponent i en moderne efterretningstjeneste, når der skal identificeres komplekse mønstre i data.
- **Zero Trust-sikkerhedsarkitektur**
Med termer som least privilege, need to know, automatisering og konfigurationskontrol er FE i gang med en transition mod Zero Trust, som er et paradigme inden for sikkerhedsarkitektur, hvor alle komponenter i arkitekturen løbende skal verificere og kontrollere adgang. Arkitekturen er nødvendig for at sikre, at FE også i fremtiden er godt rustet mod trusler fra udenlandske hackergrupper.
- **Big data-streaming**
Når det er vigtigt at store datamængder er tilgængeligt hurtigt, anvendes big data-streaming til at flytte og berige data. Det er teknologier der sikrer at meget store og meget svingende datamængder kan behandles på en driftssikker måde. Til det bruger FE bl.a. avancerede teknologier, der løbende skaleres til de datamængder, FE arbejder med.
- **Kvanteteknologi**
Kvanteteknologi er fortsat et område, FE følger tæt på forskningsniveau. Både kvantekryptering, kvantesensorer og kvantecomputere er af interesse for FE's operative evner. Samtidig følger vi løbende med i udviklingen ude i verden, så vi på bedst mulig måde kan rådgive om og arbejde med kvantegennembrud.
- **AI Center of Excellence**
FE bruger AI til at accelerere vigtige arbejdsgange. Det handler især om at uddrage relevant viden om aktører og deres aktiviteter og hensigter fra de særdeles forskelligartede og mangfoldige data, som indhentes. FE har oprettet et internt "AI Center of Excellence" for at garantere fokus på AI-løsninger, som har bred og langvarig effekt på tværs af datakilder og efterretningsområder.

DATA- OG IT-STILLINGER I FE

FE er en højteknologisk arbejdsplads, hvor der er brug for mange forskellige typer af medarbejdere med specialviden inden for bl.a. it og data. Her på siden finder du et udpluk af stillinger, der findes og er brug for i FE.

IT-SIKKERHEDSTEKNIKER

I jobbet har man en sikkerhedsteknisk funktion, hvor man bl.a. udfører scanninger, stiller krav til IT-sikkerhedskomponenter og hjælper med at implementere og vedligeholde dem. Man rådgiver og sikrer, at FE's it-systemer er på højeste mulige sikkerhedsniveau ud fra gældende bestemmelser og procedurer.

IT-SUPPORTER/HARDWARE MANAGEMENT

Ligesom på de fleste andre større arbejdspladser er der også i FE brug for dygtige it-supportere. Hos os indebærer det bl.a. installation og montering af udstyr i vores datacentre, opbygning af sikre driftsmiljøer samt installation og vedligeholdelse af sensorer hos vores kunder.

SOFTWAREUDVIKLER/DEVOPS-SPECIALIST

Som IT-udvikler kan det f.eks. være din opgave at være bindeled til udviklingshold og sikre en god overgang mellem udvikling og drift. Du vil arbejde med at optimere det containerbaserede systemlandskab og være med til at identificere automatiseringsmuligheder.

INFRASTRUKTUR- OG TEKNOLOGISPECIALISTER

Du er med til at automatisere og forbedre FE's I&O-services og implementere koncepter som Infrastructure as a Service (IaaS), Infrastructure as Code (IaC) samt Platform as a Service (PaaS). Det er en stilling, hvor du støtter FE's DevOps, udviklere og kritiske it-systemlandskab.

IT-ARKITEKTER

Hvad enten du ansættes som enterprisearkitekt, der tegner de store linjer i målarkitekturen, eller som sikkerheds-, teknologi-, applikations-, data- eller forretningsarkitekt, der fortæller hvilke løsningsmodeller, der må anvendes, eller løsningsarkitekt, får du en vigtig rolle for at skabe gode platforme og landskaber i FE's it-systemer.

NETVÆRKSKOMMUNIKATION OG TELEINFRASTRUKTUR

Her får du berøring med FE's indhentningsarbejde, når du er med til at overvåge og analysere vores SIGINT-systemer. Her får du mulighed for at arbejde med FE's netværksinfrastruktur, der understøtter FE's behov for et robust og skalerbart netværk.

AI ENGINEER

Her er du med til at udvikle, teste og implementere kunstig intelligens i FE ved bl.a. at udvikle, deployere og eksekvere modeller. Du arbejder baseret på MLOps principper med registrering af træningsdata, modeller og resultater, og med at sikre performance og validitet af AI i produktion.

BIG DATA ENGINEER

I denne stilling udvikler og driver du big data framework og data-modellen. Du sikrer validitet og performance af data pipelines som f.eks. streaming- og batch-jobs. Big data engineeren er essentiel i at sikre, at FE's data er klar til AI og kan bruges til at besvare kritiske efterretnings spørgsmål fra FE-analytikere.

DATAARKITEKT

Som dataarkitekt er du med til at designe og planlægge arkitekturen og brugen af teknologier inden for big data og datatransformation. Du samarbejder med andre arkitekter for at sikre en sammenhængende og effektiv dataarkitektur i FE.

IT SERVICE MANAGEMENT (ITSM)

I jobbet skal man arbejde med en række discipliner inden for forvaltning og styring af it-serviceydelser. Herunder identifikation af systemer, applikationer, services og elementer i lagdelingen af FE's teknologilandskab.

DATA SCIENTIST

Som data scientist har du bl.a. fokus på machine learning og dataprocessering, og du hjælper FE's analytikere med at håndtere store komplicerede datamængder, der bliver en stadig vigtigere del af efterretningsarbejdet.

DATA ENGINEER

Data engineers er i FE med til at tilrettelægge og ordne data i systemer, så data er let tilgængeligt og bearbejdeligt. Data engineeren sørger for at produktionssystemerne skaleres til de store datamængder, FE arbejder med.

Hold øje med nye jobopslag på fe-ddis.dk og på FE og CFCS's LinkedIn-sider.



For at beskytte vores medarbejderes identitet, optræder de her under et alias

”JEG BYGGER VÆRKTØJ
MED KUNSTIG
INTELLIGENS TIL MINE
KOLLEGAER”

I en højteknologisk organisation som FE er der hele tiden brug for nye værktøjer og metoder til at være et skridt foran. Mød en af dem, der er med til at holde FE forrest i det teknologiske kapløb.

Hvad er din baggrund?

Jeg er ph.d. inden for det samfundsvidenskabelige område og har gennem en årrække været ansat ved både danske og udenlandske universiteter, hvor jeg har forsket i emner inden for bl.a. samfundsvidenskab med fokus på anvendt statistik. Arbejdet med anvendt statistik ledte mig naturligt i retning af data science, der er et område, hvor der kan bruges værktøjer fra både statistik og samfundsvidenskab.

Kendte du noget til FE, og hvordan fandt du på at søge ind?

Inden jeg startede i FE, havde jeg kun et vagt indtryk af, hvad det vil sige at arbejde i en efterretningstjeneste. Af samme årsag havde jeg ikke troet, at det var et sted, hvor der var brug for mig og mine evner. Men jeg var blevet en smule træt af universitetet og ledte efter nye udfordringer, så da en bekendt nævnte, at der var et job ledigt i FE som metadata-analytiker, blev jeg nysgerrig og endte med at søge ind.

Hvad er kernen i dit arbejde?

Hvis man forestiller sig, at data er en stor planet udelukkende bestående af høstakke, og vi er interesseret i at finde en nål, så er min opgave at bygge det

værktøj, der hjælper analytikerne med at finde den rigtige høstak. Disse værktøjer kan være baseret på AI eller mere traditionelle søgemetoder. Så mit arbejde handler om at hjælpe FE's analytikere med at få det optimale ud af den komplicerede, kæmpemæssige og forskelligartede datamængde, der indsamles. Det betyder, at jeg bruger mine kompetencer inden for statistik, programmering, datahåndtering, machine learning og dataprocessering, når jeg går på arbejde.

Hvordan ser en typisk arbejdsdag ud for dig?

Når jeg kommer ind, læser jeg typisk først op på e-mails. Derefter begynder jeg enten at skrive kode til vores værktøjer, eller mødes med vores analytikere for at finde ud af, hvad FE's kunder har brug for at få svar på lige nu. Ofte er det meget aktuelle emner, vi hjælper med. Det er nu og her, det sker. Det er noget af det, der er med til at gøre arbejdet relevant og spændende.

Er det udfordrende at arbejde i FE og samtidig have et familieliv?

Det kan være en udfordring, at man ikke kan fortælle, hvad man laver, da meget af ens identitet ofte ligger i ens job. Men man finder en balance, hvor man fortæller en overordnet og nogenlunde retvisende version af sit arbejde. Til gengæld har man fri, når man har fri.

Anerkendelse og sparring får man fra sine kollegaer. Folk skal jo bruge det, jeg udvikler, så man får meget respons. Og det er da fedt at dem, der skal rapportere til beslutningstagerne kan lave bedre og mere kvalificerede rapporter, på grund af de værktøjer, som jeg bygger.



Hvis man forestiller sig, at data er en stor planet udelukkende bestående af høstakke, og vi er interesseret i at finde en nål, så er min opgave at bygge det værktøj, der hjælper analytikerne med at finde den rigtige høstak.

■ VI BESKYTTER DEN KRITISKE INFRASTRUKTUR MOD CYBERANGREB

Center for Cybersikkerhed har til opgave at understøtte robustheden mod cyberangreb i den danske kritiske infrastruktur. Her fortæller chef for Center for Cybersikkerhed, Thomas Flarup, om, hvordan den vigtige opgave sætter sit præg på medarbejderne og samarbejdskulturen i centeret.

"Hvis de seneste år har lært os noget, så er det, at cybertruslen er alvorlig og et grundvilkår for alle virksomheder, store som små", siger Thomas Flarup, der i maj 2022 satte sig i spidsen for indsatsen for at beskytte Danmark mod cyberangreb, da han tiltrådte som chef for Center for Cybersikkerhed.

Cyberkriminelle netværk og statsstøttede hackere er i dag ressourcestærke aktører, som løbende udvikler deres kapaciteter. Begge typer af hackere er hurtige til at udnytte nye sårbarheder og angrebsvinkler og finde nye måder at hacke på. Samtidig må det forventes, at konsekvenserne af cyberangreb vil blive alvorligere i fremtiden, i takt med at vores samfund bliver stadig mere digitaliseret.

THOMAS FLARUP

Chef for Center
for Cybersikkerhed



"Ransomware-angreb udstiller i de her år skyggesiden af, at den fysiske og digitale verden i stadig større grad smelter sammen. Stort set alle dele af vores samfund er afhængige af digitale services og systemer, og det kan blive virkelig alvorligt, når digitale services bliver afbrudt og taget som gidsel af cyberkriminelle," fortæller Thomas Flarup.

Cyberspionage bliver oftest udført af stater med betydelige ressourcer og evner. Staterne anvender deres ressourcer målrettet for at få adgang til sensitiv og værdifuld viden, som danske myndigheder og virksomheder ønsker at beskytte. Men det stopper ikke der, advarer Thomas Flarup:

"FE vurderer, at cyberspionage også kan blive brugt til at forberede destruktive cyberangreb. Hackere, der har tiltvunget sig adgang til et offers netværk for at udføre cyberspionage, kan for eksempel senere misbruge denne adgang til at slette alle offerets data ved hjælp af såkaldt wiper-malware, som vi så flere gange i Ukraine i løbet af 2022."

Nye teknologier bliver en gamechanger

Kigger vi lidt fremad, er nye teknologier i hastig fremmarch. Avancerede chatbotter og andre generative AI-modeller bliver stadig mere kompetente og i stand til at efterligne menneskelig intelligens i et tempo, som få havde troet muligt. Teknologien har potentiale til at revolutionere vores samfund, men der tegner sig også en række udfordringer i forbindelse med cybersikkerhed. Potentialet for misbrug begået af ondsindede aktører gør, at udviklingen af chatbotter er et område, som det er væsentligt for CFCS at følge med i.

"Det er stadig early days, men der er ingen tvivl om, at AI og kvanteteknologi bliver en gamechanger på cybersikkerhedsområdet", understreger Thomas Flarup. På kort sigt fremhæver han bl.a. risikoen for at forstærke allerede eksisterende udfordringer, for eksempel phishing-mails, som AI chatbots kan producere utroligt effektivt.

Faglighed og fællesskab

På det bagtæppe er det CFCS' opgave at understøtte robusthed mod cyberangreb i den kritiske infrastruktur. Det betyder konkret, at centeret bl.a. samler FE's særlige viden om trusselsaktører og information fra

centerets sensornetværk og omdanner den til trusselvurderinger, situationsbilleder og konkret rådgivning, der skal gøre virksomheder og myndigheder i stand til at forholde sig til deres specifikke risikobillede og opbygge et effektivt cyberforsvar.

"Det er en stor og vigtig opgave, vi har foran os, og det kan selvfølgelig mærkes. Medarbejderne i CFCS er i høj grad "purpose-driven", og på tværs af medarbejderne er der et stærkt ønske om at gøre sit bedste hver dag, fordi vi ved, at vores indsats er vigtig for Danmark", fortæller Thomas Flarup.

CFCS rummer både højt specialiserede tekniske kompetencer og generalistprofiler, men det står ikke i vejen for et tæt samarbejde.

"Den enkelte medarbejders opgaver skal klikke ind i det overordnede hele, ellers flytter det ikke noget. Hvis cyberanalysens viden for eksempel ikke kommer videre til rådgivningen, så den kan blive til konkret og situationsbestemt rådgivning, så har den ikke skabt værdi," siger Thomas Flarup og fortsætter:

"Hvis jeg blev spurgt, ville jeg sige, at det er det, der definerer CFCS som arbejdsplads – faglighed og fællesskab. Det beskriver os godt", slutter han.

CFCS

Center for Cybersikkerhed (CFCS) er nationalt kompetencecenter for cybersikkerhed. Vi vurderer truslen mod Danmark og sikrer løbende et nationalt situationsbillede på cyberområdet.

CFCS støtter samfundets sektorer i deres arbejde med at opbygge et stærkt cyberforsvar og være robuste i tilfælde af cyberangreb. Vores særlige viden, nationale overblik og efterretningsbaserede rådgivning leverer det fundament, som myndigheder og virksomheder baserer deres digitale cyberforsvar på.



Hvis de seneste år har lært os noget, så er det, at cybertruslen er alvorlig og et grundvilkår for alle virksomheder, store som små.

Thomas Flarup



■ CYBERSIKKERHED OG NYE TEKNOLOGIER

Teknologi udvikles hele tiden, og det, der var science fiction i går, kan være virkelighed i morgen. Det giver nye muligheder, men også nye trusler.

De fleste nye teknologier er skabt med gode hensigter, men kan også udnyttes til skadelige formål. Samtidig er teknologi blevet væsentlig mere kompliceret, og det kan være vanskeligt at skelne mellem, hvad der er "hype", og hvad der er reelle fremskridt.

Som efterretningstjeneste skal FE følge med i den teknologiske udvikling for selv at kunne anvende teknologien, men også for at forstå, hvad vores modstandere kan bruge ny teknologi til. Vi vil helst ikke blive overrasket. Som national cybersikkerhedsmyndighed har vi et særligt ansvar for at varsle og rådgive om de mulige sikkerheds- og cybertrusler, som nye teknologier kan medføre. I samarbejde med universiteterne søger vi derfor bl.a. løbende ph.d.-studerende, som forsker i nye teknologier, mens de er ansat hos os.

Chatrobotten, der tog verden med storm

Kunstig intelligens er gradvist blevet bedre og mere udbredt over de sidste mange år. For eksempel er det udbredt at bruge algoritmer baseret på kunstig intelligens til at detektere spam-mails og genkende motiver på billeder. Alligevel vakte det stor opsigt, da virksomheden OpenAI i efteråret 2022 lancerede den kunstigt intelligente chatrobot ChatGPT.



Der er flere gode grunde til at være varsom med brugen af chatrobotter. Selv troværdigt lydende svar kan være pure opspind, og man har ingen kontrol med, hvor de oplysninger, man fodrer maskinen med, ender henne.

Dybest set er ChatGPT en algoritme, der ud fra en enorm mængde sprogdata er trænet til at efterligne vores sprog. Så hvis brugeren siger "A", er ChatGPT bygget til at sige "B" – det vil sige den mest sandsynlige næste sætning.

De avancerede og tilsyneladende intelligente svar, som ChatGPT producerer, har vakt både beundring og bekymring, og debatten om kunstig intelligens er blusset op.

Et er, at chatrobotter som ChatGPT kan skrive eksamensopgaver. Noget andet er, at de også kan skrive falske nyhedshistorier, misinformerende opslag på sociale medier, målrettede phishing-mails og ondsindet computerkode til hackere.

Der er flere gode grunde til at være varsom med brugen af chatrobotter. Selv troværdigt lydende svar kan være pure opspind, og man har ingen kontrol med, hvor de oplysninger, man fodrer maskinen med, ender henne. Det er klart, at cybersikkerhed i relation til kunstig intelligens og chatrobotter bliver mere og mere aktuelt.

Kvantecomputerne kommer

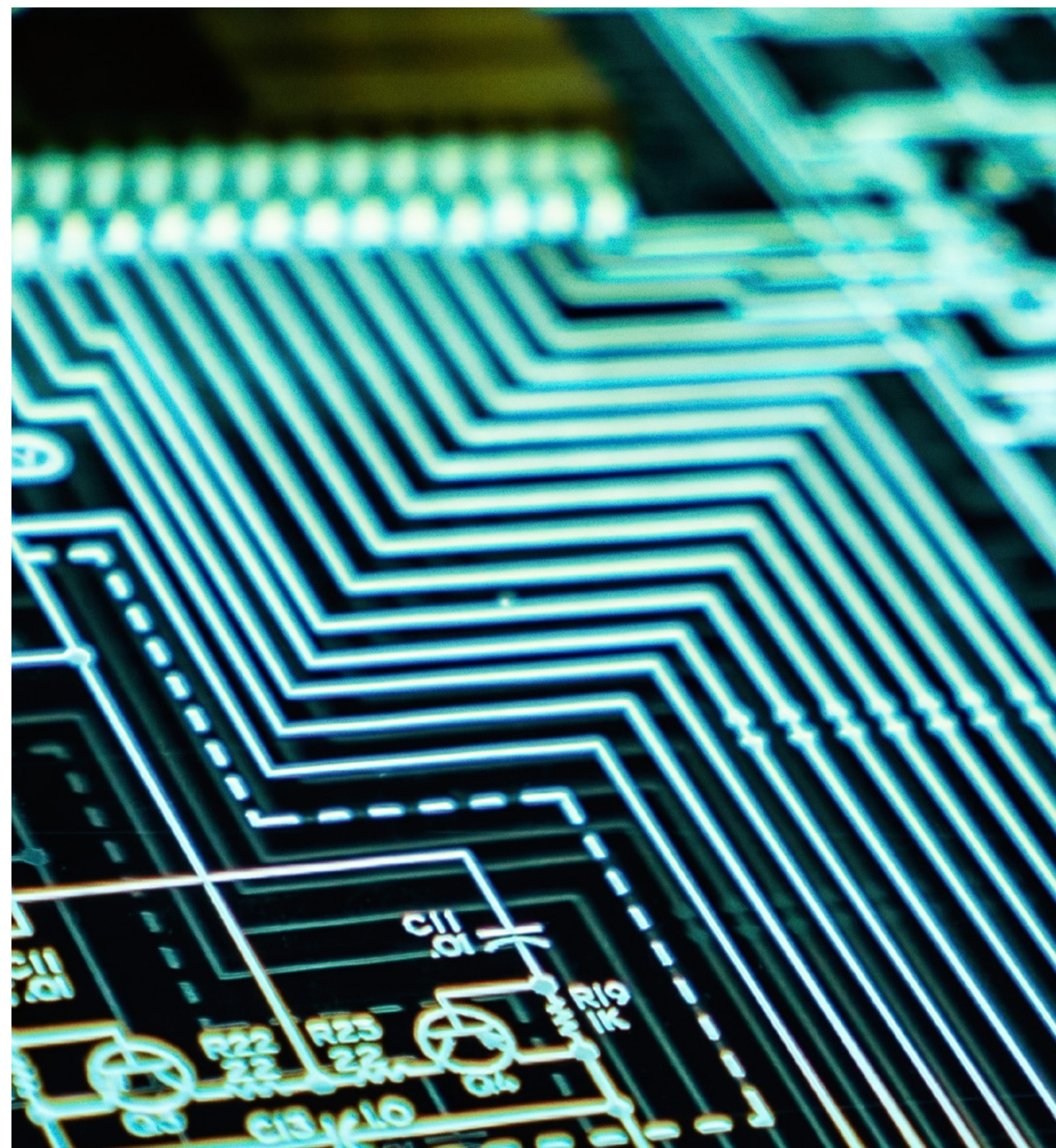
Lidt længere ude i horisonten vil kvantecomputere give nye muligheder for at løse svære problemer, som vi ikke kan løse med traditionelle computere. Det er der store kommercielle muligheder i, men også potentielle trusler mod cyber- og informationssikkerheden.

En tilpas kraftig kvantecomputer kan nemlig bryde den kryptering, der i dag sikrer vores kommunikation på internettet og beskytter vores fortrolige og klassificerede informationer. Faktisk kan en ondsindet aktør allerede i dag indhente og gemme krypteret data med henblik på senere at bryde krypteringen med en fremtidig kvantecomputer.

Det betyder, at hvis vi i fremtiden vil kunne kommunikere sikkert, for eksempel med vores bank eller mellem myndigheder, så skal vi gøre det på en anden måde end i dag. Forskning og udvikling af kommunikationsmetoder, der er sikre i en verden med kvantecomputere, er derfor et meget aktivt felt.

Én mulig løsning er at kryptere med en såkaldt kvantesikker krypteringsmetode. En anden løsning er at udveksle den hemmelige del af kommunikationen på en kvantemekanisk måde, der ikke kan aflyttes.

Hvor sikre de nye metoder er, er dog stadig noget, man evaluerer og forbedrer, efterhånden som teknologien udvikler sig. Og det er selvfølgelig noget, vi følger rigtigt godt med i.



”JEG ER KEYBOARD-KRIGER PÅ HACKERJAGT”



For at beskytte vores medarbejderes identitet, optræder de her under et alias

Cybertruslen er meget høj mod Danmark og danske interesser. Marcus er en af de personer, der er med til at forhindre destruktive hackerangreb i Danmark og hele verden.

Hvad er din baggrund og hvordan endte du i FE?

Min baggrund er en ikke-teknisk universitetsuddannelse, og mit "gateway drug" til cyberverdenen har været Capture The Flag-konkurrencer og softwareudvikling. Jeg endte i FE under mit studie. På det tidspunkt var jeg skoletræt ud over alle grænser, så da jeg faldt over et spændende stillingsopslag i FE, søgte jeg jobbet som en overspringshandling. Til min store overraskelse blev jeg kaldt til samtale, og til min endnu større overraskelse klarede jeg det acceptabelt i rekrutteringstesten. Jeg startede som studenterhjælp, og siden jeg blev færdig med min universitetsuddannelse, har jeg arbejdet i tjenesten fuld tid.

Hvad består dit arbejde i?

Mit arbejde består i at følge statsstøttede hackergrupper og deres aktiviteter imod Danmark. Det er en særlig og kompliceret opgave. Både på grund af truslen, og også fordi opgaverne er mange. Én ting er at reagere, når nogen har angrebet, men vi vil jo gerne kunne reagere inden, så man kan beskytte sig. Det kræver, at jeg sætter mig godt ind i, hvordan grupperne arbejder, og det kræver, at jeg kender min arbejdsplads og dens kapaciteter rigtig godt.

Hvornår kan du mærke, at dit arbejde gør en forskel?

For mig er noget af det mest tilfredsstillende at læse rapportering fra kollegaer rundt om i verden, hvor jeg ved, at de har opdaget hackergrupper ud fra detektionsmetoder eller andre informationer, som vi har delt med dem på baggrund af vores arbejde her i Danmark. Der bliver det super håndgribeligt, hvordan ens arbejde faktisk kan gøre en positiv forskel.

Arbejdet her er ligesom alt andet efterretningsarbejde til tider utaknemmeligt. Man hører om de situationer, hvor hackergrupperne er lykkedes at trænge ind, men sjældent om de situationer, hvor de blev opdaget på grund af vores indsats. Det er the name of the game. Men selv i de tilfælde, hvor vi er blevet udmanøvreret, ender vi alligevel ofte med at udvikle os i en positiv retning. Dels fordi vi lærer af vores fejl; dels fordi vi lærer noget nyt om gruppernes måde at arbejde på; og dels fordi alvorlige sikkerhedshændelser er med til at højne sikkerhedsniveauet og sikkerhedsbevidstheden i Danmarks kritiske infrastruktur. For mig er det tegn på, at vi gør en forskel og bevæger os fremad. Selv i modvind.

Hvordan er det at sidde ved den digitale frontlinje?

Det passer mig supergodt at sidde bag skærmen. Jeg ville ikke kunne ramme en skydeskive, om så mit liv afhang af det. Så selv om tiårige mig nok ikke ville være blevet stolt af at høre, at jeg ville komme til at sidde på et kontor og bakse med at få Excel til at stoppe med at formatere IP-adresser som datoer, så er jeg nu alligevel meget godt tilfreds med livet som keyboardkrieger.

Hvad skal man kunne for at få job i din afdeling?

Nysgerrighed, metodetæft og en sund mængde tjenesteiver. Hvis man har de ting, så kommer man langt. Der stilles ingen krav til specifik uddannelsesbaggrund, men vi har tekniske og personlige krav, vi tester for ved alle ansættelser. Alle udvikler deres kompetencer løbende efter ansættelse enten ved intern uddannelse og/eller kurser i Danmark eller internationalt – det er vi nødt til.



Nysgerrighed, metodetæft og en sund mængde tjenesteiver. Hvis man har de ting, så kommer man langt.



ESBEN HAUGLAND

Chef for Jura
og Ledelsesstøtte

Vide rammer forpligter

■ ÅBENHED I EN HEMMELIG TJENESTE

FE arbejder mest i det lukkede, men naturligt nok under stor offentlig bevågenhed og interesse. Esben Haugland er chef for Jura og Ledelsesstøtte i FE og fortæller om balancegangen for åbenhed i en hemmelig tjeneste.

Som efterretningstjeneste har FE helt særlige vilkår for at kunne udføre sit arbejde. Det indebærer, at en meget stor del af arbejdet er hemmeligt for offentligheden for at beskytte FE's arbejdsmetoder, kapaciteter og kilders sikkerhed.

Offentligheden har dog også et berettiget ønske om at få størst muligt indblik i tjenestens arbejde, bl.a. for at fastholde tilliden til FE, fortæller chef for Jura og Ledelsesstøtte i FE, Esben Haugland.

"Selv om FE arbejder i det lukkede, er både tjenesten og særligt vores arbejdsområde og viden genstand for stor offentlig bevågenhed. Det medfører et behov for at kommunikere, for hvis ikke FE kommunikerer, opstår

der et vakuum, som andre forsøger at udfylde. Ligeledes er det helt afgørende for befolkningens tillid til FE, at vi er transparente i det omfang, det er muligt. Vi må ikke lukke os unødigt om os selv", siger han.

I FE-loven står der, at tjenesten som udgangspunkt ikke er omfattet af offentlighedsloven, hvilket bl.a. har betydning for mediers og borgeres ret til aktindsigt. Men FE forsøger altid at svare på spørgsmål. Der er dog i sagens natur en lang række forhold og sager, som en efterretningstjeneste af forskellige årsager ikke kan kommentere.

"FE har været meget i medierne de senere år. Det er en udfordring, når vi så at sige ofte har én hånd bundet på ryggen og ikke kan sige særlig meget – hvis overhovedet noget. Men vi har en klar politik om at være så åbne, som vi kan. Desuden prøver vi at forklare, hvorfor vi – også når det kan virke svært at følge – nogle gange ikke kan sige noget mere konkret", siger Esben Haugland.

Ekspert og myndighed på cyberområdet

Center for Cybersikkerhed (CFCS), som er en del af FE, har en mere udadvendt rolle, hvor centeret bl.a. hjælper myndigheder og virksomheder med at ruste sig mod digitale trusler. Som myndighed for national it-sikkerhed har CFCS dermed også en offentlig ekspert- og rådgivningsfunktion for myndigheder og virksomheder i især de kritiske sektorer.

"På cyberområdet er vi bl.a. sat i verden for at rådgive. Det betyder, at vi i høj grad skal kommunikere med omverdenen for at fortælle om risici og muligheder i det domæne. Vi har derfor mange udadvendte aktiviteter i regi af CFCS," siger Esben Haugland.

CFCS deler løbende rapporter, undersøgelser og trusselvurderinger på cyberområdet med offentligheden på sin hjemmeside.

Jobopslag tegner et billede af FE udadtil

Når FE kommunikerer med omverdenen, sker det også gennem jobopslag. FE er en stor organisation og slår løbende stillinger op, der alle er med til at tegne et billede af FE som organisation og arbejdsplads. Det har været en aktiv beslutning at bruge rekrutteringsindsatsen mere aktivt som et kommunikationsværktøj.

"FE er vokset meget de senere år, og vi er i konkurrence med alle andre om at tiltrække de bedste medarbejdere. Derfor fortæller vi mere om vores opgaver i jobopslagene, end vi har gjort tidligere, og vi forsøger at komme bredere ud. Det vil selvfølgelig altid være en konkret vurdering, hvor meget vi kan sige", siger Esben Haugland.

FE OG OMVERDENEN

Når FE kommunikerer med omverdenen, sker det typisk gennem publikationer, vores hjemmeside, pressen, jobopslag og sociale medier. Hvert andet år udgives FE's beretning, INDBLIK, som du sidder med i hænderne nu. Derudover udgives UDSYN, der er FE's årlige risikovurdering til offentligheden, hvert år.

■ ÉN TJENESTE – TO LOVGRUNDLAG

FE opererer på to lovgrundlag: FE-loven og CFCS-loven. De indeholder forskellige muligheder og begrænsninger. Og det kræver 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 varslings-tjeneste for internettrusler. Center for Cybersikkerhed (CFCS) er en del af FE, men opererer på et andet lovgrundlag end det øvrige FE.

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 også, at FE som det meget klare udgangspunkt ikke må foretage målrettet indhentning mod danske statsborgere.

CFCS' arbejde er derimod rettet mod danske forhold – konkret at beskytte de vigtigste dele af det danske samfund mod cyberangreb. Det indebærer bl.a., 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.

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 CFCS og det øvrige FE.

FE bruger mange ressourcer på 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.



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

”NÅR MAN ARBEJDER I FE, STÅR FORMÅLET LYSENDE KLART”



For at beskytte vores medarbejderes identitet, optræder de her under et alias

Hvad kan man – og hvad kan man ikke inden for lovens rammer. Juristen Marie hjælper kollegaer fra hele FE med at forstå og fortolke det lovgrundlag, FE arbejder under.

Hvad er din baggrund?

Jeg er jurist og har tidligere arbejdet som anklager og i vores søstertjeneste PET. Derfor har springet til FE måske ikke været så stort, men det er alligevel noget helt andet. I FE arbejder jeg primært med FE-loven, mens andre arbejder med CFCS-loven. Til sammen sætter de to love rammerne for mit og mine kollegaers arbejde, men vi arbejder også med grundloven, Den Europæiske Menneskerettighedskonvention og en række andre lovgrundlag for at løse de mange forskellige typer af opgaver, som lander hos juristerne. Heldigvis har vi i afdelingen en bred vifte af juridiske baggrunde, som giver gode muligheder for at trække på hinandens forskelligartede kompetencer og erfaringer.

Hvad er kernen i dit arbejde som jurist i FE?

Min opgave som jurist i FE består grundlæggende i at spille mine kollegaer bedre. Hvad enten det handler om Rusland, kontraterror eller cyberoperationer, hjælper jeg mine kollegaer i andre dele af FE med at vurdere, hvad de kan, og hvad de ikke kan, inden for rammerne af loven. Mit arbejde bliver derfor meget konkret, når jeg hjælper mine kollegaer fra de operative dele af FE med at se muligheder og finde de løsninger, som giver dem de bedst mulige betingelser for at arbejde.



Min opgave som jurist i FE består grundlæggende i at spille mine kollegaer bedre. Hvad enten det handler om Rusland, kontraterror eller cyberoperationer.

Det giver samtidig en spændende indsigt i FE's opgaveløsning og mulighed for at samarbejde med nogle meget dygtige og passionerede kollegaer. Det er i sig selv både motiverende og inspirerende.

Hvad betyder det for dig at arbejde et sted som FE, hvor der er et meget klart formål?

Når man arbejder i FE, står formålet lysende klart. Vi arbejder med Danmarks sikkerhed, og det mærker man fra første dag. Det lyder muligvis som en kliche, men man føler virkelig, at man er med til at gøre en forskel. Det er samtidig et meget motiverende formål, og det er tydeligt at mærke, at det driver hele organisationen. Når alle arbejder hen mod det samme mål, er det mest et spørgsmål om, hvordan vi kommer bedst derhen.

Hvordan balancerer du mellem privatliv og arbejdsliv?

Jeg har kun fortalt de nærmeste, at jeg arbejder i FE. Det kan selvfølgelig godt give lidt udfordringer, hvis man er til bryllup og skal forklare, hvad man laver. Men man vænner sig til det og lærer hurtigt at bevæge samtalen hen på andre. Som jurist i FE er man jo ikke den mest hemmelige medarbejder, så man finder gradvist den rigtige balance i forhold til, hvem man vil fortælle det til.

Når man arbejder i FE, kan man som udgangspunkt ikke arbejde hjemmefra. Til gengæld har man fri, når man har fri, og jeg synes, at det er rigtig rart, at ens arbejdsliv og privatliv ikke flyder sammen. Jeg oplever samtidig en god fleksibilitet, hvis man skal noget privat i arbejdstiden. Lægen har jo også kun åbent, når du er på arbejde.



Vores hemmelige hverdag

■ EN RET ALMINDELIG ARBEJDSPLADS MED EN UALMINDELIG 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 bl.a. ingeniører, it-medarbejdere, selvlærte hackere, sprogofficerer, jurister, antropologer, historikere og militært ansatte. Pladsen til forskellighed gennemsyner 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 hemmelighedsboksen, 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 et 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 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 bl.a. 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 og Århusgade på Østerbro og på Sandagergård på Amager. Herudover har vi et mindre antal kollegaer i Hjørring-området.

Vi arbejder på at samle lokationerne i København i et nybygget domicil på Svanemøllens Kaserne.



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.

FE HAR OGSÅ BRUG FOR DIG

FE har brug for mange forskellige typer af ansatte. 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 er en række eksempler på nogle af de medarbejdertyper, der arbejder i FE.

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.

DATA-UDVIKLEREN

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, er ingeniør eller har en naturvidenskabelig baggrund.

DEN ELEKTRONISKE INDHENTER

Elektronisk indhentning (SIGINT) er en kompleks efterretningsdisciplin, der kræver mange forskellige kompetencer. Den elektroniske indhenter har typisk en teknisk baggrund, for eksempel som ingeniør, datalog, matematiker eller it-tekniker. Det er fagspecialister med et solidt kendskab til digital kommunikation, som bl.a. 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.

NETVÆRKS-INDHENTEREN 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 lærings-ejne, kreativitet og teknisk snilde.

FØRINGS-OFFICEREN

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 bl.a. skydning, kørsel og udvidet førstehjælp. Føringsofficerer kan have mange forskellige baggrunde, og mange har en videregående uddannelse, men det afgørende er de personlige kvalifikationer.

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, i en række forskellige 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.

KRYPTOLOGEN

Krypto, også kaldet kryptoanalyse, handler om at skaffe adgang til information, som er blevet forsøgt beskyttet af kryptering eller lignende metoder. I dag bliver data i stigende grad krypteret, så for at skabe værdi af anden indhentning er det ofte nødvendigt at kunne dekryptere data trafikken. Arbejdet som kryptoanalytiker består derfor i at forstå og analysere protokoller og kryptosystemer ved at se på den underliggende kryptografi samt softwaren omkring. Det er derfor både stærke it-faglige kompetencer samt dyb matematisk forståelse der er fundamentet i disciplinen.

DEN OFFENSIVE OPERATIONS-PLANLÆGGER

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 særdeles 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.

MILITÆR-ANALYTIKEREN

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 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.

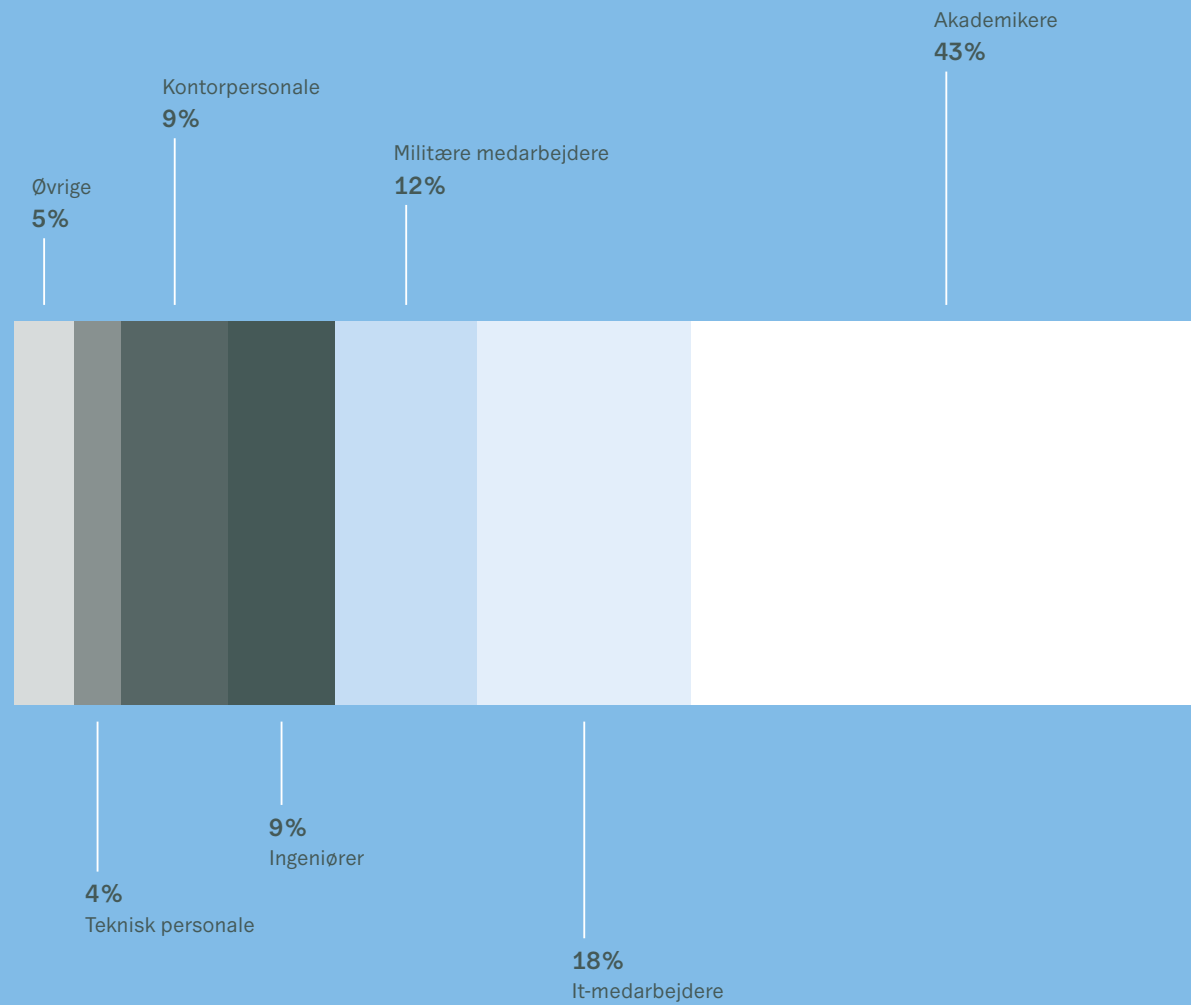
ANDRE STILLINGER

I FE findes der en lang række øvrige stillinger, der ikke nødvendigvis har med indhentning af efterretninger at gøre. Der er også brug for administrative kolleger, undervisere, oversættere, teknisk personale, jurister, vagter, projektledere og mange andre. I takt med at FE vokser i disse år, følger der også et behov for at ansætte endnu flere dygtige kollegaer.

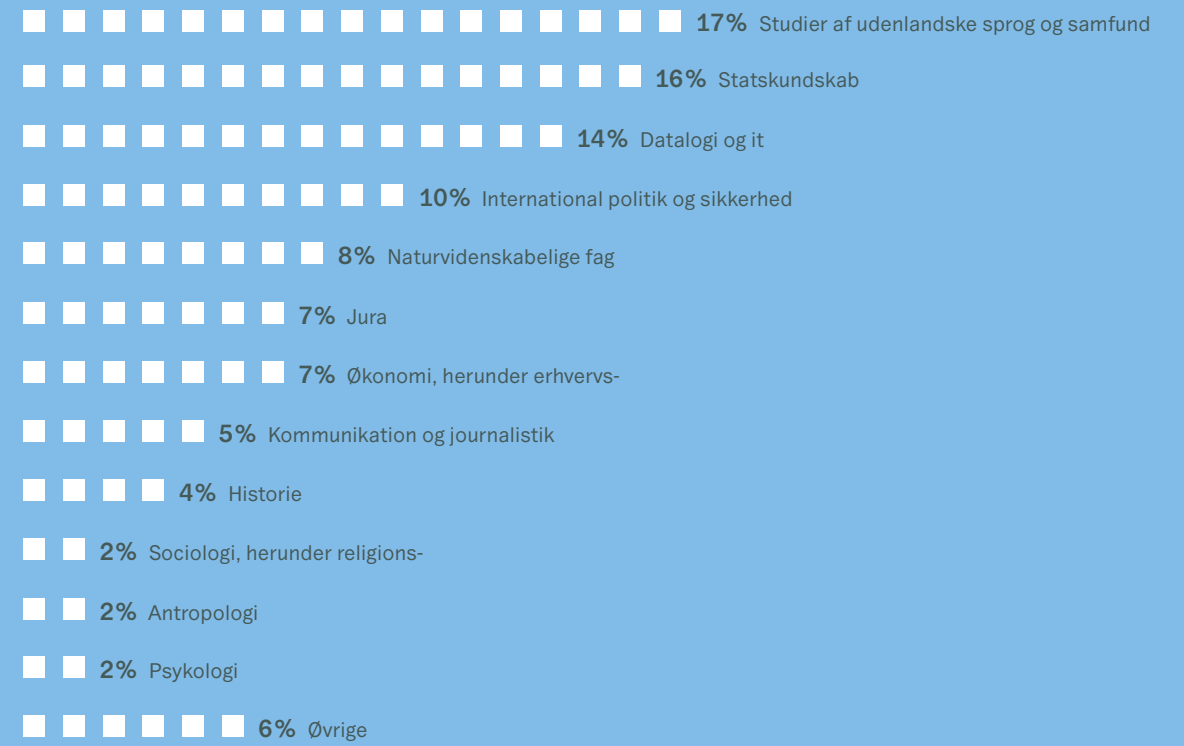
Hold øje med nye jobopslag på fe-ddis.dk og på vores vores LinkedIn-sider.

MEDARBEJDERFORDELING

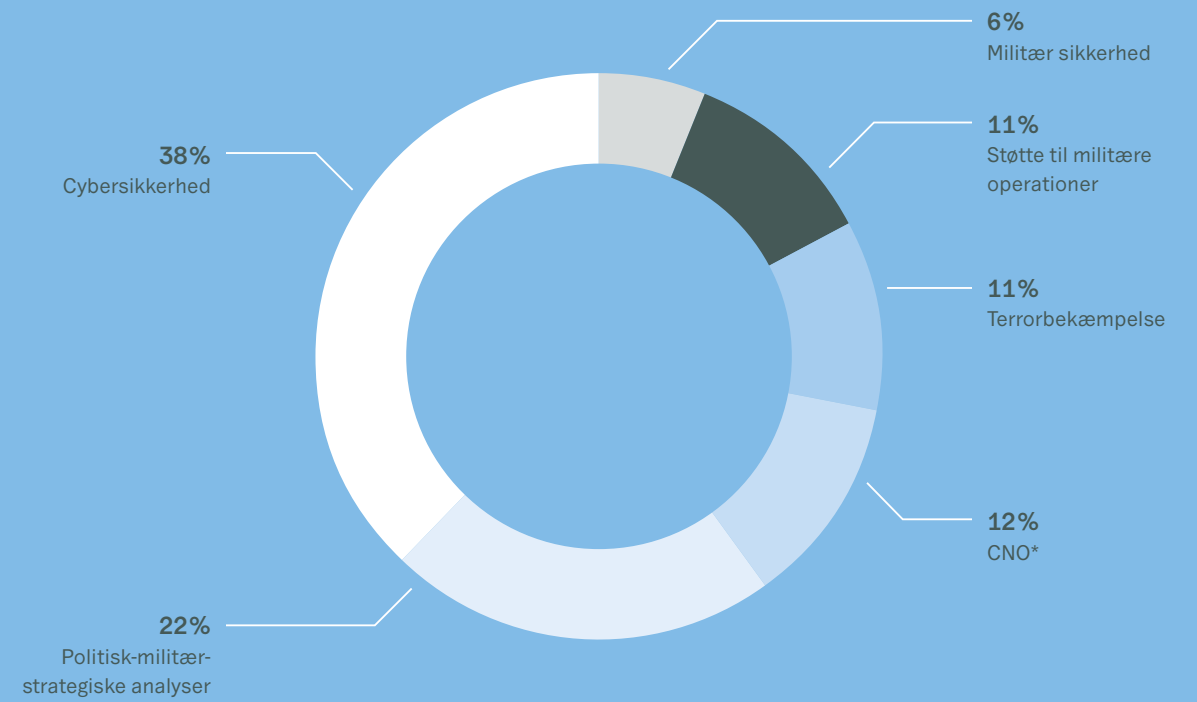
FE'S MEDARBEJDERES BAGGRUND



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.

- Størrelse: Ca. 50.000 m²
- Anlægssum: Over 2 mia. kr.
- Bygherre: PensionDanmark
- Totalentreprenør: MT Højgaard Danmark
- Driftsoperatør: DEAS Group & MT Højgaard Property Development i fælles driftsselskab
- Arkitekt: Vilhelm Lauritzen Arkitekter
- Ingeniør: Rambøll



■ FE'S NYE HOVEDSÆDE

FE's nye hovedsæde skal over de kommende år bygges på Svanemøllens Kaserne i København.

FE rykker i 2027 til nyt hovedkvarter på Svanemøllens Kaserne. Med det nye hovedkvarter kan FE samle de fleste aktiviteter og tilbyde moderne og attraktive rammer til både de nuværende og de mange nye medarbejdere, der ansættes i disse år.

Som højteknologisk og vidensbaseret arbejdsplads med unikke arbejdsopgaver er der desuden høje krav til FE's nye hovedkvarter, som skal tage højde for et meget højt sikkerhedsniveau og sikkerhedsinfrastruktur.



■ SÅDAN BLIVER DU ANSAT I FE

Fokus på sikkerhed nødvendiggør en lidt længere ansættelsesproces end mange andre steder, og det skal du som ansøger være opmærksom på, inden du søger en stilling hos os.



1 ANSØGNING

Du søger en stilling i FE ved at sende en motiveret ansøgning og CV samt dokumentation for relevant uddannelse, kurser mv. Snarest muligt efter udløbet af ansøgningsfristen vil du blive indkaldt til ansættelsessamtale eller få besked om, at du ikke er kommet i betragtning til stillingen.



3 SIKKERHEDSGODKENDELSE

Det er et ubetinget krav, at du kan sikkerhedsgodkendes, når du skal ansættes hos os. Hvis du går videre i forløbet, vil du desuden blive indkaldt til en sikkerhedssamtale, hvor der især lægges vægt på, om du har en sådan adfærd og karakter, at der ikke kan være tvivl om din pålidelighed med hensyn til at håndtere klassificerede informationer. Din ægtefælles, samlevers, registreret partners eller samboendes adfærd og karakter kan også tillægges betydning i vurderingen.



2 ANSÆTTELSESSAMTALE

En central del af FE's ansættelsesforløb er ansættelsessamtalen. I mange tilfælde afholdes der både 1. og 2. ansættelsessamtale, og ofte indgår der en personlighedsanalyse og en faglig test i den mellemliggende periode. Hvis der er tale om en stilling på ledelsesniveau, kan udvalgte ansøgere blive indkaldt til en lederprøve.



4 SAMLET VURDERING

På baggrund af en samlet vurdering og evaluering udvælger FE en ansøger, som indstilles til ansættelse og sikkerhedsgodkendelse, hvorefter der forhandles løn- og ansættelsesvilkår. Løn- og ansættelsesvilkår følger gældende overenskomst inden for staten.

■ VOKSEVÆRK KRÆVER NYTÆNKNING AF FE'S REKRUTTERING

FE vokser i disse år og rekrutterer hver måned et stort antal nye medarbejdere. For at kunne fortsætte denne vækst, har FE taget nye metoder i brug.

3.400 ansøgere til ét stillingsopslag. Det er bestemt ikke hverdagskost i FE. Men det var ikke desto mindre resultatet, da FE i 2022 lancerede en rekrutteringskampagne for at ansætte nye føringsofficerer til indhentningsarbejdet med menneskelige kilder i FE. Kampagnens stil og ordlyd var direkte og uformel og rettet mod en bred målgruppe for at sikre en høj grad af diversitet i ansøgningsfeltet.

"Vi blev overraskede over den store interesse for stillingen, og vi oplevede en langt større spredning i profilerne, end vi har været vant til tidligere. Kampagnen resulterede i mere end 3.400 ansøgninger og herunder en overvægt af ansøgninger i den kvalitet, et job i en efterretningstjeneste kræver. Samtidig lykkedes kampagnen med at nedbryde nogle fordomme om FE og gøre os mere tilgængelig som potentiel arbejdsplads," fortæller FE's HR-chef.

Ikke alle job i FE er agentjob

I FE er antallet af medarbejdere vokset markant de senere år båret af den sikkerhedspolitiske udvikling i verden. Der har samtidig været en markant stigning i antallet af ansøgere til de stillinger, der løbende slås op på FE's hjemmeside. Det er en bemærkelsesværdig udvikling i lyset af den generelt store efterspørgsel på arbejdskraft i hele samfundet.

FE har især ansat mange nye kollegaer på it- og dataområdet. Moderne efterretningsarbejde kræver nye teknologier og mennesker, der forstår at arbejde med dem. FE kan tilbyde mange spændende muligheder for at arbejde med udfordrende teknologiske problemstillinger, hvilket har vist sig så attraktivt, at FE løbende har kunnet tiltrække tilstrækkeligt med højt specialiserede it-specialister. For mange ansøgere har det også vist sig afgørende at kunne gøre en forskel for Danmark – også selvom de ikke nødvendigvis har en agent i maven.

"Det er vigtigt at synliggøre, hvilke muligheder FE kan tilbyde. Udover at være en fagligt stærk og operationel organisation, så er FE også en arbejdsplads, hvor vi forpligter os til hinanden. Man kan ikke tale om sit arbejde derhjemme, og det medvirker til et stærkt kollegaskab samt en lyst til at være en del af et fællesskab. Vi står sammen om at beskytte Danmark, og det mærker man fra dag ét i FE," siger FE's HR-chef.

Hvis du vil være en del af fællesskabet, kan du på FE's hjemmeside se, om der er en stilling, du kunne passe ind i. Du kan også møde FE til karrierevents og på relevante uddannelsesinstitutioner.

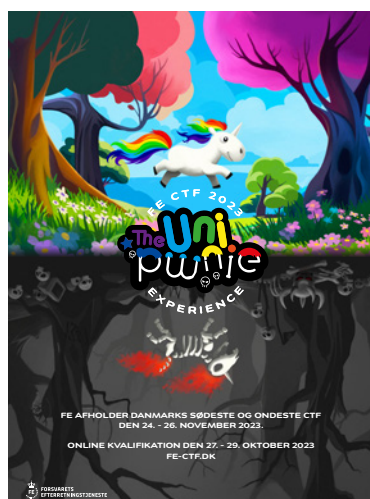


For mange har det også vist sig afgørende at kunne gøre en forskel for Danmark – også selvom man ikke nødvendigvis har en agent i maven.

■ UNIPWNIIE OG CYBER- DEMON – DEN SØDESTE OG ONDESTE CTF

FE har taget nye metoder i brug for at tiltrække talenter. Med Capture The Flag-events skal især folk i hackermiljøet gøres opmærksomme på muligheden for at arbejde i FE.

FE er i stor konkurrence med det øvrige arbejdsmarked om at tiltrække dygtige talenter – ikke mindst inden for it-området. FE's traditionelle sukkethed for at beskytte vores særlige kapaciteter har betydet, at de fleste uden for FE kun ved meget lidt om, hvad FE egentlig er for en arbejdsplads. Vil vi naturligvis stadig beskytte vores hemmeligheder, men vi arbejder målrettet på at dele så meget som muligt om, hvad FE egentlig er for en størrelse. Som led i den indsats har FE forsøgt at skabe opmærksomhed i de danske hackermiljøer ved at afholde en såkaldt Capture The Flag (CTF), der appellerer direkte til en specifik målgruppe og gør opmærksom på FE som en mulig arbejdsplads.



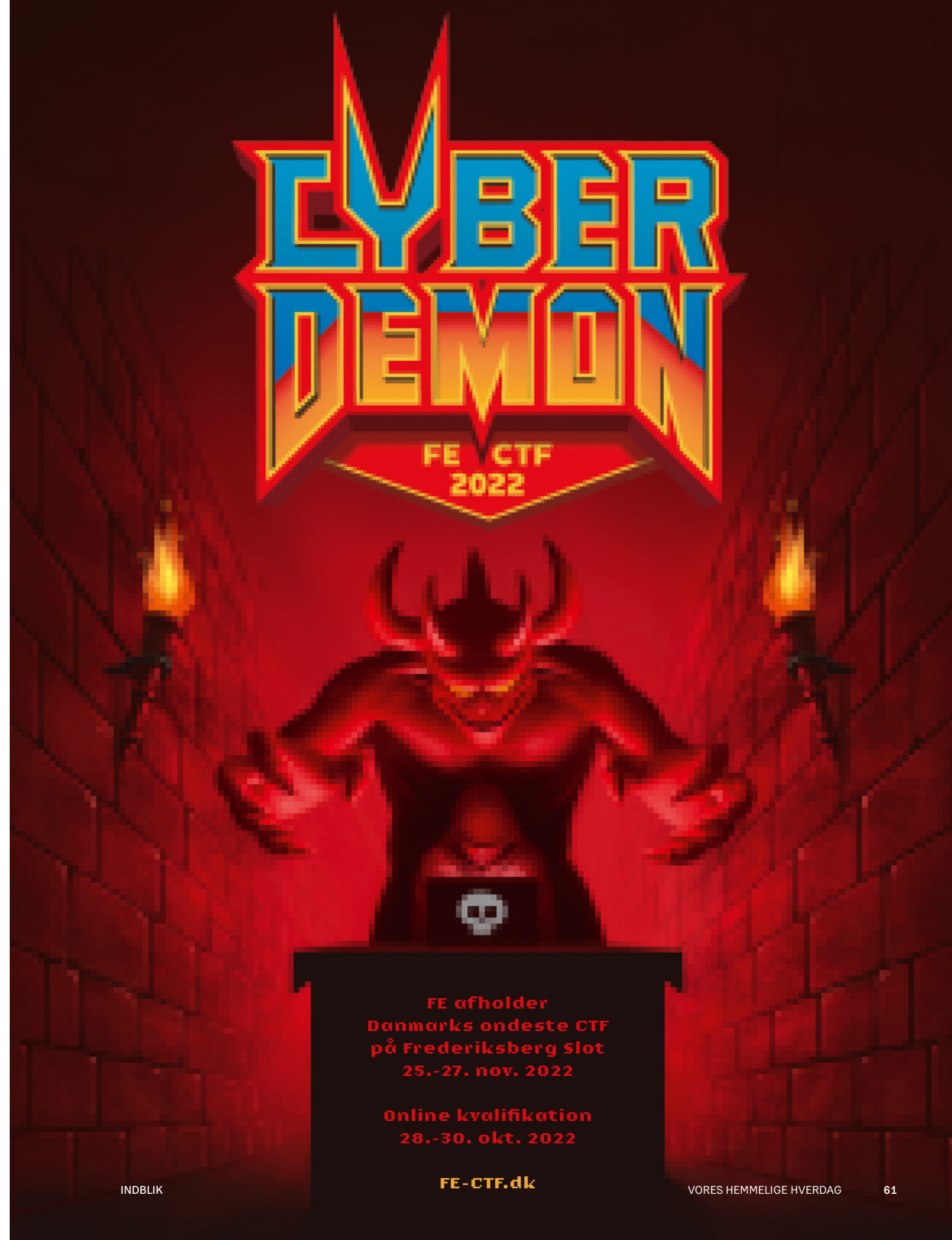
HVAD ER CTF?

CTF (Capture The Flag) er i hackersammenhæng en konkurrence om at løse opgaver med komplekse problemstillinger. Det kan være at bryde ind i systemer eller programmer, som er designet specifikt til konkurrencen, eller finde skjulte beskeder. Når en opgave er løst, får spilleren et flag, som kan omdannes til point. Spillerne kan sidde fysisk sammen, når de spiller, eller hver for sig. Varigheden af en CTF kan være forskellig, men er typisk 48 timer.

I 2022 lancerede FE for første gang en CTF i skikkelse af "Cyberdemon – Danmarks ondeste CTF", hvor ikke færre end 810 hold deltog i den indledende kvalifikation. Den følges i 2023 op med Danmarks sødeste CTF, "Unipwnie". CTF'erne er udviklet af medarbejdere i FE og er på et højt niveau. De afspejler de opgaver og den verden, potentielle nye medarbejdere møder i FE.

Deltagerne udfordres med opgaver og gåder inden for en række forskellige emner, der i mere eller mindre grad relaterer sig til hacker-discipliner. Det er bl.a. emner som software-reversering, krypto, web-sikkerhed og binary exploitation.

Indledningsvist afvikles en online kvalifikation, som er åben for alle. Herfra kvalificerer de bedste hold sig til et fysisk finaleevent, der i 2022 blev holdt på Frederiksberg Slot.



”JEG SKABER MENNESKELIG FORANDRING”



For at beskytte vores medarbejderes identitet, optræder de her under et alias

Verden er i konstant forandring. Mød Claus, der er med til at udvikle efterretningstjenesten, så de menneskelige kompetencer er med til at ruste FE til at beskytte Danmark i den virkelighed, vi står overfor.

Hvad er din baggrund?

Jeg er oprindeligt uddannet lærer og har altid arbejdet med undervisning og udvikling af menneskers kompetencer. FE var for mig en atypisk arbejdsplads inden for mit fagområde, så jeg havde derfor slet ikke overvejet, at det kunne være noget for mig. Men da jeg tilfældigvis faldt over et stillingsopslag, der matchede min faglighed samt mine ønsker for egen udvikling, blev jeg dybt motiveret til at søge stillingen. Nu har jeg været her i ni år.

Hvad består dit arbejde i?

Mine arbejdsopgaver er meget forskellige, men består hovedsageligt i at undervise andre ansatte i FE. Mit arbejde er meget udadvendt, og det kan jeg godt lide. En af mine yndlingsopgaver er at tage imod nye medarbejdere og give dem en god start i FE. Det er en vigtig opgave for både mig og FE.

Derudover udvikler FE sig på lige fod med andre store organisationer, så jeg og mine kollegaer arbejder med relevant kompetenceudvikling af medarbejdere inden for en bred vifte af fagområder, bl.a. ledelse

Hvornår kan du mærke, at dit arbejde gør en forskel?

FE's store styrke er de ansatte og deres viden. For at udvikle en organisation som FE skal medarbejderne også udvikles, og derfor er mit arbejde direkte med til at gøre en forskel. Det kan for mange være en stor omvæltning at begynde i en efterretningstjeneste, og det er vigtigt for mig at være med til at give nye medarbejdere tryghed i det. Det er spændende at være en del af, og jeg kan stadig blive overrasket over, hvor vigtig en rolle jeg har.

Hvad gør FE til en spændende arbejdsplads?

Mine kollegaer og jeg kommer med mange forskellige faglige kompetencer og uddannelsesbaggrunde, og den diversitet gør, at vi komplementerer hinanden godt. Som medarbejder i FE skal man ikke kun have lyst til at bidrage med det, man ved, men også have lyst til at udvikle sin faglighed og udvide sin opgaveportefølje inden for sit område. Det er med til at gøre FE til en spændende arbejdsplads.

Ved din familie og dine venner godt, hvor du arbejder, og hvad du laver?

Der er ikke mange, der ved, hvor jeg arbejder, og jeg kan naturligvis ikke fortælle, hvad jeg laver på mit arbejde. Sådan er det at være en del af en efterretningstjeneste, og det har jeg med tiden lært at navigere i. Det vilkår er til gengæld med til at give et stærkt kollegalt sammenhold.



FE's store styrke er de ansatte og deres viden. For at udvikle en organisation som FE, skal medarbejderne også udvikles, og derfor er mit arbejde direkte med til at gøre en forskel.

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 bl.a. til at styrke cybersikkerheden i de samfundsvigtige sektorer. Det sker for eksempel gennem rådgivning og monitorering af myndigheder og virksomheders netværkskommunikation for at imødegå de mest avancerede cyberangreb. Centeret er desuden myndighed for informationsikkerhed og beredskab på teleområdet.

Støtte til Forsvaret

Sektoren har ansvaret for at støtte Forsvaret og NATO. Det omfatter bl.a. 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 & Ledelsesstøtte

Jura & 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.

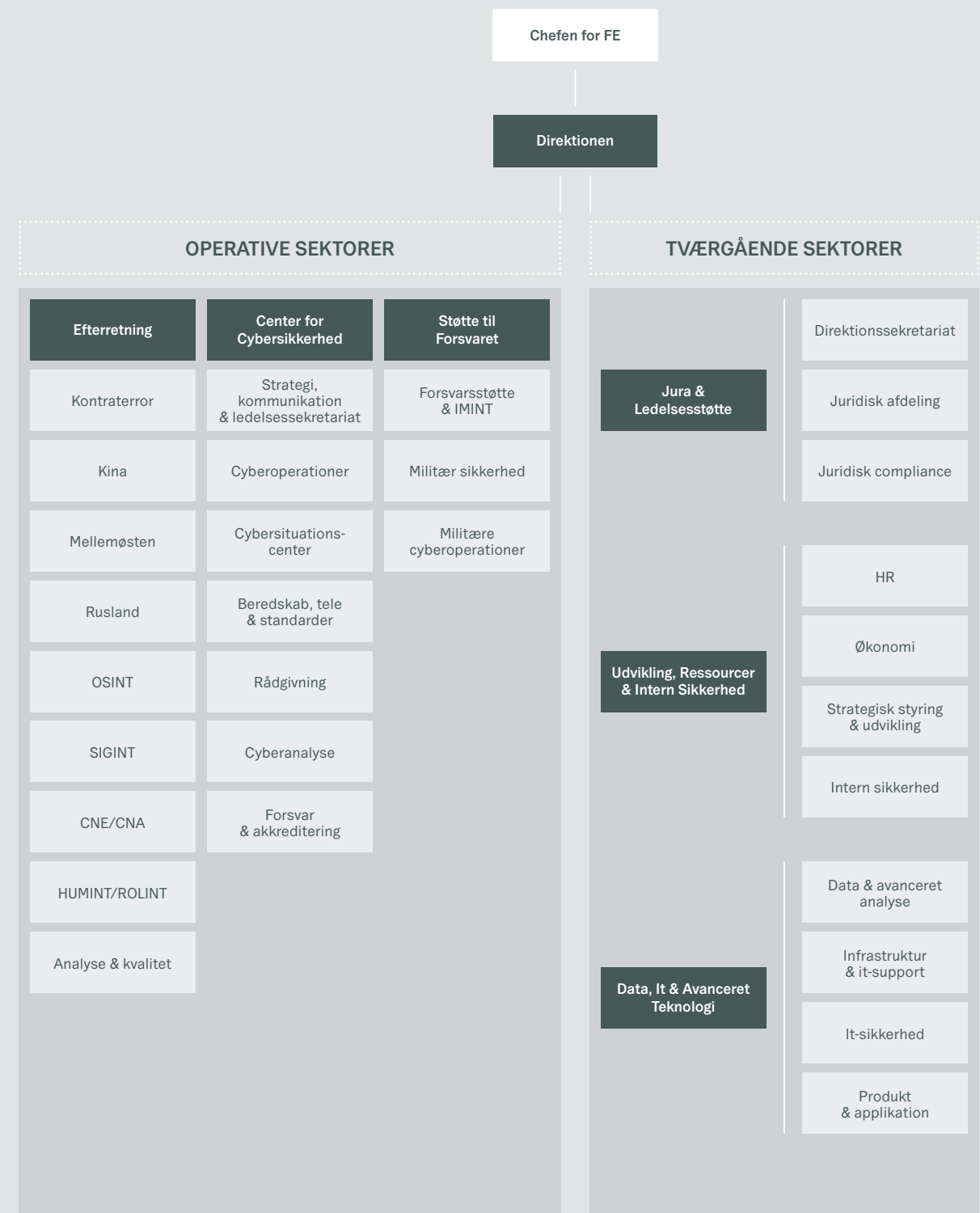
Udvikling, Ressourcer og Intern Sikkerhed

Stabssektoren 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 og for FE's elektroniske indhentningskapaciteter. Herudover står sektoren for drift og udvikling af it-systemer og applikationer samt den interne it-sikkerhed.

ORGANISATIONS DIAGRAM



■ FE'S ØKONOMISKE RAMME

FE fik i 2023 en samlet bevilling på ca. 1.388 millioner kroner, hvilket er en stigning i forhold til 2022, hvor bevillingen var på 1.109 millioner kroner.

I juni 2023 blev der indgået et nyt tiårigt forsvarsforlig (2024-2033), som betyder, at der skal investeres 143 mia. kroner i dansk forsvar og sikkerhed. Forliget er et rammeforlig, som udmøntes løbende, og derfor er FE's økonomiske ramme i perioden endnu ikke fastlagt.

FE's bevilling bliver overordnet brugt på FE's kerneopgave med at identificere og modvirke trusler mod Danmark og danske interesser. Præcis hvordan pengene bruges, kan vi ikke fortælle offentligt, da det kan afsløre FE's kapaciteter. Den teknologiske udvikling betyder dog, at der løbende investeres i nye teknologier til brug for FE's indhentning.

INDBLIK
Forsvarets Efterretningstjenestes
beretning 2021-2022

Udgivelse
November 2023

Foto
Forside: Unsplash
Side 4, 9, 27, 33, 42: Trine Bukh
Side 7, 14, 20, 23, 36, 39, 48: Unsplash
Side 29: Pexels
Side 16, 24, 30, 40, 46, 62: Adobe Stock

Design og layout
e-Types

Tryk
GraphicUnit ApS

Papir
Indhold: MultiDesign White 130 g
Omslag: MultiDesign White 300 g



Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

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