FORSVARETS EFTERRETNINGSTJENESTE

Beretning 2015 - 2016

FE's Beretning 2015-2016

Forord

Danmark står over for et stadig mere sammensat og komplekst trusselsbillede. Den globale udenrigs- og sikkerhedspolitiske scene har de seneste år været præget af hastige forandringer og opbrud. Europa har i 2015 og 2016 oplevet en stigning i antallet af terrorangreb. Angreb som er sket på tværs af landegrænserne i Europa. Samtidig ses en fortsat tiltagende trussel på cyberområdet, og også i Østersøregionen sker der en udvikling af betydning for Danmarks sikkerhed som følge af blandt andet øget russisk militær aktivitet.

Den stigende kompleksitet og den hastige udvikling stiller store krav til FE og vores opgave med at afdække, varsle og modvirke udefrakommende trusler mod Danmark. Som en af Danmarks markante vidensorganisationer stræber vi konstant efter at omsætte vores viden til operativ effekt – f.eks. ved at bidrage til den samlede kontraterrorindsats sammen med Politiets Efterretningstjeneste (PET) og internationale samarbejdspartnere, ved at afdække og imødegå cyberangreb eller ved at bidrage til grundlaget for politiske beslutninger.

Vores viden gør og skal gøre en forskel for Danmark og danske interesser.

Som led i en ambitiøs udviklingsdagsorden har FE en målsætning om at blive en af de mest dynamiske og operativt fokuserede vestlige efterretningstjenester. For at forfølge dette mål og for at løse vores opgaver bedst muligt har vi et stort fokus på vores vigtigste ressource, nemlig vores medarbejdere. Vi har fået mange nye kollegaer, og vi bruger fortsat mange ressourcer på at både tiltrække og fastholde de bedste og mest kompetente medarbejdere, der leverer resultater af stadigt højere kvalitet og har et operativt fokus.

I 2016 har FE oprettet et hackerakademi med ønsket om at tiltrække medarbejdere med særlige kompetencer. På Hackerakademiet uddannede FE i 2016 hackere, som kan udføre offensiv netværksindhentning, og her i 2017 fokuserer FE tillige uddannelsen på at forsvare Danmark mod cyberangreb. Som et led i rekrutteringsprocessen lancerede vi en kampagne med skjulte budskaber i såvel traditionelle som sociale medier. Det kan du læse mere om i denne beretning.

I beretningen kan du også få et indblik i vores organisation. FE tilpasser løbende organisationen til det ændrede trusselsbillede. Efter mange års fokus på terrorbekæmpelse blev afdelingen for kontraterror til en selvstændighed enhed - Sektor for Kontraterror. Desuden har vi etableret en ny militær CNO-sektor (Computer Netværk Operationer), der er ansvarlig for at understøtte Forsvaret i relation til cyberoperationer både defensivt og offensivt. Omorganiseringer der vil ruste FE til at bidrage til at imødegå de trusler, som Danmark står over for.

Beretningen handler primært om FE som virksomhed. Vil du læse om FE's efterretningsmæssige vurderinger, skal du læse vores årlige publikation "Efterretningsmæssig Risikovurdering", der ligesom beretningen her ligger på FE's hjemmeside fe-ddis.dk.

God læselyst

Lars Findsen
Chef for Forsvarets Efterretningstjeneste
Kastellet, juni 2017

Indhold

KASTELLET, KØBENHAVN

Kastellet er opført i 1663 og er et af de ældste og bedst bevarede fæstningsanlæg i Nordeuropa.

Opgaver

FE har tre hovedopgaver:
- Vi er Danmarks udenrigs- og militære efterretningstjeneste
- Vi er Danmarks militære sikkerhedstjeneste
- Vi er den nationale it-sikkerhedsmyndighed

Som efterretningstjeneste skal FE medvirke til at forebygge og modvirke trusler mod Danmark og danske interesser. Det gør vi ved at indhente, analysere og formidle oplysninger om forhold i udlandet, som har betydning for Danmark og danske interesser, til regeringen og nationale myndigheder. Dette bidrager til, at Danmark som suveræn stat kan føre sin udenrigs-, sikkerheds- og forsvarspolitik på grundlag af selvstændige, nationale efterretningsmæssige vurderinger.

I FE's arbejde forstås danske interesser bredt og kan f.eks. omfatte politiske, militære og økonomiske områder samt teknisk-videnskabelige oplysninger af betydning for Danmarks sikkerhed, dansk økonomi mv. Det gælder også konflikter og sikkerhedsspørgsmål af betydning for dansk udenrigs- og sikkerhedspolitik samt konkrete trusler fra forskellige aktører i forhold til eksempelvis danske ambassader, udsendte soldater eller andre danske mål i udlandet.

Synergi mellem de tre hovedopgaver

FE's tre overordnede opgaver hænger tæt sammen, og det giver klare synergier, at de er samlet i FE. Det gælder både i forhold til videndeling og tekniske færdigheder, som kan styrke FE's evne til at imødegå trusler mod Danmark.

Beskyttelsen af Danmark og danske interesser

Efterretningsvirksomhed og beskyttelsen af danske interesser er kernen i FE's arbejde, og det som vi bruger størstedelen af vores ressourcer på. Som efterretningstjeneste bruger vi de særlige muligheder, vi har til at indhente relevante oplysninger, som ikke er alment tilgængelige omkring f.eks. stormagters ageren eller de trusler, som udspringer fra terrorgrupper. Oplysninger bliver bearbejdet og analyseret og derefter leveret som efterretningsprodukter til vores kunder. FE's produkter bruges blandt andet som baggrund for politiske beslutninger eller i forbindelse med Forsvarets militære operationer.

Beskyttelse af det danske forsvar

FE er ansvarlig for den militære sikkerhedstjeneste, der skal beskytte Forsvaret mod terrorisme, spionage, sabotage og andre former for kriminalitet. Beskyttelsen omfatter bl.a. medarbejdere, materiel og bygninger både i Danmark og i udlandet. FE er samtidig national sikkerhedsmyndighed inden for Forsvarsministeriets område.

Styrkelse af Danmarks robusthed mod cyberangreb

FE's Center for Cybersikkerhed (CFCS) er Danmarks nationale it-sikkerhedsmyndighed og nationalt kompetencecenter på cybersikkerhedsområdet. CFCS blev oprettet i 2012 som en del af FE. Centerets opgave er at bidrage til at beskytte den digitale infrastruktur i Danmark og til at styrke Danmarks robusthed mod cyberangreb. CFCS har særligt fokus på at imødegå avancerede cyberangreb mod danske myndigheder og virksomheder, der varetager samfundsvigtige funktioner.

Hvorfor er vi hemmelige?

FE ønsker ikke at være mere hemmelig end højst nødvendigt, og vi vil gerne fortælle så meget om os selv og vores arbejde som muligt. Men der er alligevel nogle særlige forhold omkring efterretningsarbejdet, som gør, at vi ikke kan være åbne om alt, hvad vi foretager os. Vi er nødt til at beskytte vores kapaciteter, vores medarbejdere og vores kilder. Desuden er vi nødt til at sikre den særlige tillid mellem os og andre efterretningstjenester, som vi samarbejder med.

Vi skal beskytte vores kapaciteter

En efterretningstjeneste har nogle særlige muligheder for at indhente oplysninger, som ellers ikke er umiddelbart tilgængelige. Det er afgørende for effekten af vores arbejde, at det kun er os, der kender vores muligheder. FE indhenter f.eks. kommunikation via forskellige kapaciteter. Det gør vi for at skaffe oplysninger om forhold, der kan have betydning for Danmarks sikkerhed, herunder trusler mod Danmark. Hvis de personer, der kommunikerer om disse trusler, ved, hvilken kommunikation FE måske lytter med på, vil de højst sandsynligt finde andre måder at kommunikere på. Derfor fortæller vi ikke offentligt, præcis hvad vi gør, eller hvordan vi gør det.

Vi skal beskytte vores medarbejdere

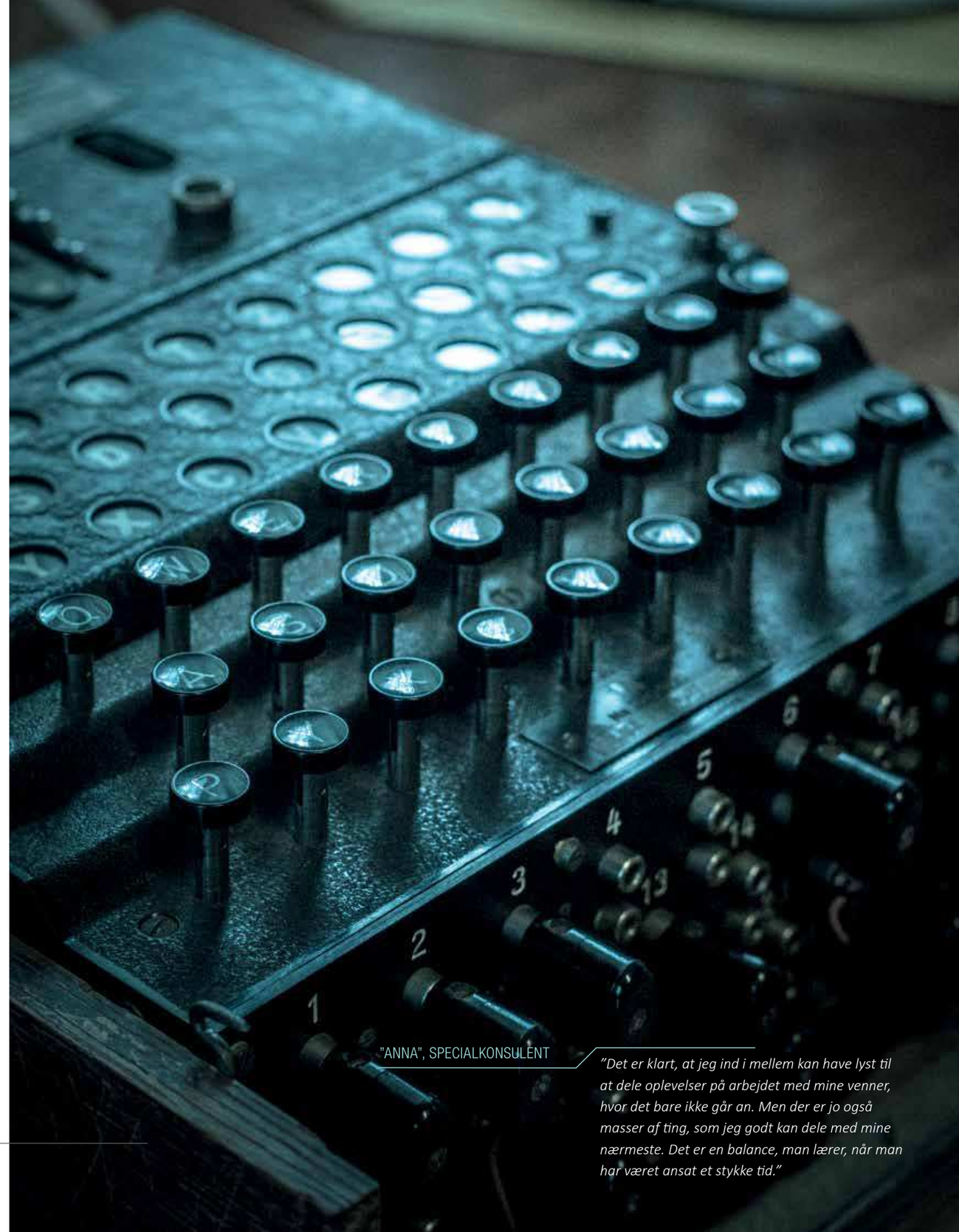
Helt generelt beskytter vi vores medarbejdere – både fysisk og mod andre fremmede efterretningstjenester. Det at være ansat i en efterretningstjeneste kan give anledning til uønsket opmærksomhed. Vi sender medarbejdere ud i verden for at indsamle oplysninger. I visse tilfælde kan det arbejde være forbundet med betydelig fare.

Vi skal beskytte vores kilder

Efterretningsarbejde er et spørgsmål om tillid. Hvis FE f.eks. har rekrutteret en kilde, der afslører følsomme informationer til os, skal denne kilde kunne stole fuldt ud på, at FE ikke kompromitterer vedkommende og afslører, hvor hemmelighederne kommer fra. Hvis kildens informationer falder i de forkerte hænder eller bliver offentligt kendt og derfor måske kan spores tilbage til kilden, vil kilden være kompromitteret, hvilket kan medføre en række konsekvenser for såvel kilden som FE. Afhængigt af situationen kan kompromittering af kilden indebære en betydelig fare for kilden.

Vi skal beskytte vores samarbejdspartnere

Tillid er også af afgørende betydning for forholdet mellem os og de efterretningstjenester, vi samarbejder med. Vi deler oplysninger med andre efterretningstjenester, og vi får til gengæld oplysninger fra dem, som kan have betydning for Danmarks sikkerhed. Også vores samarbejdspartnere skal kunne stole på, at denne deling af informationer sker i fuld fortrolighed. Absolut fortrolighed og gensidig tillid er de væsentligste spilleregler for al efterretningssamarbejde. Hvis FE tilsidesætter hensynet til samarbejdspartnere eller kilder, risikerer vi, at FE fremover ikke modtager vigtige oplysninger. Det vil påvirke vores evne til at varetage vores opgaver effektivt. Særligt for et mindre land som Danmark er det vigtigt at sikre gode og tætte relationer med andre efterretningstjenester. Du kan læse mere om FE's partnersamarbejde på side 19.



ENIGMA KODEMASKINE

"ANNA", SPECIALKONSULENT

"Det er klart, at jeg ind i mellem kan have lyst til at dele oplevelser på arbejdet med mine venner, hvor det bare ikke går an. Men der er jo også masser af ting, som jeg godt kan dele med mine nærmeste. Det er en balance, man lærer, når man har været ansat et stykke tid."

Efterretningstjenesters særlige vilkår

"Som efterretningstjeneste har vi særlige muligheder for at få adgang til informationer, der ikke er alment tilgængelige, og som andre gerne vil holde hemmelige."

KASTELLET, KØBENHAVN

FE har haft til huse på Kastellet siden tjenestens begyndelse i 1967.

Mulighederne for at indhente data er helt centrale for FE. Som efterretningstjeneste har vi særlige muligheder for at få adgang til informationer, der ikke er alment tilgængelige, og som andre gerne vil holde hemmelige. Vi benytter forskellige metoder til at indhente vores oplysninger på, såkaldte indhentningsdiscipliner (se side 16-17).

FE's indhentning er geografisk neutral. Med andre ord kan indhentningen ske fra en hvilken som helst geografisk lokalitet, herunder Danmark. Det afgørende er, at indhentningen er rettet mod forhold i udlandet af betydning for Danmark og danske interesser.

Det er et vilkår for en udenrigsefterretningstjeneste, at efterretningsarbejde ofte vil være i strid med lovgivningen i det land, som indhentningen er rettet mod, eller hvor den foregår. Det samme kan gøre sig gældende for udenlandsk efterretningsvirksomhed på dansk grund, som kan være i strid med dansk lovgivning.

Som efterretningstjeneste er det kun muligt at varsle om fremtidige udviklinger på baggrund af omhyggelig bearbejdning og analyse af de indhentede oplysninger. Det gør vi ved at anvende en række faste sandsynlighedsgrader. Jo større sikkerhed og præcision vi kan frembringe, jo større er nytten af FE's produkter.

For at sikre troværdigheden af efterretningsgrundlaget arbejder FE med strukturerede metoder til at analysere de indhentede oplysninger. FE vurderer kontinuerligt kildernes pålidelighed og deres adgang til oplysningerne. Dernæst vurderer vi oplysningens sandsynlighed og troværdigheden af oplysningen. Vores evne til målrettet at validere oplysninger ved hjælp af vores øvrige kilder og indhentningsformer er af afgørende vigtighed. Ofte har vi også mulighed for at udføre vigtig og omfangsrig validering af oplysninger ved hjælp af frit tilgængelige metadata på internettet. På denne måde kan vi forarbejde rådata og gøre det til validerede oplysninger, der fungerer som udgangspunkt for det videre analysearbejde og i sidste ende fører til udarbejdelse af efterretninger til brug for vores kunder.

Efterretningskredsløbet: Efterretningsarbejdet er en holdindsats

Efterretningskredsløbet er en stiliseret fremstilling af den måde, vi arbejder på. I det daglige er der tale om en dynamisk proces, der består af en række sammenhængende og overlappende delprocesser, hvor nye oplysninger og dermed nye efterretningsbilleder kontinuerligt fører til justerede og ændrede behov for indhentning af informationer.

Identifikation af behov

Efterretningsprocessen begynder i tæt dialog med FE's kunder for at identificere deres behov for viden. I efterretningskredsløbet bliver kundernes ønsker om oplysninger omsat til konkrete, prioriterede efterretningsbehov, som derefter bliver nedbrudt til konkrete emner for indhentning. På den baggrund beslutter FE, hvilke indhentningskapaciteter der skal bringes i spil for at indhente oplysningerne. Efterretningsbehovene behandles i prioriteret rækkefølge, da der ikke er ressourcer til at lægge lige meget vægt på alle områder.

Samarbejde i efterretningsteams

Efterretningsarbejdet er en holdindsats, og FE arbejder i stigende grad med integrerede teams på vores vigtigste indsatsområder. FE's efterretningsteams er sammensat af specialister på tværs af organisationen, som har til opgave at drive efterretningskredsløbet fremad og optimere FE's samlede indsats på prioritetsområderne. Det tætte samarbejde mellem eksempelvis føringsofficerer (se side 17), bearbejdere, it-specialister og analytikere er med til at sikre, at FE skaffer de rette informationer til at dække de højest prioriterede efterretningsbehov.

Fra indhentning til produkt

Uanset hvilken indhentningsform der anvendes, er processen fra indhentning til produkt ofte kompliceret og tidskrævende. Processen stiller store krav til specialiseret teknisk viden inden for vidt forskellige teknologier og samarbejdet i vores efterretningsteams. Vi skal være i stand til at identificere, hvor de oplysninger, der efterspørges, er tilgængelige, f.eks. ved hjælp af opsnappet kommunikation eller menneskelige kilder. Når vi har sikret indhentningen, kommer udfordringen med at lagre og strukturere de meget store datamængder. De tekniske indhentningsformer frembringer i stigende grad krypteret materiale, der forudsætter, at krypteringen brydes, før materialet kan bruges.

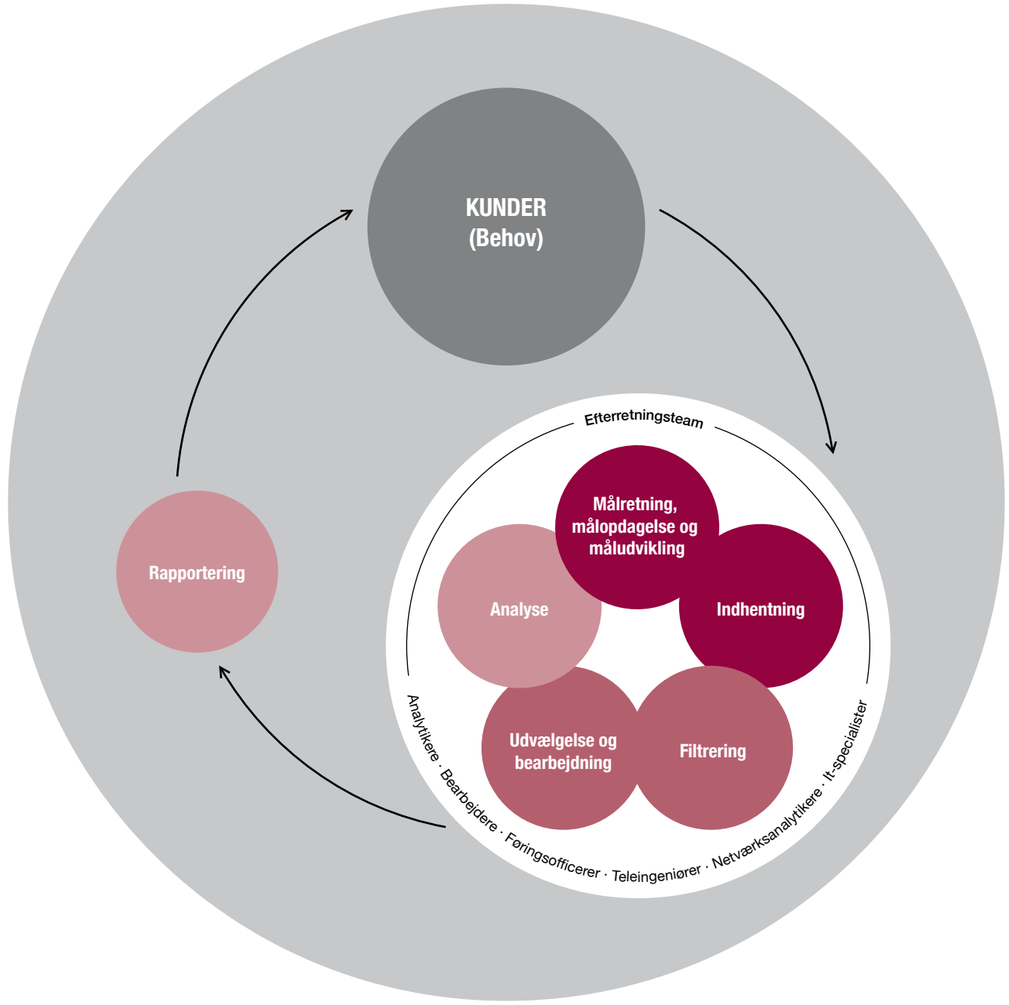
Et efterretningsbillede er altid et øjebliksbillede. Derfor er det centralt, at FE hele tiden igangsætter ny indhentning og samarbejder med partnere for at konsolidere efterretningsbilledet. For at udvikle vores egen indhentning bedst muligt afdækker vi bl.a. kommunikationsinfrastruktur og metoder og identificerer de potentielle kilder, der kan sikre os adgang til de ønskede oplysninger. I daglig tale kalder vi dette for målretning, målopdagelse og måludvikling.

Arbejdet i FE's efterretningsteams er med til at sikre, at vi kan danne det bedst mulige efterretningsbillede inden for tjenestens prioriterede indsatsområder. Ud fra disse efterretningsbilleder er det bl.a. analytikernes opgave at rapportere til kunder og partnere. FE's produkter omfatter bl.a. efterretningsvurderinger, temasignaler, situations- og trusselsvurderinger samt briefinger til centraladministrationen og Forsvaret.

"LINE", SEKTIONSCHEF

"Medarbejderne har ofte en innovativ tilgang til arbejdet og indgår med hver deres speciale i et tæt samarbejde i FE's efterretningsteams. En sektionschefs arbejde består bl.a. i at identificere de nødvendige kompetencer samt at sparre med medarbejderne med fokus på, at efterretningskredsløbet fungerer optimalt."

EFTERRETNINGSKREDSLØBET



Indhentningsdiscipliner

FE er en all source-efterretningstjeneste, hvilket betyder, at vi beskæftiger os med alle typer af informationsindhentning.

Der er fordele og ulemper ved alle former for indhentningsdiscipliner. Disse tager vi højde for, når vi overvejer, hvilke indhentningsformer der skal bruges. En helt afgørende faktor er de risici, der er forbundet med brugen af indhentningsdisciplinerne. Overordnet set arbejder FE med følgende fem indhentningsdiscipliner:

SIGINT

SIGINT står for Signals Intelligence, som er elektronisk indhentning af forskellige typer af signaler som dataoverførsler mellem computernetværk, telekommunikation osv. Den elektroniske indhentning sker f.eks. fra permanente indhentningsfaciliteter, der indhenter mod satellitter. Det kan også være indhentningsfaciliteter opstillet i udlandet, som er mulige at 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 systemer til at behandle det indhentede materiale og er teknisk komplekst. Det skyldes, at mængden af kommunikation er stærkt stigende, samtidig med at der hele tiden udvikles nye teknologier.

Electronic Intelligence (ELINT) er en disciplin, der også er en del af SIGINT, og som omfatter evnen til indhentning mod non-kommunikation, eksempelvis radarsignaler.

SIGINT er passiv og forbundet med en forholdsvis lav risiko set fra efterretningstjenestens side.

NETVÆRKSINDHENTNING

Netværksindhentning er også kendt som Computer Network Exploitation (CNE). Denne indhentningsform er i 'familie' med SIGINT, da der er tale om elektronisk indhentning mod computernetværk. Den kræver typisk, at man skaffer sig adgang til lukkede netfora, it-systemer og computere, hvilket kræver stor indsigt i it. Mange af de personer, der arbejder med netværksindhentning, har derfor samme kompetencer som hackere.

HUMINT

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

HUMINT kræver ofte direkte personlig involvering fra efterretningstjenestens medarbejdere og/eller fra de kilder, som skaffer oplysningerne. Det betyder, at der er personer, der løber en konkret risiko for at blive afsløret og potentielt udsætter sig selv for fare. Derfor er HUMINT forbundet med en betydelig risiko og er en indhentningsform, der kun anvendes, når risici nøje er afvejet i forhold til de mulige gevinster.

IMINT

IMINT står for Imagery Intelligence og er efterretninger, der baserer sig på billedmateriale indhentet af forskellige sensorer. Sensorerne genererer billeder af objekter eller områder optisk, elektronisk, digitalt samt via andre visualiseringsmidler.

OSINT

OSINT står for Open Source Intelligence, hvilket er indsamling af oplysninger fra åbne kilder, der typisk omfatter offentligt tilgængelig information fra internettet, trykte medier, tv m.m. OSINT er dog langt mere end det at læse nyheder og bruge opslagsværker. OSINT drejer sig også i høj grad om avanceret og systematisk indsamling af oplysninger fra bl.a. internettet.

INDHENTNINGSSTATION AMAGER

Radomer er lavet af særligt glasfiber, der holdes oppe af lufttryk. Radomer beskytter antenner mod vind og vejr.

Udenlandske partnere

Deling af efterretninger med partnertjenester i andre lande bidrager til at skabe en mere komplet forståelse af et trusselsbillede, der ofte overskrider landegrænser og har en stigende kompleksitet. Samarbejdet med udenlandske partnertjenester er derfor helt afgørende for FE's opgaveløsning. Udveksling om indhentningsmetoder, teknologier og kapaciteter styrker FE's evne til at forebygge og modvirke trusler mod Danmark og danske interesser. Partneres efterretninger indgår i vidt omfang i FE's analyser og derigennem i en betydelig del af de produkter, som FE udarbejder til sine kunder.

I 2015-2016 har FE derfor fortsat prioriteret sine partnerrelationer højt. Angrebene i blandt andet Paris og Bruxelles har vist, hvordan terrornetværk opererer på tværs af landegrænser i Europa. Det vidner om vigtigheden af, at sikkerheds- og efterretningstjenester samarbejder på tværs af landegrænser. Det samme er gældende inden for eksempelvis cyberområdet, hvor FE samarbejder med udenlandske tjenester for at imødegå cyberspionage og cyberkriminalitet. Da FE er en all source-tjeneste, samarbejder vi med partnertjenester på tværs af forskellige indhentningsdiscipliner såsom SIGINT, CNE og HUMINT m.m.

FE har traditionelt set samarbejdet med tjenester i den vestlige verden, men i takt med den stigende udfordring med terrorisme har FE også samarbejde med en række tjenester i andre dele af verden, herunder Mellemøsten og Afrika. Samarbejdsformen kan være både bilateral og multilateral, ligesom FE indgår i efterretningsmæssige samarbejder i NATO og EU under hensyntagen til det danske EU-forsvarsforbehold. FE deltager også i samarbejder, hvor efterretningstjenester fra forskellige lande arbejder sammen om et særligt emne, eksempelvis om at anvende en særlig indhentningsform eller imødegå en specifik trussel.

Et fortroligt samarbejde

FE's partnersamarbejde er opbygget over mange år og er baseret på troværdighed, tillid og fortrolighed. Det gælder de udvekslede oplysninger eller metoder såvel som eksistensen af selve samarbejdsrelationen. Det er en central spilleregel, at FE hverken bekræfter eller afkræfter eksistensen af et partnersamarbejde, heller ikke over for øvrige partnere. Hvis FE's partnere får indtryk af, at FE ikke kan opretholde den fulde fortrolighed, vil konsekvensen typisk være, at relationen tager skade. Det gælder ikke kun i forhold til den partner, der oplever manglende diskretion, men også i forhold til FE's øvrige partnere.

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

En særlig arbejdsplads

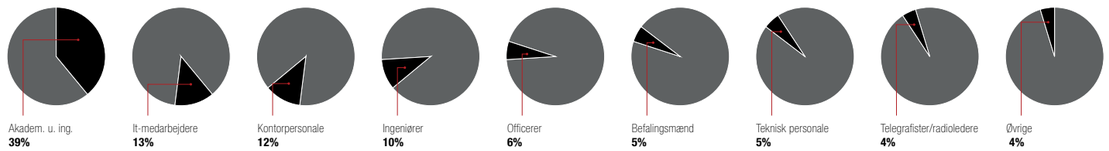
FE er en arbejdsplads, hvor ansøgerne ikke kender deres opgaver fuldt ud, før de begynder i jobbet. Det overrasker nok ikke, men et job i en efterretningstjeneste adskiller sig fra andre jobs. Det er et job, hvor man får mulighed for at arbejde med ting, man ikke gør andre steder.

FE er en bred vidensorganisation

Da FE er en all source-efterretningstjeneste, har vi alle indhentningsdisciplinerne samlet under ét tag, og det gør FE til en fagligt alsidig virksomhed, hvor medarbejdere besidder en lang række forskellige faglige kompetencer, lige fra it og antropologi til historie og militærfaglige kompetencer.

MEDARBEJDERNES BAGGRUND

*Første gruppe - akademikere uden ingeniører - er uddybet på side 23



FE er en organisation, hvor medarbejderne får rig mulighed for at have fingrene dybt begravet i deres fagområde og mulighed for at holde sig ajour på deres felt, men hvor det også er en forudsætning, at de kan indgå i tæt samarbejde med andre faggrupper. Både specialisering og samarbejde er en forudsætning for effektivt at kunne bidrage til at højne den nationale sikkerhed.

FE løser mange typer opgaver inden for en række specialiserede fagområder. Medarbejderne er afgørende for, at FE kan løse sine opgaver, og der er brug for personer med forskellige og ofte helt særlige kompetencer.

FE har en stor faglig spændvidde. Den største medarbejdergruppe er akademikerne, som samlet udgør knapt halvdelen af de ansatte.

En betydelig gruppe af FE's medarbejdere har en it-uddannelse eller anden teknisk baggrund, mens andre medarbejdere udfører administrative opgaver inden for økonomi, logistik og HR. FE lægger stor vægt på, at medarbejderne er gode til at samarbejde og dele viden på tværs af fagligheder og på tværs af organisationen.

Cirka 2/3 af FE's medarbejdere arbejder direkte med de efterretningsmæssige opgaver, mens de øvrige arbejder med udviklingsopgaver og støttefunktioner, ikke mindst i forhold til FE's indhentningssystemer.

FE's bevilling på finansloven var i 2015 på 675 mio. kr., og i 2016 var bevillingen 827 mio. kr.

I 2017 har FE en bevilling på 871 mio. kr.

Stigningen fra 2015 til 2016 og årene fremover skyldes, at partierne bag forsvarsforliget i 2015 besluttede, at FE skulle styrke indsatsen mod terror samt traf beslutningen om at etablere en militær CNO-kapacitet i FE. CNO står for "Computer Network Operations", og enheden skal kunne gennemføre både defensive og offensive operationer på netværk og it-systemer.

FE bruger en væsentlig del af bevillingen til lønninger. Derudover er der udgifter til almindelig drift af udstyr og bygninger.

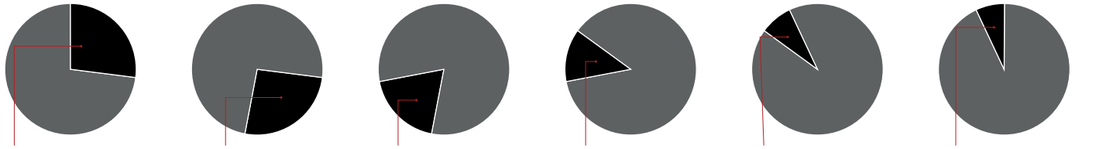
FE kan ikke oplyse, hvor mange ansatte vi har. Det skyldes, at de folk, der truer Danmark og danske interesser, ikke skal have indblik i omfanget af vores kapaciteter.

VIDENSORGANISATION

"Da FE er en all source-efterretningstjeneste, har vi alle indhentningsdiscipliner under ét tag."

MEDARBEJDERE FORDELT PÅ FE'S OVERORDNEDE FOKUSOMRÅDER*

* Fordelingen er ikke sammenlignelig med den angivne fordeling i FE Beretning 2013-2014 på grund af ny organisationsstruktur



*) CNO er under opbygning. Tallet er status ved udgangen af 2016. Når ressourcerne ikke anvendes til CNO, indgår de i løsning af FE's øvrige opgaver.

Alternativ rekruttering og kontakt med uddannelsesmiljøer

I 2015 og 2016 har FE intensiveret sin deltagelse på job- og uddannelsesmesser, hvor vi deltager med medarbejdere, som kan fortælle, hvordan det er at være ansat i FE.

Når vi rekrutterer, bruger vi i høj grad tests – både faglige og personlige – hvilket gør det lettere at finde de rette kandidater. I forhold til it-stillinger har vi også brugt såkaldte 'challenges' (nøddeknækkeropgaver) som en alternativ måde at finde de rette ansøgere (se f.eks. artikel om Hackerakademiet side 24). Ansøgerne fortæller os, at opgaverne giver et godt indtryk af, hvilke opgaver man som ansat i FE kommer til at arbejde med.

I 2017 har vi igangsat initiativer med fokus på øget samarbejde med studerende på de videregående uddannelser inden for it-området.

Hvis du overvejer et job i FE

Allerede når du søger arbejde i FE, vil din omgangskreds m.fl. kunne finde det interessant. Vi anbefaler derfor, at du beskytter dig selv og er diskret i forhold til, at du har søgt job hos FE. Det gælder både ansigt til ansigt med folk, du møder, men også på de sociale medier (f.eks. Facebook og LinkedIn).

At man skal være diskret omkring sit job er et generelt vilkår for at være ansat i en efterretningstjeneste. I det hele taget er der meget sikkerhed forbundet med at arbejde i en efterretningstjeneste. Det skal du som ansøger gøre dig bevidst om inden en eventuel ansættelse.

Hvis du får job i FE

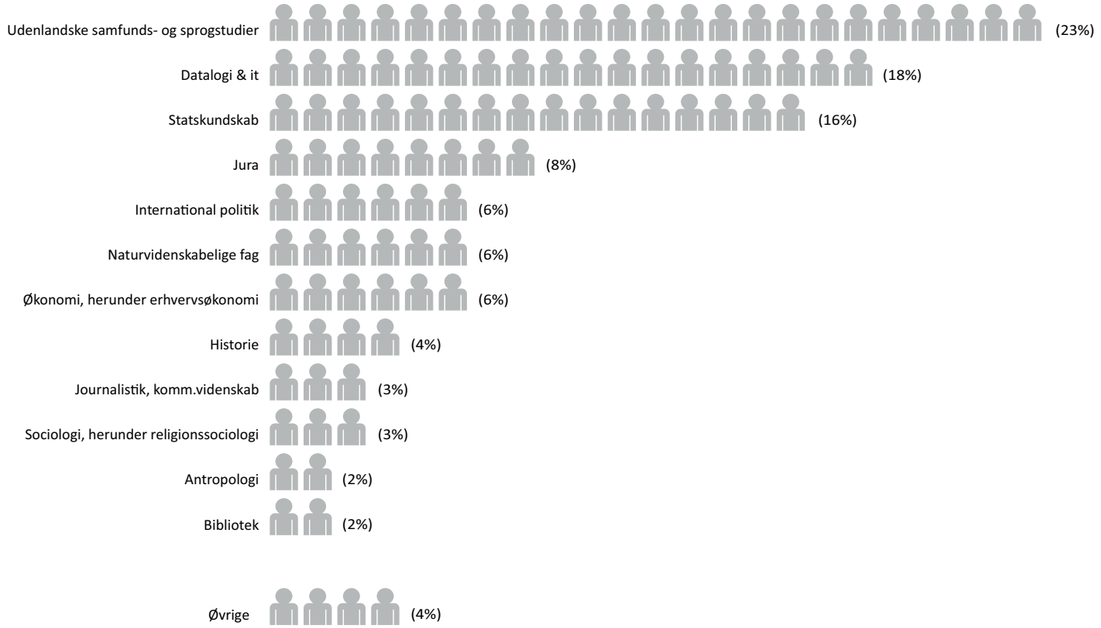
I 2015 og 2016 har FE haft stor opmærksomhed på at etablere og gennemføre fælles introforløb for nye medarbejdere med henblik på at give dem den bedst mulige start. FE benytter også en makkerordning, hvor man som nyansat i FE bliver tilknyttet en erfaren medarbejder, som kan bidrage til en god ankomst på arbejdspladsen.

Hvis du overvejer et job i FE, kan du holde øje med stillingsopslag på vores hjemmeside www.fe-ddis.dk, følge os på LinkedIn eller på portalen "Job i Staten".

Vi har til huse på Kastellet og i Holsteinsgade, som ligger på Østerbro, samt på Sandagergård på Amager. Et mindre antal stillinger ligger i Hjørring-området.

UDDANNELSESMÆSSIG BAGGRUND

FE's civile akademikere uden ingeniører under kontorchefniveau, i procent



"ASGER", ANALYTIKER

"Min opgave er blandt andet at afdække, hvem der er hvem i et netværk. Men jeg kan ikke udarbejde en troværdig analyse af en region uden også at have den viden om kultur, sprog og historie, som mine kolleger med lokalkendskab kommer med. Vores arbejde er komplekst og betinget af dybe, tværfaglige samarbejder. Denne dynamik betyder samtidig, at jeg føler, at jeg bliver klogere hver dag, jeg går på arbejde."

CHEF FOR HACKERAKADEMIET

"Vi lavede en gimmick som en del af kampagnen. Vi var klar over, at der ikke ville gå lang tid, før løsningen var offentlig kendt, men gåden betød, at vi kom ud til en anden type kandidater."

Hackerakademiet – rekruttering med skjulte budskaber

FE har mange hemmelige sider af sin organisation, og det er ikke alt, vi kan fortælle om stillingerne, før nyansatte begynder i FE. FE's HR-afdeling er dog på LinkedIn, og vi deltager også på relevante jobmesser, hvor vi taler med potentielle ansøgere om jobbet i FE. I 2016 prøvede FE kræfter med en ny rekrutteringsform. FE oprettede et hackerakademi, hvor udvalgte talenter fik 4½ måneders uddannelse af FE's egne specialister. De kandidater, der gennemførte uddannelsen, er efterfølgende blevet ansat i FE. På uddannelsen lærte de blandt andet, hvordan man forsvarer sig mod hackere samt egentlige hacker-teknikker.

At arbejde som hacker er et særligt job, der f.eks. kan betyde, at man kan være med til at afdække oplysninger om udenlandske terrorgrupper eller enkeltpersoner, der forsøger at rejse til Danmark for at gennemføre terrorangreb. Det er et job, der kræver både højt teknisk niveau og særlige personlige kompetencer. Rekrutteringsprocessen, der gik forud for optagelse på Hackerakademiet, var også speciel.

Skjulte udfordringer til kandidaterne

I stedet for et almindeligt stillingsopslag valgte vi at annoncere i et dagblad og på sociale medier. Annoncen havde et billede af en hætteklædt, ansigtsløs hacker og budskabet: "Har du det, der skal til for at blive en del af en hemmelig eliteenhed?".

Det rygtedes hurtigt, at der var et skjult budskab i grafikken på "hackerannoncen". Bag billedet af den hætteklædte person var der flere kodestumper, men en af disse ville springe i øjnene på rigtige specialister. Denne kode var en krypteret tekst, der dekrypteret gav et telefonnummer. Ringede man til det, lød der endnu en besked – efterfulgt af en hyletone, der korrekt afkodet gav adressen på en internetside med endnu en opgave, der kunne løses ved brug af særlige it-kompetencer.

FE har oplevet en stor interesse for Hackerakademiet. Der var over 100 personer, der søgte ind på akademiet, og FE fik det antal velkvalificerede kandidater, vi ønskede. Successen gentages derfor i 2017.

Hvorfor har FE brug for hackere – og hvorfor så mange?

Som efterretningstjeneste skal FE medvirke til at forebygge og modvirke trusler mod Danmark og danske interesser. Det gør vi blandt andet ved at indhente oplysninger om forhold i udlandet af betydning for Danmark. FE anvender flere forskellige indhentningsdiscipliner, hvoraf netværksindhentning er en af dem.

Vi bruger blandt andet netværksindhentning til at afdække mulige terrorangreb mod Danmark eller danske interesser.

FE forventer, at der i de kommende år vil blive stillet endnu højere krav til den teknologiske ekspertise. Vi forventer derfor, at behovet for it-specialister fortsat vil være højt, hvilket ligeledes skyldes beslutningen om en ny militær CNO-sektor (Computer Netværk Operationer), der skal understøtte Forsvaret i relation til cyberoperationer både defensivt og offensivt.

Medarbejdertyper

FE har mange forskellige typer af medarbejdere, der alle bidrager til produktionen af efterretninger. Det kan være teknikere og it-kyndige medarbejdere, der arbejder med FE's elektroniske indhentning af information og sikkerhed, føringsofficerer med særlige kontaktskabende egenskaber, som har kontakt til kilder, samt analytikere og bearbejdere med forskellige specialer. Her følger en række eksempler på de medarbejdertyper, der er direkte beskæftiget med FE's produktion af efterretninger:

DEN ELEKTRONISKE INDHENTER

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

NETVÆRKSINDHENTEREN OG -BESKYTTEREN

I FE er der flere måder at arbejde med it-netværk på med det formål at skaffe efterretninger og beskytte netværk. Netværksmedarbejderen har et dybt kendskab til internettets struktur, computere, programmer og applikationer. I Center for Cybersikkerhed (CFCS) arbejder eksempelvis malwareanalytikere med at opdage og analysere ondsindede programkoder for at finde ud af, hvem der står bag. Typisk har medarbejderne læst datalogi eller andre it-relaterede fag, mens andre er mere eller mindre selvlærde personer med usædvanlig flair for it.

TELEINGENIØREN

I CFCS fører teleingeniører tilsyn med informationssikkerhed og beredskab i telesektoren. Det er en dynamisk opgave, som kræver et godt kendskab til både telesektoren og eksisterende trusler mod telenettet. Teleingeniøren skal derfor have overblik og evne til at arbejde på tværs og opretholde en god dialog med telebranchen. Teleingeniøren skal være i stand til konstant at vurdere nye trusler og risici. Typisk har teleingeniøren en uddannelse som civilingeniør og har tidligere arbejdet hos et teleselskab eller en leverandør af teleudstyr.

FØRINGSOFFICEREN

Føringsofficeren, der også kaldes indhenteren, skaffer oplysninger fra menneskelige kilder, altså personer, som videregiver oplysninger, der ofte er af følsom karakter, til føringsofficeren. Føringsofficeren skal være god til at få alle typer af mennesker i tale og til at håndtere stress og uforudsete situationer. Han eller hun skal også være villig til at løbe en vis risiko, men uden at være dumdristig. Føringsofficerer kan have mange forskellige baggrunde. Mange har en videregående uddannelse, men det afgørende er ens personlige kvalifikationer.

BEARBEJDEREN

Bearbejderen, der også kaldes SIGINT-analytikeren, har veludviklede it-kundskaber og kan typisk et eller flere fremmedsprog på højeste niveau. Ud over at besidde gode it- og sprogkundskaber skal bearbejderen arbejde på tværs af de forskellige dele af efterretningsprocessen og skal derfor kunne favne flere faglige verdener. Bearbejderen skal være i stand til at overskue og arbejde med mange forskellige typer komplekse data og skal typisk arbejde i mange forskelligartede systemer indeholdende forskellige typer data. Bearbejderen udvælger, analyserer, oversætter og/eller formidler relevante efterretninger til brug for all source-analysen. Bearbejderen har i kraft af sin lange videregående sproglige og/eller samfundsvidenskabelige uddannelse stor kulturforståelse samt stort landekendskab og har ofte boet i eller arbejdet med et bestemt område gennem længere tid. Disse kompetencer bliver især bragt i spil i samarbejdet med FE's HUMINT-kapacitet og med all source-analytikerne.

ANALYTIKEREN

Analytikerens arbejdsområde er defineret geografisk (eksempelvis Syrien eller Rusland) eller emnemæssigt (eksempelvis terror- eller cybertrusler). Analytikeren, der også kaldes all source-analytikere, udfærdiger produkter til FE's kunder og partnere på basis af alle FE's discipliner. Desuden er det centralt for analytikeren at arbejde tæt sammen med FE's indhentere for at sikre, at indhentningen dækker FE's efterretningsbehov. Analytikeren skal både have et grundigt fagligt kendskab til sit område, men også have forståelse for indhentningens muligheder for nye efterretningsmæssige mål, hvorfor analytikerne og bearbejderne arbejder tæt sammen i dagligdagen. Analytikeren har typisk en samfundsvidenskabelig eller humanistisk akademisk uddannelse og har ofte også boet i og/eller arbejdet med et bestemt område gennem længere tid.

MILITÆRANALYTIKEREN

Den militære analytiker arbejder sammen med de civile analytikere, bearbejdere og indhentere inden for områder, der er opdelt både på geografi og på emner. Militæranalytikeren bidrager med sine militære kompetencer og står typisk for de dele af analysen, hvor der er tale om 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. Militæranalytikeren kan desuden have en særlig viden, der går på tværs af de tre værn i Forsvaret, eller specialistviden inden for et afgrænset område og varetager blandt andet kontakten til Forsvaret. Militæranalytikeren kan udsendes sammen med Forsvaret for at levere direkte efterretningsstøtte til de udsendte enheder.

"CECILIE", PARTNERANSVARLIG

"Min hverdag er meget afvekslende. Den ene dag er jeg på kontoret, den næste dag mødes jeg med en samarbejdspartner i udlandet for at undersøge nye muligheder i samarbejdet. Jeg er opmærksom på, hvem jeg står over for – så jeg bedst muligt kan repræsentere FE's interesser, når jeg er ude i verdenen."

Organisation

FE er overordnet organiseret i seks sektorer samt en ledelsesstab. De seks sektorer samt ledelsesstaben er yderligere opdelt i en række afdelinger, på nær Kontraterror, der består af sektioner. De fleste af FE's medarbejdere er placeret i FE's bygninger i Kastellet, på Amager og i Holsteinsgade på Østerbro. Derudover har FE indhentningsstationer på henholdsvis Amager og ved Hjørring.

FE's ledelsesgruppe består af chefen for FE og cheferne for hver af de seks sektorer samt chefen for Ledelsesstaben.

Ledelsesstaben
Ledelsesstaben understøtter chefen for FE samt FE's ledelsesgruppe med tværgående og strategiske opgaver og håndterer FE's presse og kommunikation. Staben varetager endvidere den overordnede kontakt til de nationale kunder samt forbindelsen til og koordination af samarbejdet med FE's udenlandske samarbejdspartnere. Desuden har staben ansvaret for de juridiske opgaver i FE.

Staben blev oprettet pr. 1. januar 2017.

Operation & Indhentningssektor
Sektoren er ansvarlig for at indsamle informationer og stille dem til rådighed for FE's analytikere. Sektoren omfatter tre forskellige indhentningsdiscipliner: Signals Intelligence (SIGINT), Computer Network Exploitation (CNE) og Human Intelligence (HUMINT).

Politisk & Militær Analysesektor
Sektoren har ansvaret for at bearbejde og analysere FE's informationer og stille dem til rådighed som efterretninger til FE's kunder inden for områderne politisk og militær analyse.
Politisk og Militær Analysesektor var tidligere en del af FE's samlede analysesektor, men blev i efteråret 2016 en selvstændig sektor.

Kontraterrorsektor
Sektoren varetager bearbejdning og analyse af terrorrelaterede informationer med henblik på at omdanne disse informationer til efterretninger til brug for FE's kunder, herunder navnlig også PET.

Kontraterrorsektoren var tidligere en del af FE's samlede analysesektor, men blev i efteråret 2016 en selvstændig sektor.

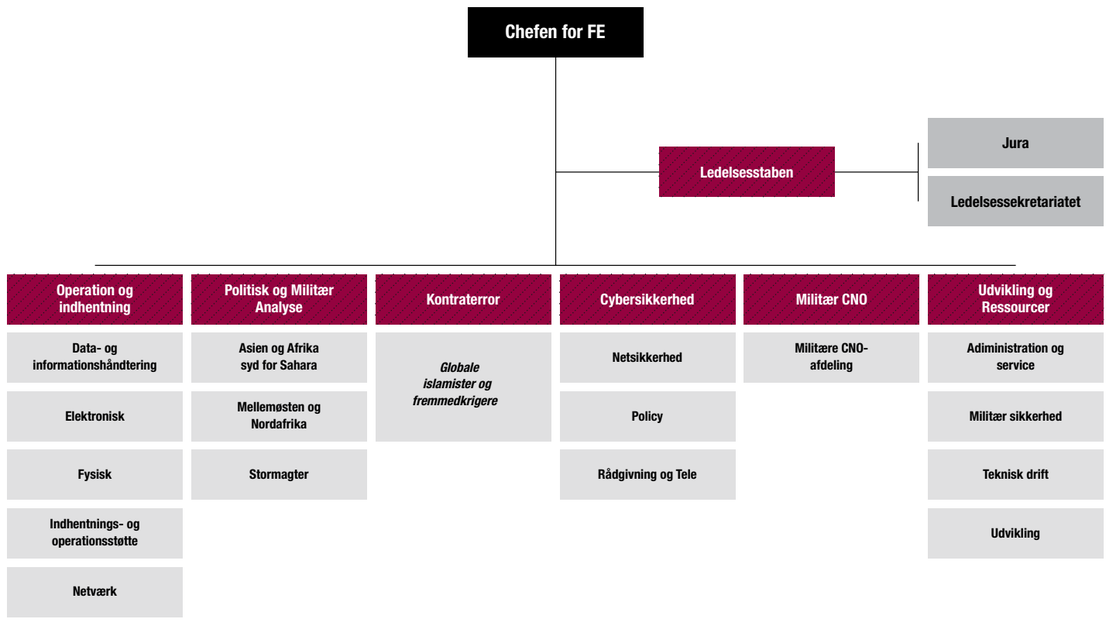
Center for Cybersikkerhed
Centeret varetager opgaverne som national it-sikkerhedsmyndighed, netsikkerhedstjeneste og kompetencecenter på cybersikkerhedsområdet.

Militær Computer Network Operations (CNO) sektor
Sektoren har ansvaret for at understøtte Forsvaret i relation til cybernetværksoperationer både defensivt og offensivt.

Sektoren blev oprettet i efteråret 2016 som følge af den nuværende politiske aftale på forsvarsområdet, hvor det er besluttet at etablere en militær CNO-kapacitet.

Udviklings- og Ressourcesektor
Sektoren har ansvaret for FE's udviklings- og driftsopgaver, herunder teknisk drift og administration. Sektoren har endvidere ansvaret for at lede og kontrollere den militære sikkerhed inden for Forsvarsministeriets område.

ORGANISATIONSDIAGRAM



Produkter og kunder

Den efterretningsmæssige produktion til vores kunder er en af FE's kerneopgaver og det synlige resultat af FE's efterretningsarbejde.

FE's varslinger drejer sig ofte om højaktuelle forhold, men vi arbejder også med mere langsigtede strategiske analyser og vurderinger af tendenser, der kan udvikle sig til trusler mod Danmark og danske interesser.

Produkterne udarbejdes ud fra FE's oplysninger om udvalgte landes og regioners politiske, økonomiske og militære forhold og om prioriterede tematiske områder som terror- og cybertrusler. Det gør os i stand til at informere og varsle vores kunder om forskellige staters og andre aktørers hensigter, kapaciteter og adfærd. Informationer af denne type øger regeringens indsigt i de pågældende landes hensigter og adfærd og bidrager til, at Danmark som suveræn stat kan føre sin udenrigs-, sikkerheds- og forsvarspolitik på grundlag af selvstændige, nationale efterretningsmæssige vurderinger.

Produkterne indgår som regel som en del af et politisk beslutningsgrundlag, eksempelvis for folketingsbeslutninger om indsættelse af danske militære bidrag i forbindelse med internationale operationer.

Specielt i forhold til terror- og cybertrusler skal FE ikke blot kunne varsle om, men også bidrage til at modvirke angreb mod Danmark og danske interesser. Dette stiller naturligvis særligt store krav til produkternes rettidighed og præcision.

FE sender efterretningsrapporter til sine kunder mange gange om ugen. Produkterne omfatter både skriftlige rapporter, mundtlige briefinger og operative indsatser.

De fleste af FE's produkter er klassificerede. For at få adgang til disse informationer skal læseren derfor være sikkerhedsgodkendt til den relevante klassifikationsgrad, teksten er klassificeret til. FE skriver enkelte ikke-klassificerede situations- og trusselsvurderinger, som publiceres på FE's hjemmeside.

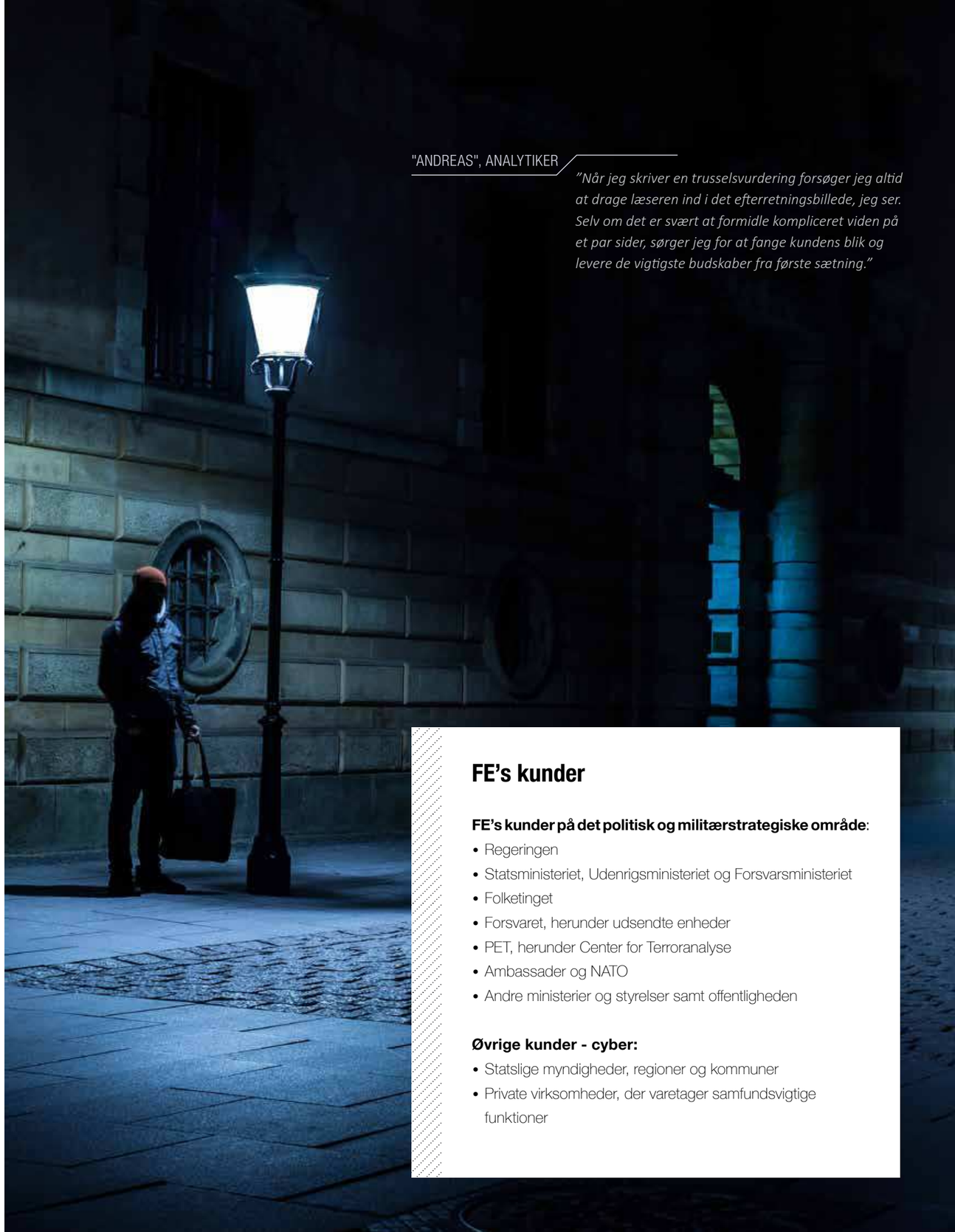
FE lægger vægt på at være i tæt dialog med kunderne på alle niveauer. Det giver kunderne mulighed for at stille uddybende spørgsmål og komme med ønsker til FE's fremtidige rapportering. Dialogen med kunderne foregår direkte med de fagpersoner i FE, som har den specifikke viden, som kunderne efterspørger. Derudover gennemfører FE årligt kundemøder, hvor samarbejdet og prioriteringen af FE's efterretningsmæssige fokusområder drøftes. Kundernes behov er afgørende for FE's prioriteringer af fokusområder og har derfor også betydning for efterretningskredsløbet (se side 15).

Læs mere om FE's og Center for Cybersikkerheds produkter på hjemmesiderne: www.fe-ddis.dk og www.cfcs.dk

Årlige brugertilfredshedsundersøgelser

FE udarbejder hvert år en brugertilfredshedsundersøgelse blandt vores største kunder. Spørgsmålene i undersøgelsen handler om produkternes rettidighed, relevans og kvalitet i forhold til kundernes behov. Resultaterne fra undersøgelserne har været positive med en score på ca. 4 ud af 5 mulige.

FE bruger undersøgelserne som grundlag for en dialog med kunderne for derigennem at optimere vores produkter i forhold til kundernes behov.



"ANDREAS", ANALYTIKER

"Når jeg skriver en trusselsvurdering forsøger jeg altid at drage læseren ind i det efterretningsbillede, jeg ser. Selv om det er svært at formidle kompliceret viden på et par sider, sørger jeg for at fange kundens blik og levere de vigtigste budskaber fra første sætning."

FE's kunder

FE's kunder på det politisk og militærstrategiske område:

- Regeringen
- Statsministeriet, Udenrigsministeriet og Forsvarsministeriet
- Folketinget
- Forsvaret, herunder udsendte enheder
- PET, herunder Center for Terroranalyse
- Ambassader og NATO
- Andre ministerier og styrelser samt offentligheden

Øvrige kunder - cyber:

- Statslige myndigheder, regioner og kommuner
- Private virksomheder, der varetager samfundsvigtige funktioner

Trusler mod Danmark og danske interesser

Danmark står over for et stadigt mere komplekst trusselsbillede. I løbet af 2015 og 2016 er der sket en markant udvikling på flere områder. Det gælder f.eks. terrortruslen mod Danmark fra militante islamistiske grupper, Ruslands politiske og militære aktiviteter regionalt og globalt samt den stadigt stigende cybertrussel. FE's arbejde handler om at skabe et klart efterretningsbillede af de trusler, som Danmark står over for, så regeringen kan træffe beslutninger, der kan imødegå truslerne.

FE's efterretningsprodukter skal være præcise, pålidelige og rettidige og skal kvalificere de beslutninger, som Statsministeriet, Udenrigsministeriet, Forsvarsministeriet, Forsvaret og andre centrale myndigheder skal træffe (se Produkter og kunder s. 32). FE rapporterer til en snæver kreds af kunder om en række landes hensigter, kapaciteter og adfærd. FE følger ligeledes netværk, grupper og enkeltpersoner, der kan udgøre en trussel mod Danmark.

Denne viden bringer vi ud til offentligheden i FE's årlige publikation Efterretningsmæssig Risikovurdering, hvor de efterretningsmæssige vurderinger skrives i en ikke-klassificeret version til offentligheden. I Risikovurderingen vurderer FE udviklingen i en række lande og konfliktområder.

Kort om de største trusler

Terrorbekæmpelse er et prioriteret indsatsområde i Danmark og mange lande i Vesten. Det er lykkedes for personer med tilknytning til militante islamistiske grupper at gennemføre både større og mindre terrorangreb i Vesten, herunder i Europa, i løbet af 2015 og 2016. For at imødegå truslerne har der været fokus på i endnu højere grad at styrke samarbejdet om terrorbekæmpelse mellem FE og PET. Desuden har FE med nye regler i FE-loven fået mulighed for målrettet at indhente oplysninger om danskere, der befinder sig i udlandet, hvis FE har bestemte grunde til at formode, at de pågældende deltager i aktiviteter, der kan indebære eller forøge en terrortrussel mod Danmark og danske interesser. Medfører en sådan indhentning, at der sker indgreb i meddelelseshemmeligheden, skal FE indhente en retskendelse. Denne nye beføjelse giver FE bedre mulighed for at bidrage til at forebygge terrorangreb i Danmark.

FE har de seneste år i stigende grad prioriteret arbejdet med Ruslands politiske og militære aktiviteter, da disse har betydning for den internationale stabilitet og sikkerhed. Det gælder ikke mindst i Danmarks nærområde. Rusland gennemfører militær opbygning og modernisering, og Østersøregionen er blevet et væsentligt friktionsfelt mellem Rusland og NATO. Rusland vil ikke risikere en direkte militær konfrontation med NATO, men vil i de kommende år fortsætte med at udgøre en betydelig sikkerhedspolitisk udfordring for Vesten og Danmark.

Cyberforsvar er ligeledes et prioriteret område i FE. Der er en meget høj cybertrussel mod Danmark, særligt fra cyberspionage, men også fra cyberkriminalitet. Hertil kommer en potentiel trussel fra fremmede stater, som benytter cyberangreb til at forsøge at påvirke meningsdannelsen. De metoder og teknikker, der anvendes, er blevet stadigt mere avancerede. Truslen fra destruktive cyberangreb mod Danmark er lav, men vil kunne stige i forbindelse med eksempelvis en skærpet politisk eller militær konflikt, hvor Danmark deltager.

Terrorbekæmpelse

Målet med FE's indsats på terrorområdet er at forebygge og modvirke terrorangreb mod Danmark og danske interesser i udlandet samt at indgå i den internationale kamp mod terror. Denne indsats har i 2015 og 2016 budt på et intensiveret samarbejde mellem FE og Politiets Efterretningstjeneste (PET) samt en understøttende indsats til det danske bidrag til koalitionen mod ISIL. FE har i 2015 og 2016 bidraget til at identificere og modvirke trusler og angrebsplaner mod Danmark og andre lande fra terrornetværk i udlandet. FE har samtidig hjulpet PET med løbende at vurdere truslen fra danskere, der er udrejst for at kæmpe for ISIL, samt varslet udsendte danskere om terrortruslen i de områder, de er udsendt til.

Terrortruslen mod Danmark og danske interesser i udlandet fra personer tilknyttet militante islamistiske grupper er alvorlig. I løbet af de seneste år har militante islamistiske grupper med tilknytning til ISIL etableret sig i flere lande i Mellemøsten, Afrika og Asien. I særligt Syrien og Irak har ISIL tiltrukket militante islamister fra store dele af verden, herunder Danmark. ISIL og grupper med tilknytning til ISIL er dog i dag under pres flere steder og vil ikke på sigt kunne fastholde de områder, som de kontrollerer. Derimod har grupper med tilknytning til al-Qaida formået at fastholde deres tilstedeværelse i flere områder i Mellemøsten, Afrika og Asien. Ud over den generelle terrortrussel fra især ISIL og al-Qaida vil flere lande i Mellemøsten, Central- og Sydasien samt Afrika de næste år opleve, at militante islamister vender tilbage fra konfliktområderne. Det vil skærpe terrortruslen i disse områder yderligere. Den dynamiske forandring af eksisterende konfliktzoner og fremkomsten af nye opholdssteder for militante islamistiske netværk stiller generelt set store krav til FE's evne til at afdække, varsle og modvirke de nye trends og specifikke terrortrusler mod Vesten, herunder Danmark.

Terrorbekæmpelse er et prioriteret indsatsområde i Danmark og mange lande i Vesten. Til trods for dette er det lykkedes for personer med tilknytning til militante islamistiske grupper at gennemføre både større og mindre terrorangreb i Vesten i løbet af 2015 og 2016. Disse terrorangreb understreger nødvendigheden af, at FE fortsat har daglig fokus på at forstå, vurdere og imødegå angrebsplanlægning mod Vesten. Den komplekse trussel fra kombinationen af internationale terrornetværk og personer, som udfører angreb på egen hånd, og den accelererende teknologiske udvikling nødvendiggør en bred og omstillingsparat tilgang til terrorbekæmpelse. Denne tilpasning har FE haft stort fokus på i 2015 og 2016, hvor bl.a. terrorpakken har givet nye muligheder i FE.

Terrorbekæmpelse foregår på flere niveauer. Den direkte forebyggende indsats varetages i Danmark af PET. FE's indsats på ter-

En kompleks terrortrussel

Terrortruslen fra globale terrorgrupper som al-Qaida og især ISIL er de sidste par år blevet yderligere kompleks. Det skyldes bl.a. en øget produktion og tilgængelighed af voldelig propaganda, som opfordrer enkeltpersoner til at udføre terrorhandlinger i Vesten. I 2015-2016 har der været adskillige eksempler på alvorlige terrorangreb i Vesten udført af enkeltpersoner med sympati for globale islamistiske terrorgrupper som ISIL. Samtidig har globale terrorgrupper fortsat fokus på at gennemføre koordinerede og opsigtsvækkende terrorangreb i Vesten, som involverer flere gerningsmænd og længere tids planlægning. Arbejdet med at afdække og forhindre begge typer af terrorangreb, hvor tidsperioden fra idé til handling kan være alt fra få timer til flere måneder, udgør en særlig udfordring for efterretnings- og sikkerhedstjenester og understreger behovet for tæt samarbejde mellem FE og PET.

Terrorpakken

Som følge af aftalen om terrorpakken, der blev indgået i april 2015 efter terrorangrebene i Paris og København, fik FE en ekstra bevillig på samlet 415 millioner kr. frem til 2018 til at styrke indsatsen mod terror. FE har siden styrket arbejdet med at imødegå terror på en række områder, herunder:

- Kapaciteten til fysisk og elektronisk efterretningsindhentning
- Evnen til at behandle indhentede informationer
- Evnen til at opdage og forfølge nye terrortrusler
- Internationalt samarbejde
- Indsatsen mod cyberterror
- Samarbejdet med PET

Initiativer inden for alle de pågældende områder er sket ved tiltag såsom øgede it-investeringer og tilgang af nye medarbejdere. Formålet med initiativerne har været at øge FE's operative kapaciteter samt styrke FE's evne til at modvirke terrortruslen.

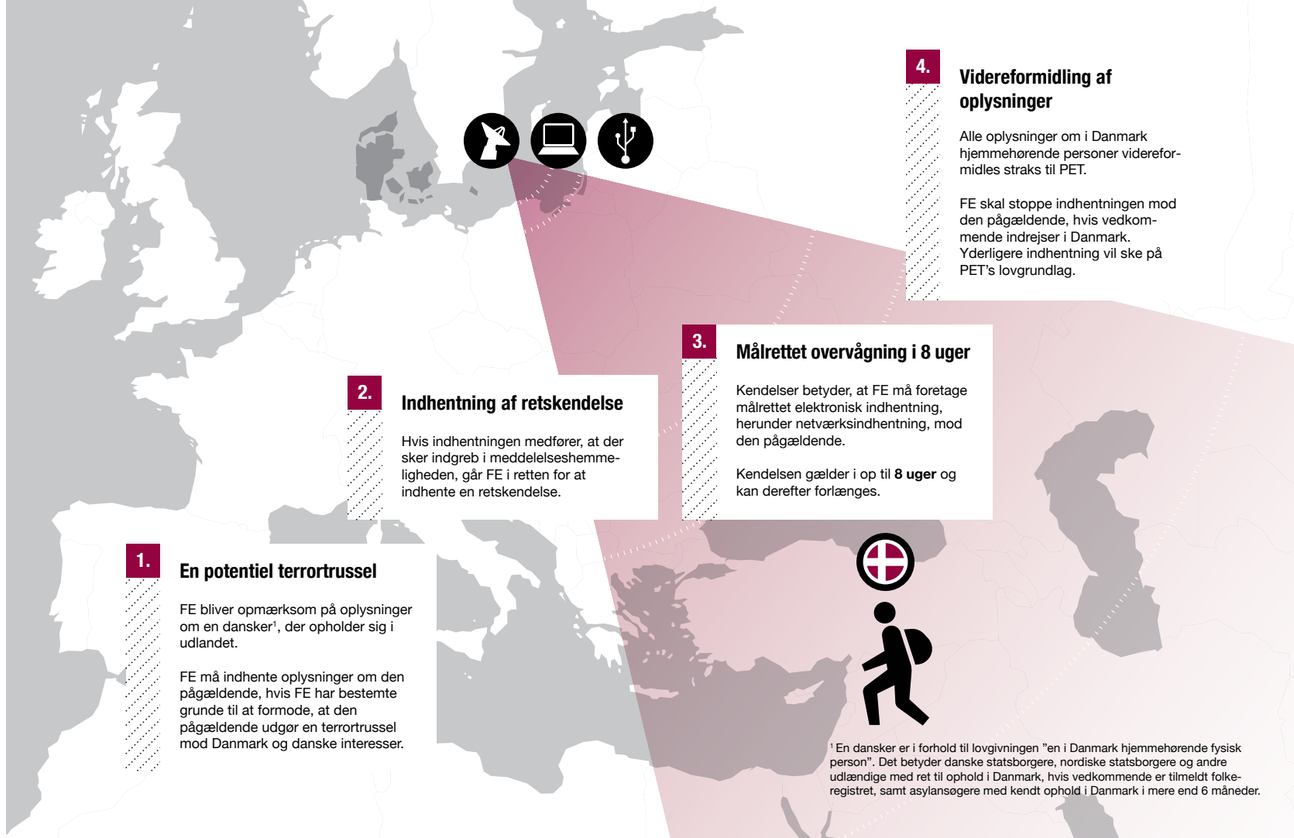
Effekten af initiativerne kan i særlig grad ses for de tiltag, der er koblet til de tre førstnævnte områder. Det er i særlig grad FE's indhentning og analysekapacitet rettet mod Syrien og Irak, der er blevet styrket. Det har betydet en øget kvalitativ og kvantitativ varsling til PET og vores samarbejdspartnere. I takt med at alle tiltag bliver implementeret, forventes en fortsat styrkelse af FE's indsats mod terror i de kommende år.

roområdet består i høj grad af at varsle relevante myndigheder om terrortrusler, der udgår fra udlandet mod Danmark og danske interesser, så myndighederne kan træffe de nødvendige forebyggende tiltag og forholdsregler. Dette gælder for eksempel varsling af Udenrigsministeriet til brug for deres rejsevejledninger eller til brug for sikkerhedsforanstaltninger på danske ambassader. Det gælder i særdeleshed også videndeling og udveksling af efterretninger med PET om trusselsudviklingen i udlandet med potentiel betydning for Danmark. FE samarbejder også med andre landes efterretnings- og sikkerhedstjenester om truslen mod Danmark og udlandet.

Terrorgrupper har ofte netværk og sympatisører i flere lande. Samtidig har truslen fra et stigende antal udrejste ekstremister fra vestlige lande – de såkaldte fremmedkrigere – udgjort en voksende udfordring, også for Danmark. Det gælder f.eks., når personer bosiddende i Danmark rejser til udlandet for at modtage militant træning eller deltage i kamphandlinger eller terrorangreb og siden returnerer til Danmark. Disse grænseoverskridende terrornetværk og truslen, der udgår fra dem og især fra danske fremmedkrigere, har givet anledning til ændret lovgivning i Danmark. Tidligere kunne alene politiet, og i disse sager navnlig PET, få retskendelse til f.eks. indgreb i meddelelseshemmeligheden mod danske statsborgere. FE kunne efterfølgende efter anmodning fra PET indhente informationer om disse personer i udlandet. Siden december 2015 har også FE fået mulighed for at indhente kendelser i retten med henblik på indgreb i meddelelseshemmeligheden mod danske statsborgere, som opholder sig i udlandet. Dette kan FE gøre, hvis personen opholder sig i udlandet, og retten er enig i, at der er bestemte grunde til at formode, at den pågældende deltager i aktiviteter, der kan indebære eller udgøre en øget terrortrussel mod Danmark og danske interesser. Lovændringen giver dermed FE mulighed for at foretage målrettet indhentning af oplysninger vedrørende disse personer, så FE i en tidlig efterretningsmæssig fase kan løse sine opgaver med bl.a. at forebygge og modvirke trusler mod Danmark og danske interesser.

EFTERRETNINGSMÆSSIG RISIKOVURDERING 2016

"Mindst 6.000 personer fra Vesten er siden 2012 rejst til konflikten i Syrien og Irak. Det er ikke alle, som har deltaget i væbnet kamp, men en stor andel kæmper eller har kæmpet sammen med ISIL eller andre militante islamistiske grupper. Det er muligt, at antallet af kamperfarne ISIL-ekstremister, som rejser tilbage til Vesten, vil blive øget, i takt med at ISIL kommer under yderligere pres i Syrien og Irak. På grund af den militante træning og voldsparathed, som mange af disse personer har tilegnet sig, vil de udgøre en alvorlig terrortrussel mod Vesten i mange år."



Samarbejde med PET fører til bedre terrorbekæmpelse

PET og FE har hvert sit lovgrundlag og i udgangspunktet hvert sit fokus. De to tjenesters arbejdsområder er ikke desto mindre nært forbundne. Dette gælder ikke mindst i forhold til bekæmpelse af terrorisme, herunder indsatsen for at modvirke den trussel mod Danmark og danske interesser, som bl.a. de såkaldte danske 'fremmedkrigere' udgør.

De tæt forbundne arbejdsområder er bl.a. afspejlet i henholdsvis FE- og PET-loven, der giver de to tjenester en særlig adgang til at udveksle oplysninger.

FE og PET arbejder løbende på at styrke samarbejdet og finde måder, hvorpå tjenesterne i fællesskab kan højne indsatsen for sikkerheden i Danmark. Som en del af det samarbejde har FE en kontraterroranalytiker fast udstationeret i PET. Udstationeringen går på skift mellem terroreksperter i FE, så alle relevante analytikere indgår i ordningen. Gennem et godt kendskab til hinandens rutiner, systemer og behov kan de to tjenesters løbende samarbejde og udveksling af oplysninger styrkes i overensstemmelse med de lovgivningsmæssige rammer herfor.

FE's udstationerede medarbejder har sin dagligdag i PET i en periode og lærer dermed, hvordan man bedst byder ind med sin viden, så den spiller sammen med PET's behov. PET har stor viden om det militante islamistiske miljø i Danmark, men i det øjeblik personen eller gruppen udrejser eller kommer i kontakt med grupper i udlandet, kan FE byde ind med sin viden. FE kan også byde ind med oplysninger fra udenlandske partnere, som af gode grunde kan ligge inde med stor viden om f.eks. en danskers kontakter i Syrien eller Irak.

Med dette samarbejde bliver PET og FE bedre til at skabe et klart billede af et potentielt angreb, og hvad der skal gøres for at modvirke en terrorhandling mod Danmark eller danske interesser i udlandet.

Når FE-medarbejderen ikke længere er i PET, er der opbygget en god forståelse for, hvordan FE's viden bringes bedst muligt i spil og støtter PET's indsats.

Tilsynet med Efterretningstjenesterne fører tilsyn med både FE og PET og kontrollerer bl.a., at de to tjenesters udveksling af oplysninger sker inden for rammerne af henholdsvis FE- og PET-loven.

ANALYTIKER, "JONAS"

"Efter jeg har været i PET, kan jeg nemmere bringe min FE-viden om 'terrortruslen fra udlandet' i spil for PET. Og jeg kan også hjælpe mine kollegaer med at give dem den rette kontaktperson, så vores viden kommer hurtigt frem. I terrorsager er tid altid en afgørende faktor."

Rusland

FE har i 2015-2016 i stigende grad prioriteret Ruslands politiske og militære dispositioner og hensigter. Ruslands adfærd har stor betydning for den internationale stabilitet og sikkerhed, herunder ikke mindst i Danmarks nærområde, og Rusland vil også i de kommende år fortsætte med at være en betydelig sikkerhedspolitisk udfordring for Vesten og Danmark.

Rusland og Østersøen

FE har fulgt Ruslands adfærd i Østersøregionen, hvor Rusland gennem de seneste år er begyndt at intensivere sine forsøg på at påvirke den strategiske balance til Ruslands fordel.

Rusland er i 2016 begyndt at udmønte en række planlagte militære tiltag, som er reaktioner på det stærkt forværrede forhold til Vesten, tydeligst den påbegyndte opbygning af de landmilitære styrker i det vestlige Rusland. Hertil kommer igangværende militær modernisering i blandt andet Østersøregionen, som er blevet et væsentligt friktionsfelt mellem Rusland og NATO. Det gælder især Baltikum. Rusland vil fortsat forsøge at svække troværdigheden af NATO's kollektive forsvarsforpligtelse over for netop de tre baltiske lande. Den øgede militære kapacitet vil kunne udgøre en trussel mod NATO's muligheder for at forstærke de tre baltiske lande med styrker i tilfælde af en eskalerende krise.

Selv om det er FE's vurdering, at Rusland ikke vil risikere en direkte militær konfrontation med NATO, vil der fortsat være risiko for fejlopfattelser og misforståelser. Det skyldes ikke mindst Ruslands mistro til NATO og den russiske risikovillighed. Det bidrager samlet til større usikkerhed, herunder i Østersøregionen.

Derfor arbejder FE målrettet for at få viden om Ruslands hensigter over for Danmark og lande i Danmarks nærområde.

Russiske påvirkningskampagner

FE har i 2016 øget sit fokus på Ruslands forstærkede påvirknings- og indflydelseskampagner i Vesten. Inden for de seneste få år har både Ruslands mål og midler udviklet sig fra primært gennem massemedier at påvirke synet på Rusland til gennem en bredere vifte af påvirkningskanaler også at skulle påvirke udviklingen internt i EU-landene, udviklingen i USA og forholdet mellem vestlige lande.

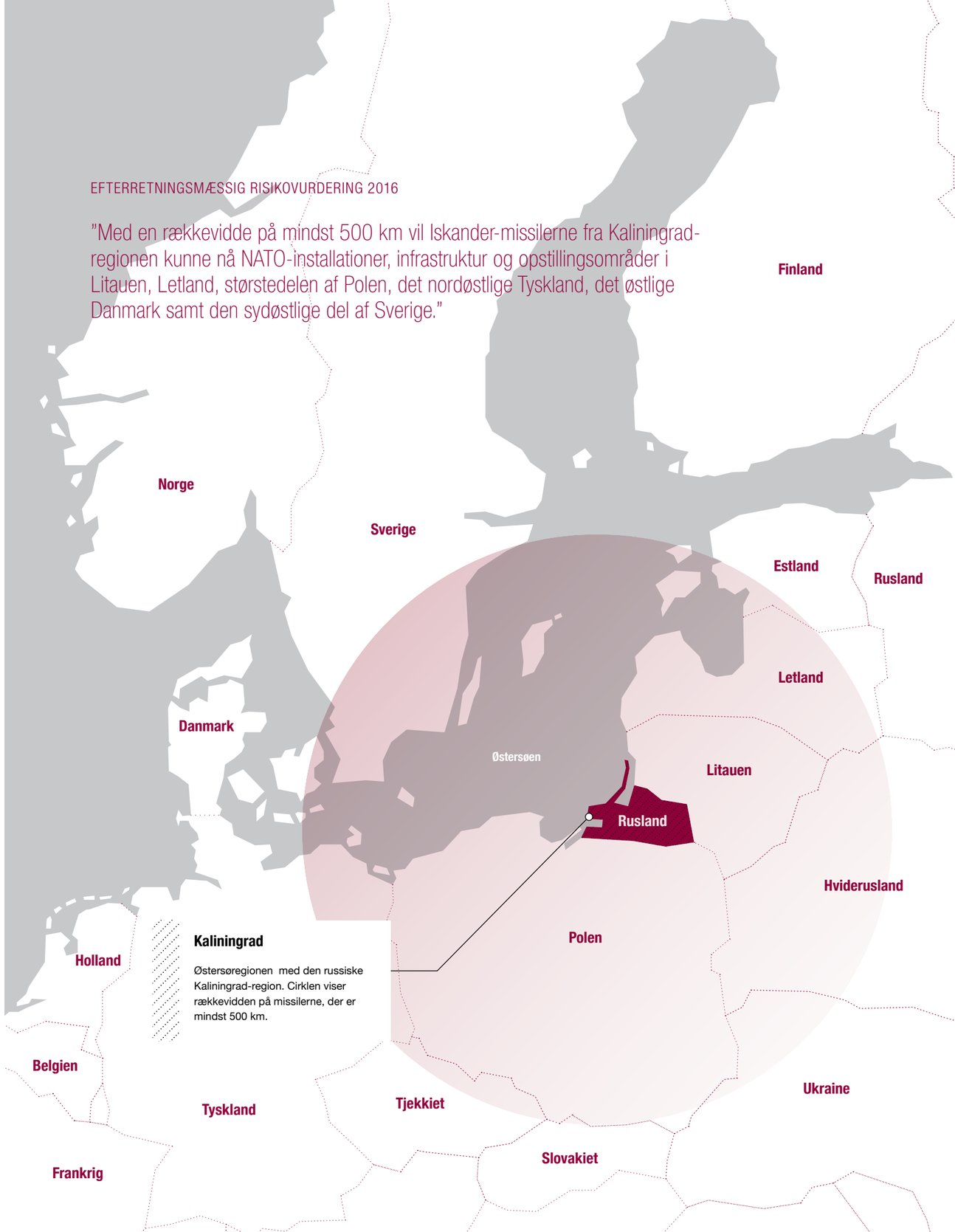
Ruslands rolle i Syrien

FE har også haft et stort fokus på Ruslands rolle i Syrien i 2015 og 2016. Det gælder i høj grad de russiske militære aktiviteter, som har været afgørende for, at det syriske styre har kunnet gå i offensiven mod den væbnede opposition. Men det gælder også Ruslands politiske engagement, hvor det er lykkedes for Rusland at placere sig på niveau med USA som en central og uomgængelig part i de internationale forhandlinger om den syriske konflikt.

Påvirkningskampagner

Rusland anvender en lang række virkemidler til at påvirke meningsdannelsen i vestlige lande. Det sker blandt andet gennem russiske statskontrollerede medier rettet mod et vestligt publikum, men det sker også gennem russiske tænketanke og forskningsinstitutioner og uofficielle mediekanaler som gratis nyhedsportaler, bloggere og kommentatorer, som foregiver at være uafhængige. Rusland anvender desuden målrettet sociale medier til at påvirke holdningsdannelsen i vestlige lande. Hertil kommer sandsynligvis også hacking og selektiv offentliggørelse af informationer, der også skal påvirke meningsdannelsen.

"Med en rækkevidde på mindst 500 km vil Iskander-missilerne fra Kaliningrad-regionen kunne nå NATO-installationer, infrastruktur og opstillingsområder i Litauen, Letland, størstedelen af Polen, det nordøstlige Tyskland, det østlige Danmark samt den sydøstlige del af Sverige."



Cybertrusler

Cybertrusler er et af FE's højst prioriterede områder, og FE har i 2015-2016 yderligere opbygget kapacitet til at kunne imødegå den stadigt stigende cybertrussel fra især statslige og statsstøttede aktører. FE har også et tæt samarbejde med nationale og udenlandske samarbejdspartnere, hvor vi udveksler oplysninger om cyberspionage og cyberangreb.

Der er en meget høj cybertrussel mod Danmark, særligt fra cyberspionage, men også fra cyberkriminalitet. Hertil kommer en potentiel trussel fra fremmede stater, som benytter cyberangreb til at forsøge at påvirke meningsdannelsen i andre lande. Cybertruslen er en særdeles aktiv trussel, der har både sikkerhedspolitiske og samfundsøkonomiske konsekvenser for Danmark.

Cyberspionage mod offentlige og private mål udgør den alvorligste cybertrussel mod Danmark. Truslen kommer primært fra stater eller statsstøttede aktører, hvis interesse i at spionere mod Danmark kan være både strategisk, politisk og kommerciel. FE har gennem de seneste år konstateret flere angreb fra stater, og der er kontinuerlige forsøg på at kompromittere både danske myndigheder og virksomheder. Cyberkriminalitet er ligeledes stigende i omfang og kompleksitet og udgør en meget høj trussel mod både myndigheder, virksomheder og borgere. I 2016 har FE's Center for Cybersikkerhed (CFCS) udarbejdet 14 offentliggjorte trusselsvurderinger og en række klassificerede efterretningsvurderinger på cyberområdet.

Samarbejdsfora

For at skabe øget kendskab til cybertruslen og styrke den proaktive dialog om cyberforsvar har CFCS i 2015-2016 udbygget centerets relationer med interessenter og samarbejdspartnere i Danmark.

CFCS har således i 2015-2016 gennemført en række møder i Den Tværministerielle Kontaktgruppe vedrørende Cybersikkerhed, som er et netværk for ministeriers topledelser, og i Det Strategiske Samarbejdsforum om Cybersikkerhed, hvis medlemmer omfatter en lang række samfundsvigtige virksomheder fra den private sektor samt brancheorganisationer på ledelsesniveau.

CFCS har yderligere gennemført fælles konferencer for medlemmerne af de to interessentfora med henblik på at styrke det offentlige-private samarbejde. I 2015 etablerede CFCS yderligere to tekniske samarbejdsfora, som adresserer cybersikkerhed på et teknisk niveau og cybersikkerhed i mainframe installationer. Sidstnævnte forum, som var en udløber af sikkerhedshændelsen hos it-leverandøren CSC, blev nedlagt ultimo 2016 efter fælles overenskomst mellem deltagerne.

CFCS lægger vægt på at have denne åbne og tillidsfulde dialog med bl.a. statslige myndigheder, brancheorganisationer og større virksomheder inden for de sektorer, der beskæftiger sig med samfundsvigtige funktioner. At have en løbende dialog er vigtigt for at understøtte et højt informationssikkerhedsniveau i Danmark.

Den frivillige underretningsordning

Den frivillige underretningsordning er et supplement til de obligatoriske underretningsordninger for offentlige myndigheder og for telesektoren. At dele oplysninger om sikkerhedsbrud kan umiddelbart opfattes som en unødig blottelse af et internt anliggende og potentielt forretningskritiske forhold. Den frivillige underretningsordning er derfor undtaget fra aktindsigt i henhold til Lov om net- og informationssikkerhed, der trådte i kraft den 1. juli 2016. Siden ordningen trådte i kraft, har CFCS modtaget ni underretninger, som bl.a. vedrører DDoS-angreb, phishingforsøg og CEO-fraud-mails.

Viden om cyberangreb

Ud over at være national it-sikkerhedsmyndighed er CFCS kompetencecenter på cybersikkerhedsområdet. CFCS udarbejder løbende vejledninger inden for aktuelle områder med det formål at understøtte en forebyggende indsats samt at minimere uønskede konsekvenser, når der sker cyberangreb. CFCS udarbejder tillige undersøgelsesrapporter i forbindelse med afdækning af større cyberangreb, så offentlige myndigheder og virksomheder kan drage nytte af erfaringerne, herunder udarbejde tiltag med henblik på øget beskyttelse. I 2015-2016 rykkede CFCS i gennemsnit ud med et team en til to gange om måneden, og CFCS håndterede i samme periode mere end 1000 sikkerhedshændelser og udsendte mere end 200 varslinger.

Når FE's Center for Cybersikkerhed rykker ud

I perioden 2015-2016 blev to danske mellemstore it-hosting-virksomheder udsat for cyberangreb. Begge virksomheder udbyder forskellige it-løsninger såsom hosting, konsulentbistand, udvikling og drift og har offentlige myndigheder som kunder.

Hvad sker der ved cyberangreb, og hvordan hjælper CFCS?
Da CFCS i løbet af 2016 blev opmærksom på, at de to danske it-hosting-virksomheder muligvis kunne være blevet kompromitteret af en statsstøttet aktør, kontaktede centeret de to virksomheder med henblik på at yde assistance i sagen. Indledningsvis indhentede CFCS samtykke, der gav centeret adgang til data, der skulle analyseres. På baggrund af angrebenes karakter nedsatte CFCS et udrykningshold, et såkaldt Incident Response Team (IRT).

Generelt er sammensætningen af et IRT i forbindelse med en udrykning ikke fast, men etableres ud fra operative hensyn fra sag til sag. Der trækkes på et vidt spænd af kompetencer, men typisk vil et IRT som minimum bestå af netværksspecialister, forensics-eksperter, malwareanalytikere og incident managers.

Når IRT'en er hos virksomheden, er den første opgave – sammen med virksomhedens tekniske personale – at sørge for "førstehjælp" og "brandslukning" i forhold til de påvirkede systemer. IRT'en skal både minimere og vurdere skadens omfang, ligesom det er tilsvarende vigtigt at forhindre et avanceret cyberangreb (APT-angreb) i at sprede sig og gøre skade i det omgivende samfund. Her kan det i visse tilfælde være nødvendigt at isolere dele af en virksomheds infrastruktur – eller helt at genetablere den – for at undgå, at malware spreder sig yderligere eller hackere trænger dybere ind.

I den konkrete sag har IRT'ens tekniske specialister fundet to typer APT-malware på de kompromitterede maskiner. Aktøren har brugt to forskellige typer malware i sit angreb, der blandt andet kan have været brugt til at fjernstyre kompromitterede maskiner og til at stjæle loginoplysninger eller anden følsom information. Begge typer malware er designet til at gøre dem svære at finde, når de kører på en kompromitteret maskine. Endvidere er dele af deres funktionalitet skjult for at gøre det svært at finde ud af præcis, hvordan de fungerer, hvis de skulle blive fundet alligevel. Ud over den APT-relaterede malware er der også fundet flere typer malware, der bruges til almindelig berigelseskriminalitet eller andet misbrug. CFCS' analyse af de kompromitterede computere viser, at aktøren aktivt har forsøgt at skjule sin operation ved at forsøge at slette sine spor. Der er også fundet tegn på, at aktøren har overvåget de kompromitterede maskiner for at se, om angrebet blev opdaget.

Det er sandsynligt, at angrebet er gennemført af en statslig eller statsstøttet aktør, muligvis med henblik på at anvende it-hosting-virksomhederne som springbræt til data på kundernes netværk eller at sprede malware til senere misbrug.

I perioden 2015-2016 har CFCS observeret, at flere danske it-hosting-virksomheder er blevet ramt af cyberangreb, og CFCS har i den forbindelse assisteret de pågældende virksomheder. I 2015-2016 rykkede CFCS i gennemsnit ud med et IRT en til to gange om måneden, og CFCS håndterede i samme periode 1104 sikkerhedshændelser og udsendte 219 varslinger.

APT-angreb

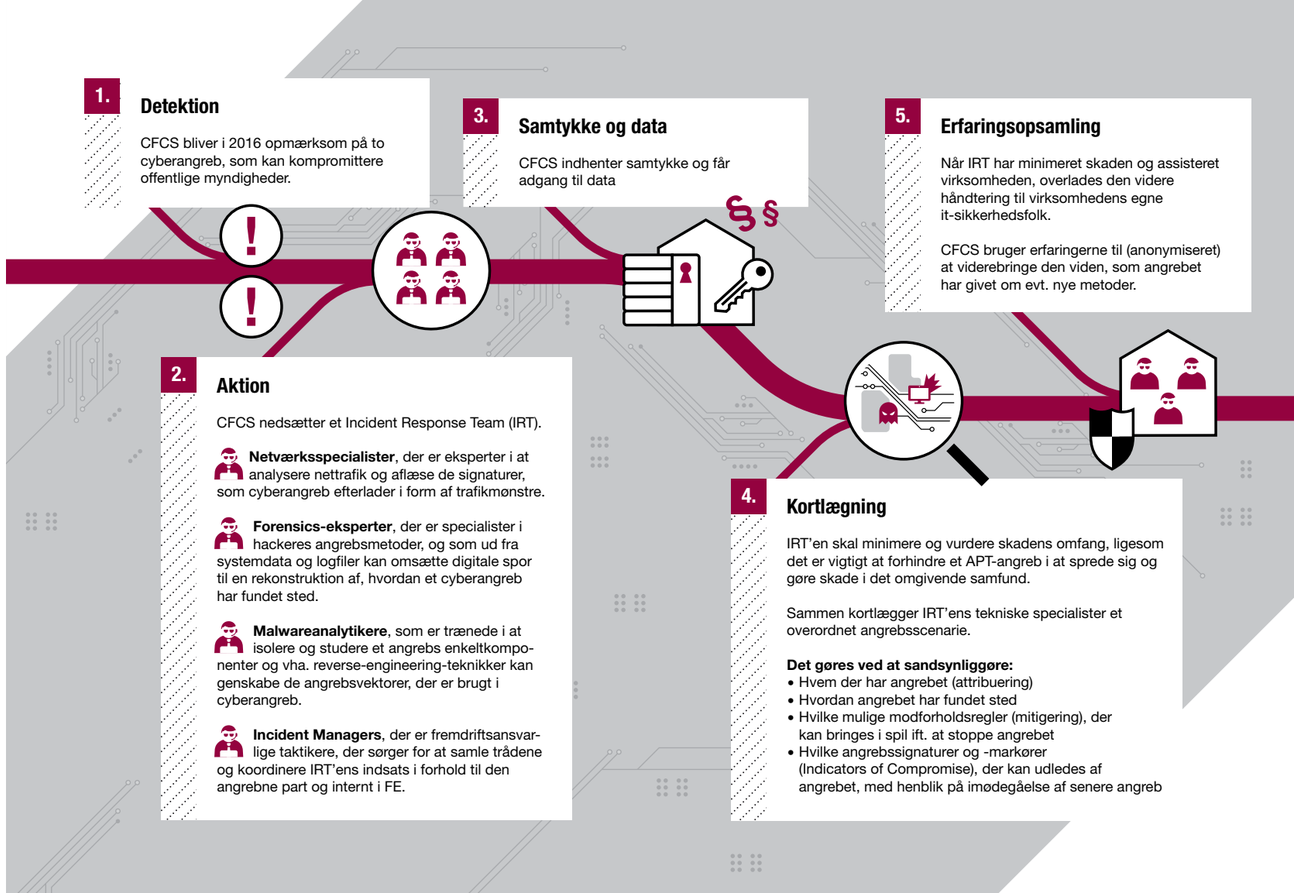
APT står for Advanced Persistent Threat. Det er betegnelsen for et særligt avanceret, målrettet og vedholdende hackerangreb. APT-angreb kræver store ressourcer, teknisk indsigt og konkret viden om målet. Angriberne bruger specielle hacker-værktøjer, der gør dem i stand til at skjule sig i et kompromitteret netværk, og de angriber ofte over lang tid. Når der er tale om APT-angreb, er det meget sandsynligt, at det er stater eller statsstøttede grupper, der står bag.

CFCS' rolle som national it-sikkerhedsmyndighed

FE har i 2015-2016 styrket CFCS' tilsyn med informationssikkerheden på Forsvarsministeriets område.

Fokus for CFCS' tilsyn i 2016 har været implementeringen af ISO27001-standarden vedrørende ledelsessystemer for informationssikkerhed på Forsvarsministeriets område. Formålet med tilsynet har været at vurdere, om styringen af informationssikkerheden er tilrettelagt hensigtsmæssigt, pålideligt og sikkerhedsmæssigt forsvarligt med henblik på at sikre informationernes fortrolighed, integritet og tilgængelighed. Den enkelte myndighed er herefter ansvarlig for at følge op på resultaterne fra CFCS' tilsyn.

CFCS tilser således myndighedernes efterlevelse af de militære sikkerhedsbestemmelser i FKOBST 358-1, jf. kapitel 6, som samtidig udgør Forsvarets informationssikkerhedspolitik. Tilsynet har i 2016 blandt andet omfattet myndighedernes risikovurdering og risikohåndtering, herunder implementering af udvalgte it-kontroller. Tilsynet har også omfattet myndighedernes tilrettelæggelse af handleplaner og awarenessaktiviteter på informationssikkerhedsområdet.



Arktis

FE har i 2015 og 2016 fulgt udviklingen af de strategiske forhold i Arktis og ydet bred støtte til relevante partnere i Forsvaret og centraladministrationen. FE har især fulgt Ruslands politiske og militære intentioner i regionen og Kinas økonomiske engagement i det arktiske område, herunder i Grønland.

I forhold til Rusland har FE især haft fokus på, om Rusland fastholder det nuværende samarbejdsspor, ikke mindst i spørgsmålet om retten til de omstridte områder i Arktis. Samarbejdskursen kan komme under internt pres i den russiske ledelse, særligt hvis Rusland ikke når sine centrale mål ad denne vej. Rusland har allerede ved flere lejligheder gennemført flere symbolpolitiske militære aktiviteter nær Nordpolen.

FE følger samtidig Ruslands fortsatte militære udbygning i Arktis. Den russiske tilstedeværelse er primært defensiv, men rummer dog også mere offensive komponenter og har samlet set en stærk symbolsk betydning.

Kina har i 2015-2016 øget sit engagement i Arktis. Kinas primære interesser i regionen er af kommerciel karakter og knytter sig først og fremmest til muligheden for kortere sejlruter og adgang til naturressourcer. FE følger denne udvikling tæt og fokuserer derfor også på, hvordan Kina forsøger at positionere sig som en indflydelsesrig aktør i Arktis, både i det internationale samarbejde om regionen og bilateralt med de arktiske stater.

FE følger også Kinas interesser i Grønland. Eventuelle kinesiske investeringer i Grønland vil sandsynligvis ikke være en del af en central statsligt styret plan. Som en følge af tætte forbindelser mellem kinesiske virksomheder og det politiske system i Kina er der dog særlige risici forbundet med omfattende kinesiske investeringer i Grønland.

Kampen mod ISIL i Syrien og Irak

FE har gennem flere år fulgt udviklingen af ISIL fra at være en mindre al-Qaida-gruppe i Irak til at blive et større selvudråbt islamisk kalifat i 2014 med mange undergrupper over hele verden. Siden ISIL begyndte at udnytte ustabiliteten i Irak og i Syrien til at erobre et stort sammenhængende territorium, har gruppen ikke blot udgjort en terrortrussel i regionen og i Vesten, den har også fået betydning for borgerkrigen i Syrien og stabiliteten i Irak, ligesom den har været medvirkende til, at op mod 13 millioner civile har måttet flygte.

Danmark deltager i kampen mod ISIL i Syrien og Irak i en koalition af allierede lande anført af USA. Bekæmpelsen af ISIL kræver substantiel viden om organisationen og dens måde at operere på, men også om de internationale aspekter af de konflikter i Syrien og Irak, som ISIL indgår i. Blandt andet har Ruslands intervention i Syrien fra 2014 ændret dynamikken for det syriske styre i borgerkrigen, ligesom Irans og Tyrkiets indblanding i såvel Syrien som Irak har kompliceret konflikterne og dermed også kompliceret kampen mod ISIL.

FE leverer derfor både relevant viden om ISIL og om de regionale og internationale aktørers militære engagement i Syrien og Irak. FE trækker i den forbindelse på flere former for indhentning og på tjenestens politiske og militære specialister samt terroranalytikere i sin rapportering, der især er rettet mod Statsministeriet, Udenrigsministeriet, Forsvarsministeriet og Forsvaret.

I 2015 og 2016 støttede FE således løbende danske beslutningstagere med relevant viden om truslen fra ISIL og udviklingen i kampen mod ISIL. Det gjaldt ikke mindst i forbindelse med regeringens overvejelser og folketingsbeslutning B108 af 19. april 2016 om et substantielt militært bidrag med F-16-kampfly, transportfly og specialstyrker.

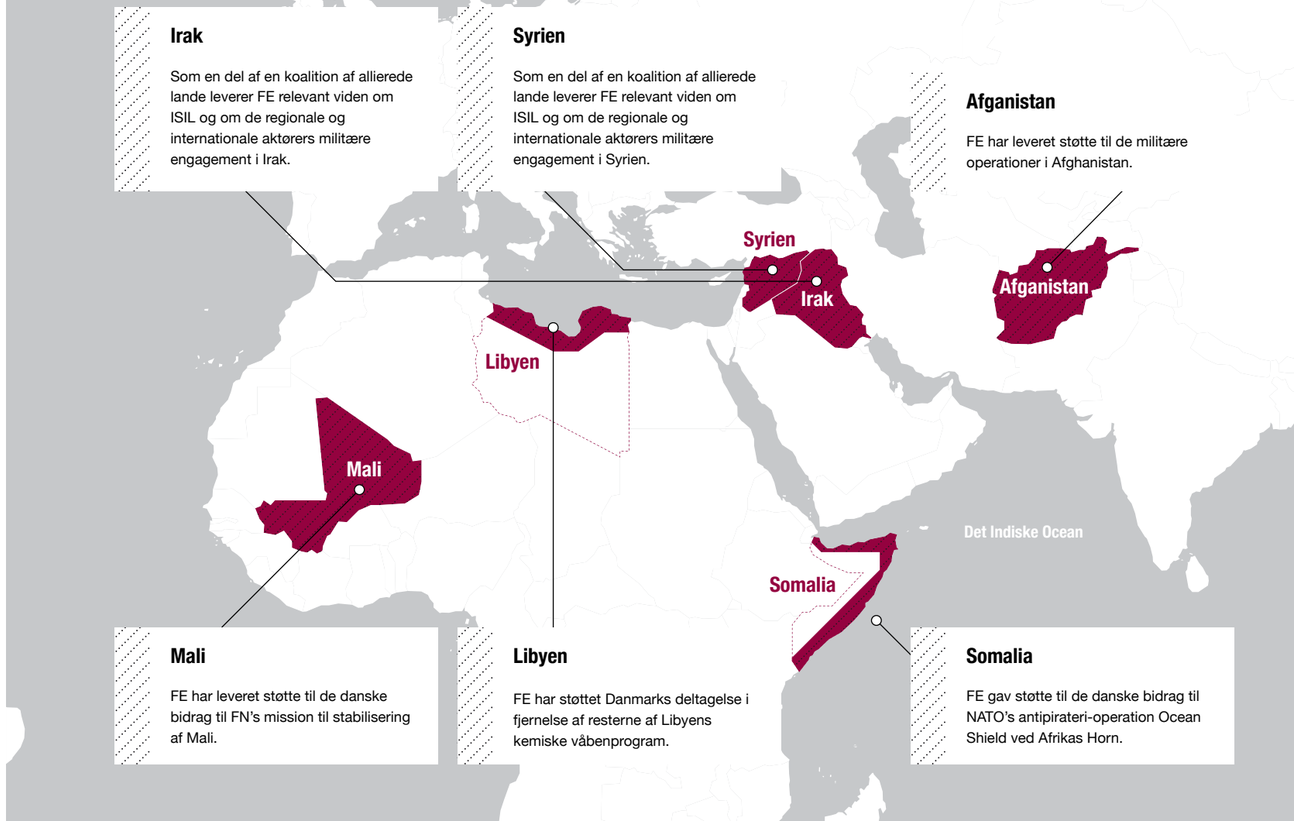
FE støttede F-16-bidraget under indsættelsen med indhentet materiale og ikke mindst analyse. Materialet indgik som en del af det danske bidrags samlede målanalyse.

Efterretningsmæssig støtte til militære operationer

FE støtter den politiske og militære beslutningsproces, når der skal tages stilling til, om og hvordan Danmark skal deltage i en militær operation. Det sker ved, at FE udarbejder analyser, orienteringer og trusselsvurderinger på baggrund af indhentede oplysninger. Støtten fortsætter under den efterfølgende forberedelse og udsendelse af den militære enhed.

FE støtter Forsvaret i missionsområdet med rådgivning og efterretninger af betydning for operationen. Efterretningerne omfatter fjendtligtsindede personers og gruppers hensigter, placering af enheder, aktiviteter og kapaciteter.

I 2015 og 2016 har FE leveret støtte til de militære operationer i Afghanistan, Syrien, Irak og Mali samt til de danske bidrag til NATO's antipirateri-operation Ocean Shield ved Afrikas Horn. FE har også støttet Danmarks deltagelse i fjernelse af resterne af Libyens kemiske våbenprogram. Endelig har FE støttet Flyvevåbnets afvisningsberedskab med F-16 og overvågning af dansk nærområde.



Cyberstøtte til Forsvaret

Den teknologiske udvikling har medført en øget digitalisering i alle aspekter af vores hverdag, og det er både det civile samfund og den militære verden, som er berørt af denne udvikling.

Det danske forsvar er derfor i stigende grad afhængig af digital infrastruktur og har behov for at kunne beskytte egne netværk, systemer og data. Udviklingen åbner også nye muligheder for at fremme egne militære mål.

Derfor er det i forbindelse med den nuværende politiske aftale på forsvarsområdet besluttet at etablere en Computer Network Operations (CNO) kapacitet, der skal kunne gennemføre defensive såvel som offensive operationer på netværk og it-systemer.

Eftersom FE allerede i en årrække har beskæftiget sig med en række af de discipliner, som den nye CNO-kapacitet skal anvende, er det fundet hensigtsmæssigt, at tjenesten opbygger CNO-enheden og efterfølgende stille kapaciteten til rådighed for Forsvaret, så den kan bruges i forbindelse med militære operationer. Planlægningen af operationerne kommer til at foregå i Værnsfælles Forsvarskommando, hvor der i starten af 2017 blev etableret en CNO-planlægningssektion, der skal sikre, at CNO i fremtiden bliver tænkt ind i planlægningen af militære operationer.

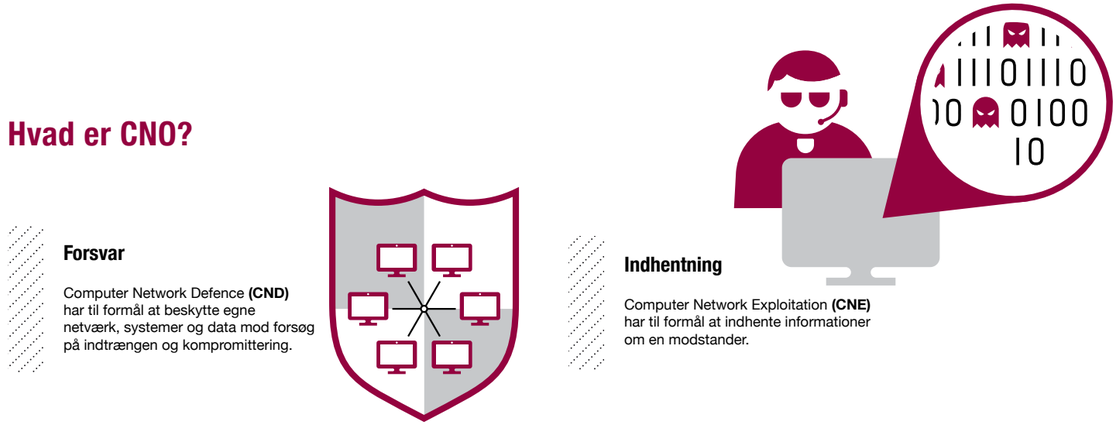
Den nye enhed skal konkret bruges til at beskytte computernetværk ved myndigheder under Forsvarsministeriet, både i den hjemlige struktur og i forbindelse med Forsvarets internationale operationer. Enheden skal desuden kunne understøtte militære operationer ved at indhente efterretninger om en modstander eller ved at angribe en modstanders digitale infrastruktur.

I forbindelse med Computer Network Defence (CND) og Computer Network Exploitation (CNE) er der tale om netværksbaserede handlinger, som FE allerede udfører i dag. Derimod er der i forbindelse med Computer Network Attack (CNA) tale om en ny disciplin, som FE ikke hidtil har beskæftiget sig med.

CNO-enheden er en helt ny kapacitet på et område, som er i rivende udvikling. Det er derfor næppe muligt i første forsøg at lægge sig fast på en permanent sammensætning og organisation af den militære CNO-enhed. CNO-kapaciteten etableres med udgangspunkt i de aktuelt kendte præmisser for derefter at blive videreudviklet, efterhånden som erfaringer drages. Der bliver derfor tale om en trinvis opbygning i to faser med en evaluering undervejs.

Enheden er bemandet med både civilt og militært personale. Opbygningen af visse tekniske funktioner har allerede været i gang i en periode, men siden efteråret 2016 er den fulde implementering indledt. Det er forventningen, at opbygningen af den første fase bliver afsluttet med udgangen af 2017.

Hvad er CNO?



Sikkerhed i Forsvaret

Forsvaret er til for at beskytte det danske samfund. Men ligesom der er en række trusler mod det danske samfund, er der også trusler mod Forsvaret. Det er en af FE's opgaver at forebygge, at Danmark og dansk forsvar bliver udsat for skadelige sikkerhedshændelser.

FE støtter derfor Forsvarets interne sikkerhed. Det sker gennem både en forebyggende sikkerhedsindsats og en kontraefterretningsindsats. Sikkerhedsindsatsen skal beskytte Forsvarets mange forskelligartede værdier såsom medarbejdere, våben, ammunition, køretøjer, it- og kommunikationsudstyr, skibe, fly, bygninger, informationer, persondata, dokumenter og meget andet.

Den forebyggende indsats omfatter blandt andet sikkerhedsbriefinger, risikovurderinger og sikkerhedsgodkendelser. For at matche de dynamiske trusler samt den hastige teknologiske udvikling foregår en stor del af FE's forebyggede sikkerhedsindsats gennem awarenessbriefinger og rådgivning til Forsvarets enheder og medarbejdere – både i Danmark og i forbindelse med internationale operationer. Eksempelvis yder FE sikkerhedsrådgivning til Forsvarets projekt om anskaffelse af nye kampfly.

Det er FE's kontraefterretningstjenestes opgave at identificere og varsle om trusler rettet specifikt mod Forsvaret og dets medarbejdere fra terrorisme, spionage, sabotage, påvirkningskampagner (se beskrivelse på side 40) eller anden kriminalitet. De to mest markante trusler mod Forsvaret er terror og spionage.

FE kigger på den samlede spionagetrussel mod Forsvaret, hvor de anvendte metoder kan være alt lige fra bredspektrede cyberangreb til de mere målrettede som social engineering, hvor enkeltpersoner kontaktes via mail, opkald eller fysisk med det formål at presse dem for oplysninger.

1. Rekognoscering

Aktøren foretager en indledende afdækning af dig via de sociale medier, herunder dine interesser, familieforhold, jobsituation mv. Alt sammen for at kunne indlede en kontakt med dig ud fra dine interesser, idet aktøren har identificeret, at du kan være et aktiv for ham/hende i forhold til at skaffe de oplysninger, som aktøren er ude efter – enten nu eller i et langsigtet perspektiv.

2. Kontakt

Du møder en person på en konference. Mødet virker tilfældigt, men faktisk er det aktøren, som har researchet på dig og derfor kender dine interesser. I udveksler navne på grund af jeres fælles interesser. Efterfølgende modtager du en henvendelse fra personen, som siger tak for sidst, og foreslår, at I kan holde kontakten ved lige – enten fysisk eller via de sociale medier.

3. Angreb

Du modtager en mail, som snyder dig til at lukke en virus ind i jeres systemer. Du klikkede på linket, fordi aktøren brugte oplysninger, som han/hun har afluret om dig. Det kan f.eks. være, at du handler i en online sportsbutik. Det kan også være en falsk ordrebekræftelse fra et site, hvor du ofte handler eller en falsk mail med en invitation til en sportsevent fra en i dit netværk.

4. Exit

Personen har nu fået adgang til dit log-on og måske også systemadministratorens. Personen sørger derfor for at fjerne sporene efter indbruddet og kan nu fremover nøjes med at logge ind med dit eller systemadministratorens password. Vedkommende har nu adgang hele tiden og kan hente oplysninger og ekstrahere informationer og data, når han/hun ønsker det.

"GREGERS", KONTRAEFTERRETNINGSOFFICER

"En af mine opgaver er at holde øje med personer i Forsvaret, der udviser tegn på radikalisering – både højreekstremistisk og militant islamistisk. Jobbet udfordrer mig både analytisk og operativt, og det giver super god mening."

FE har stort fokus på terrortruslen. Dette gælder både truslen mod Danmark og danske interesser generelt samt truslen mod Forsvaret specifikt. Siden oktober 2014 har der været angreb på uniformerede myndighedspersoner i Storbritannien, Canada, Belgien, Frankrig og USA, hvilket har skærpet opmærksomheden på sikkerheden for uniformerede medarbejdere i Forsvaret. For at imødegå sådanne trusler støtter FE kontinuerligt Forsvaret med sikkerhedsvurderinger og rådgivning.

FE er også opmærksom på problemstillingen vedr. ansatte i Forsvaret, som har modtaget militær træning, som kan bruges i andre henseender og potentielt kan udgøre en trussel mod Danmark. Derfor holder FE øje med, om der er nuværende eller tidligere ansatte fra det danske forsvar, der er rejst til konfliktzoner. Det er en del af FE's opgaveløsning at være opmærksom på adfærd, herunder f.eks. radikalisering, og træffe de nødvendige foranstaltninger. Da der vil være tale om danske statsborgere, vil situationen blive håndteret i tæt samarbejde med Politiets Efterretningstjeneste (PET).

FE giver anbefalinger til Forsvaret på baggrund af konkrete trusselvurderinger og foreslår justeringer i beredskabet, men det er Forsvaret selv, der iværksætter og gennemfører de konkrete justeringer og sikkerhedstiltag.

Hvad er social engineering?

Spionage kan antage mange former, og social engineering er et af værktøjerne til at stjæle oplysninger med. Social engineering er kunsten at manipulere nogen til at gøre noget, de ellers ikke ville gøre, med henblik på at afgive fortrolig information. Social engineering kan udføres både fysisk og elektronisk – eller som oftest som en kombination – og består typisk af disse fire faser: rekognoscering, kontakt, angreb og exit. Social engineering kan både ske inden for Forsvaret og i alle andre sammenhænge.

Ét blandt flere værktøjer, som kan bruges til at udføre social engineering, er spear-phishing, som er et målrettet angreb mod enkeltindivider. Spear-phishing udføres ofte i form af en mail, der lader til at komme fra en kendt afsender, så modtageren narres til f.eks. at besvare mailen eller åbne en medsendt fil eller anden aktivitet, som i sidste ende gør skade for vedkommende og dennes arbejdsplads.

Hvad er kontraefterretning?

Hvor den militære efterretningstjeneste bl.a. har til opgave at skaffe informationer om modstanderens kapaciteter, hensigter og planer mv., skal den militære kontraefterretningstjeneste bidrage til sikkerheden i den militære enhed. Det gøres ved at identificere, analysere og give anbefalinger til, hvordan truslerne fra terrorisme, spionage, sabotage, subversion, organiseret kriminalitet og civile uroligheder kan imødegås. Kontraefterretning går altså ud på at identificere, analysere og give anbefalinger, så Forsvaret undgår de trusler, der rettes mod Forsvaret selv.

SANDAGERGÅRD, AMAGER

"FE's lokaliteter er på Kastellet, i Holsteinsgade på Østerbro samt på Sandagergård på Amager. FE har også en indhentningsstation i Hjørring-området."

Kontrol med FE

Der føres på flere områder kontrol med, om FE overholder de gældende regler, som vi som efterretningstjeneste er underlagt. Forsvarsministeren varetager på regeringens vegne den overordnede kontrol med FE, og Folketinget (det såkaldte Kontroludvalg) fører den parlamentariske kontrol, ligesom FE også er underlagt bevillingsmæssig kontrol, som Rigsrevisionen står for.

Ud over den parlamentariske og bevillingsmæssige kontrol er FE underlagt en omfattende kontrol med indhentning, behandling og videregivelse af personoplysninger, som foretages af Tilsynet med Efterretningstjenesterne.

Tilsynet med Efterretningstjenesterne
Tilsynet med Efterretningstjenesterne har siden 2014 ført kontrol med FE, Politiets Efterretningstjeneste (PET) og Center for Cybersikkerhed (CFCS). Tilsynet udøver sine funktioner selvstændigt og i fuld uafhængighed.

Tilsynets medlemmer er udpeget af regeringen og består af en formand, der skal være landsdommer, og fire medlemmer, der alle skal opfylde kriteriet om at nyde almindelig agtelse og tillid i det danske samfund. Tilsynet har sit eget domicil, budget og sekretariat. Tilsynet har også sit eget kontor hos FE, hvorfra det har adgang til alle oplysninger, så det er i stand til at føre tilsyn med FE. Tilsynet er løbende i kontakt med tjenestens jurister, ligesom FE's øvrige specialister deltager i møder med Tilsynet efter behov.

Kontrol med den efterretningsmæssige virksomhed
I 2015 og 2016 gennemførte Tilsynet kontrol med FE's behandling af oplysninger om i Danmark hjemmehørende fysiske og juridiske personer. Tilsynet har i 2016 f.eks. ført kontrol med:

- Oplysninger indhentet i henhold til FE-lovens § 3, stk. 3 (indhentning af oplysninger om en i Danmark hjemmehørende fysisk person, når denne opholder sig i udlandet, og der er bestemte grunde til at formode, at den pågældende deltager i aktiviteter, der kan indebære eller forøge en terrortrussel mod Danmark og danske interesser).
- FE's videregivelse af oplysninger til udenlandske samarbejdspartnere.
- Tværgående operationer mellem PET og FE.
- FE's behandling af oplysninger i vores elektroniske analysesystem og i forbindelse med vores fysiske indhentning.
- Indhentningssystemer, søgeværktøjer og øvrige it-systemer og -værktøjer, herunder kontrol af søgninger i rådata.
- FE's indsamling og indhentning af oplysninger via offentligt tilgængelige kilder og netværksindhentning.
- Sager om sikkerhedsgodkendelse inden for militær sikkerhed.
- Medarbejdernes arbejdspladser, herunder personlige drev, Outlook-mapper og skabe.
- FE's interne kontrol.
- Indledende kontrol af it-informationssikkerhed i henhold til persondatalovens §§ 41 og 42.

Kontrol med Center for Cybersikkerhed
Tilsynet med Efterretningstjenesterne fører ligeledes tilsyn med CFCS' behandling af personoplysninger. Tilsynet har i henhold til CFCS-loven tilsvarende bemyndigelser og adgang til oplysninger som efter FE-loven. Tilsynet har i 2016 blandt andet gennemført kontrol af følgende områder i CFCS:

- Behandling af personoplysninger i CFCS' Netsikkerhedstjeneste.
- Udveksling af personoplysninger med den efterretningsmæssige del af FE.
- Videregivelser af personoplysninger.
- Samarbejde med politiet, herunder PET.
- Informationssikkerhed i henhold til CFCS-lovens § 18.
- CFCS' interne kontrol.

Læs mere på Tilsynets hjemmeside www.tet.dk, hvor også de årlige redegørelser er offentliggjort.

"METTE", JURIST

"Vi skal kunne svare på alle juridiske spørgsmål, der vedrører de mange forskellige efterretningsmæssige opgaver. Det kræver blandt andet, at vi har et godt samarbejde med alle de operative medarbejdere og forstår meget komplicerede it-løsninger."

Jura møder it

FE er en meget teknologitung virksomhed. For at løse opgaver bedst muligt bliver der løbende udviklet nye it-værktøjer. FE's jurister inddrages i et stort antal it-projekter, så juraen er tænkt ind fra starten. På den måde sikres det, at systemerne understøtter de lovgivningsmæssige rammer, som FE er underlagt, samt at Tilsynet kan føre en effektiv kontrol.

FE i dialog med offentligheden

En stor del af det, som FE laver, er i vid udstrækning hemmelig og dermed lukket for den brede offentlighed. Det gælder i høj grad den konkrete viden omkring forskellige efterretningsmæssige forhold, som FE tilegner sig igennem sit arbejde. Omvendt er FE – som en af Danmarks største vidensorganisationer – også sat i verden for at udbrede den viden de rette steder og til de rette personer. Så i FE er vi interesserede i en åben og tæt interaktion med mange aktører, når det er muligt. Derudover er det vigtigt, at der i befolkningen hersker tillid omkring FE. Dette fordrer en vis åbenhed omkring FE's arbejde og metoder, hvilket denne Beretning også er udtryk for.

FE i pressen

Når FE er i pressen, handler det ofte om risikovurderinger fra efterretningsvirksomheden og på cyberområdet. Da FE i 2016 offentliggjorde den årlige Efterretningsmæssige Risikovurdering, skete det ved en pressebriefing i Kastellet. Det var et udtryk for et ønske om at gå i dialog med de journalister, som beskæftiger sig netop med FE's område.

En anden lancering, FE gik ud med i den brede offentlighed i 2016, var præsentationen af et nyt hackerakademi, der uddanner hackere. Offentliggørelse skete i såvel landsdækkende presse, via en uddannelsesmesse og gennem annoncer på sociale medier. Det var en utraditionel rekrutteringsmetode, som FE valgte at bruge for at tiltrække højt kvalificerede it-specialister, hvor konventionelle jobopslag typisk ikke slår til. Metoden har vist sig effektiv og vil blive anvendt igen i 2017.

FE har også deltaget i DR1's dokumentar "Danskere omringet af IS", der blev vist i oktober 2016. Dokumentaren var med til at forklare de bagvedliggende årsager til konflikterne i Irak og Syrien. Dette bidrog vi til med et ønske om at byde ind med den særlige viden, FE har.

FE på sociale medier

I 2015 begyndte FE at gøre brug af sociale medier.

FE har to konti på LinkedIn, som fortrinsvist bliver brugt til rekruttering og som supplement til stillingsopslag på vores hjemmeside og relevante jobdatabaser. At der er to LinkedIn-konti skyldes de grundlæggende forskellige fokus, som arbejdspladsen har. Hvor den efterretningsmæssige del af FE har fokus på trusler fra udlandet, så har Center for Cybersikkerhed (CFCS) fokus på beskyttelse af dansk it.

Desuden har CFCS en profil på Twitter, hvor centeret kommunikerer om cyberhændelser, udvikling i it-sikkerhed og andet, som bidrager til debatten om it-sikkerhed. På dette medie fortæller vi også om ledige stillinger, events og konferencer, som CFCS deltager i.

Center for Cybersikkerhed

CFCS har generelt en mere åben profil over for offentligheden sammenlignet med den efterretningsmæssige del af FE. Arbejdet med cybersikkerhed har stor betydning for danske myndigheder og virksomheder og forudsætter derfor en synlig og udadvendt rolle. Som nationalt kompetencecenter for cybersikkerhed bliver CFCS ofte citeret på området i danske medier. For at styrke cybersikkerheden i Danmark deltager CFCS ofte med indlæg på it-konferencer og giver ekspertinterviews til danske medier.

Akademisk samarbejde

Analyse og vurdering af indhentede oplysninger kræver dygtige analytikere, der kan omsætte de væsentligste oplysninger til efterretninger. I den forbindelse er det vigtigt, at FE ikke er isoleret fra det arbejde, der foregår i tænketanke og forskningsmiljøer. FE deltager derfor i sikkerhedspolitiske møder og konferencer, og vi afholder sikkerhedspolitiske seminarer med dele af det akademiske miljø.

FE har i snart 20 år afholdt seminarer, hvor vores analytikere kan drøfte aktuelle sikkerhedspolitiske emner og fremlægge egne vurderinger i en lukket kreds af akademiske eksperter fra både ind- og udland. Det foregår typisk med indlæg og diskussion om et sikkerhedspolitisk emne, hvor deltagerne kan afprøve forskellige fremtidsscenarier og hypoteser. I 2015 og 2016 har FE blandt andet afholdt seminarer om Arktis og om sproglig formidling af usikkerhed.

Analytikerne og de eksterne eksperter får gennem det akademiske samarbejde udviklet deres netværk, og det giver mulighed for at opfange nye tendenser i forskningsverdenen.

FE bidrager desuden til undervisning i efterretningsfaget på Institut for Statskundskab på Københavns Universitet og på den Myndighedsfælles Efterretningsanalytikeruddannelse på Forsvarsakademiet.

Uddannelsessamarbejde om cybersikkerhed

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) har siden sin oprettelse haft fokus på dialog med uddannelses- og forskningssektoren. CFCS prioriterer denne dialog blandt andet for at optimere mulighederne for, at myndigheder og virksomheder kan ansætte de rette kandidater med relevante kompetencer inden for cybersikkerhed – og på den måde være med til at styrke cybersikkerheden i samfundet generelt. Dialogen giver ligeledes mulighed for at tiltrække dygtige kandidater med de særlige it-kompetencer, som CFCS har brug for i sin opgavevaretagelse.

De sidste to år har dialogen med uddannelses- og forskningssektoren både haft et kort og et langt sigte. På den korte bane har centeret givet mulighed for, at studerende med en opgave inden for cybersikkerhedsområdet kan vejledes af en medarbejder fra centeret, at studerende med de rette kompetencer kan lægge deres praktikforløb i centeret, og endelig er der også oprettet studenterstillinger i centerets netsikkerhedstjeneste. Den langsigtede indsats handler om at sikre de rette uddannelsestilbud på området for cybersikkerhed. Centeret har i den forbindelse medvirket til at skabe et overblik over de mangeartede uddannelsestilbud inden for cybersikkerhed og har også været i dialog med uddannelsesinstitutioner om at opbygge nye uddannelser på området.

"LASSE", IT-SPECIALIST

"Jeg udvikler 'hackerkonkurrencer', som giver it-studerende indblik i FE's it-opgaver. Mine kollegaer og jeg udarbejder selv de mange it- og kryptoopgaver, som vi bruger til hackerkonkurrencer. Ved disse events er flere studerende blevet interesseret i at komme fagligt i dybden med den del af cyberområdet, som FE varetager. Foruden faste it-stillinger har vi også givet studerende mulighed for et specialesamarbejde. Jeg skrev faktisk også selv speciale i samarbejde med FE."

"FE har i snart 20 år afholdt seminarer, hvor vores analytikere kan drøfte aktuelle sikkerhedspolitiske emner og fremlægge egne vurderinger i en lukket kreds af akademiske eksperter fra både ind- og udland."

Forsvarets Efterretningstjeneste
Beretning udgivet juni 2017
Design: Kontrapunkt
Fotos: CphCph,
Kristian Granquist (forord),
US NAVY/Scanpix (Rusland)
Oplag: 2.500
Trykkeri: Dystan & Rosenberg

Kastellet 30
2100 København Ø
Telefon 33 32 55 66
www.fe-ddis.dk
www.cfcs.dk
LinkedIn
@Cybersikkerhed