FORSVARETS EFTERRETNINGSTJENESTE

BERETNING 2013-2014

Forsvarets Efterretningstjeneste

Beretning 2013-2014

Vi tilstræber så stor åbenhed om vores arbejde som muligt, selv om der altid vil være en grænse for, hvor åben en efterretningstjeneste kan være.

Thomas Ahrenkiel, chef for FE

Forord

Forsvarets Efterretningstjeneste (FE) udgiver hvert andet år en beretning om vores virksomhed, og hvad FE har arbejdet med de seneste to år. Formålet med beretningen er at give offentligheden et bedre kendskab til vores opgaver, metoder, organisation og medarbejderprofiler. Vi tilstræber så stor åbenhed om vores arbejde som muligt, selv om der altid vil være en grænse for, hvor åben en efterretningstjeneste kan være.

2013-2014 har været en begivenhedsrig periode, både ude i verden og i FE. Udviklingen i Mellemøsten, Ukraine-krisen og Ruslands adfærd har særligt optaget os.

I 2014 vedtog Folketinget to nye love, der fastsætter rammerne for henholdsvis FE's og Center for Cybersikkerheds virksomhed. Med de to lovgrundlag er der samtidig blevet etableret et nyt og uafhængigt tilsyn, Tilsynet med Efterretningstjenesterne, som har til opgave at føre kontrol med FE og Center for Cybersikkerhed. Der er tale om et markant styrket tilsyn med FE.

Indsatsen på cyberområdet har fortsat høj prioritet for FE. Center for Cybersikkerhed har fået bedre muligheder for at undersøge og forebygge cyberangreb via centerets netsikkerhedstjeneste.

Der har de seneste år været stort fokus i offentligheden på efterretningstjenesternes arbejde. Den øgede opmærksomhed skyldes i høj grad den tidligere efterretningsmedarbejder Edward Snowdens offentliggørelse af oplysninger fra den amerikanske efterretningstjeneste NSA. Sagen har bidraget til både den globale og danske debat om overvågning og efterretningstjenesternes arbejdsmetoder.

Beretningen handler primært om FE's virksomhed og går ikke i detaljer med FE's efterretningsmæssige vurderinger. I stedet henvises til vores årlige publikation "Efterretningsmæssig Risikovurdering", der ligesom FE's første beretning for 2011-2012 kan findes på hjemmesiden www.fe-ddis.dk.

God læselyst

Thomas Ahrenkiel
Chef for Forsvarets Efterretningstjeneste
Kastellet, oktober 2015

HOVEDINDGANGEN PÅ SANDAGERGÅRD

Sandagergård blev indviet 1. maj 1957

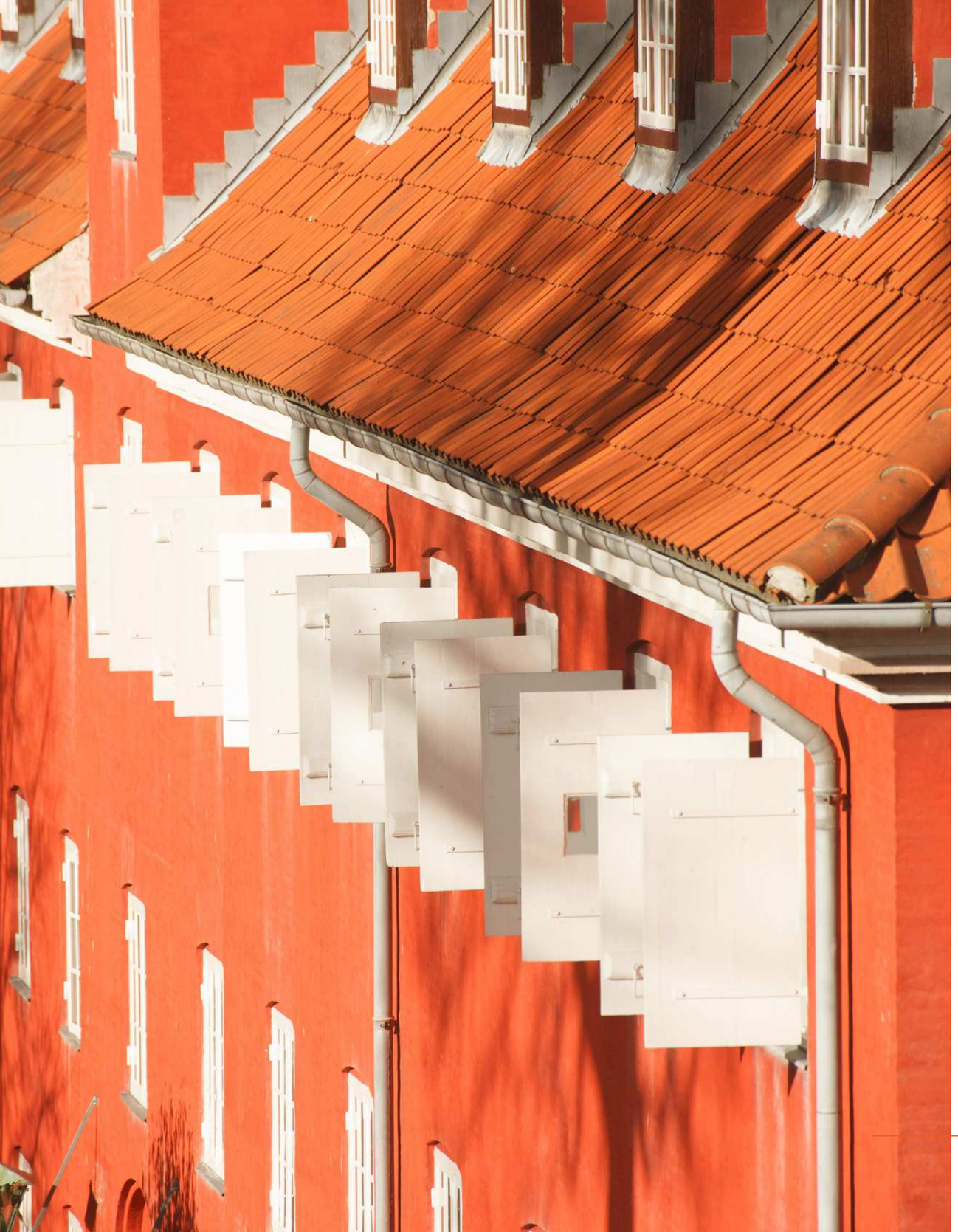
Indhold

Forord 5

OPGAVER 9
- Trusler mod Danmarks interesser 10
- Terrorbekæmpelse 12
- Cybertrusler 14
- Militære operationer 16
- Arktis 17
- Masseødelæggelsesvåben 19
- Pirateri 20
- Center for Cybersikkerhed 23
- Militær sikkerhed 28

METODER 30
- Efterretningsarbejde 31
- Efterretningskredsløbet 32
- Indhentningsdiscipliner 35
- Udenlandske partnere 38
- Produkter og kunder 41
- FE i medierne 42

RAMMER 44
- Ressourcer og medarbejdere 45
- Medarbejdertyper 48
- Organisation 50
- Lovgrundlag 52
- Kontrol med FE 55
- Fælles domicil 56



OPGAVER

FE har tre hovedopgaver:
- Vi er Danmarks udenrigs- og militære efterretningstjeneste
- Vi er Danmarks militære sikkerhedstjeneste
- Vi er national 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 af 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 for eksempel omfatte politiske, militære og økonomiske udviklinger 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, der kan udgøre en trussel mod eksempelvis danske ambassader, udsendte soldater eller andre danske mål i udlandet.

En tjeneste, flere specialer

Efterretningsvirksomhed
Efterretningsvirksomhed er kernen i FE's arbejde. Det er efterretningsarbejdet, som FE bruger størstedelen af sine ressourcer på, og vi benytter her efterretningstjenestens særlige muligheder for at indhente relevante oplysninger, som ikke er alment tilgængelige. Oplysningerne bliver bearbejdet, analyseret og leveret til FE's kunder.

Center for Cybersikkerhed
Center for Cybersikkerhed blev oprettet i 2012 som en del af FE og er Danmarks nationale it-sikkerhedsmyndighed. Centeret bidrager til at beskytte Danmarks kritiske informations- og kommunikationsteknologiske infrastruktur (ikt-infrastruktur) og til at styrke Danmarks evne til at imødegå cyberangreb.

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

De tre overordnede områder 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 imødegåelsen af trusler mod Danmark.

Den efterretningsmæssige del af FE's arbejde er rettet mod forhold i udlandet. FE arbejder til gengæld med trusler i Danmark som følge af rollen som militær sikkerhedsmyndighed for Forsvaret, ligesom den del af Center for Cybersikkerhed, der har til opgave at varsle danske myndigheder og virksomheder om cyberangreb, arbejder med danske mål.

KASTELLET, KØBENHAVN

Kastellet blev opført i 1663

Trusler mod Danmarks interesser

FE's arbejde tager udgangspunkt i det trusselsbillede, som Danmark står over for. Truslerne er alvorlige og komplekse, og de ændrer løbende karakter. Det stiller særlige krav til FE med hensyn til at forebygge og modvirke trusler mod Danmark og danske interesser.

FE informerer og varsler om globale og regionale udviklinger, der nu og i fremtiden kan have betydning for dansk udenrigs-, sikkerheds- og forsvarspolitik. FE indhenter oplysninger om en række landes politiske, militære og økonomiske forhold, der gør os i stand til at rapportere om forskellige landes hensigter, kapaciteter og adfærd. FE følger ligeledes netværk, grupper og enkeltpersoner, der kan udgøre en trussel mod Danmark.

I FE's årlige Risikovurdering samles aktuelle efterretningsbaserede vurderinger af udviklingen i en række lande og konfliktområder, ligesom der varsles om mulige fremtidige brændpunkter.

FE har i 2013-2014 særligt fokuseret på:

- Rusland
- Mellemøsten
- Terrorisme
- Cybertrusler
- Arktis
- Masseødelæggelsesvåben
- Pirateri
- Kina
- Afghanistan

FE har de seneste år i stigende grad prioriteret Ruslands politiske og militære dispositioner, da disse kan have betydning for den internationale stabilitet og sikkerhed. FE vil også fremadrettet have fokus på Ruslands ageren. FE har desuden fulgt udviklingen i Mellemøsten og Nordafrika, hvor ustabiliteten er blevet udnyttet af terrororganisationer som al-Qaida og Islamisk Stat i Irak og Levanten (ISIL). I 2014 har navnlig konflikterne i Syrien og Irak fyldt meget i FE's arbejde. FE har i en årrække også haft fokus på cybertrusler og udviklingen i Arktis, herunder Kinas rolle.

Rusland og Ukraine-krisen

FE har siden begyndelsen af krisen i Ukraine fulgt udviklingen i det østlige Ukraine og den russiske militære opbygning tæt. Få dage efter den politiske omvæltning i Kiev i februar 2014 kunne FE rapportere om, at Rusland gennemførte troppekoncentrationer mod Krim, som klart pegede på, at Rusland ville sikre sig halvøen militært.

FE har især fulgt Ruslands politiske og militære hensigter og ageren over for Ukraine, herunder Ruslands støtte til de russisk ledede separatister i det østlige Ukraine. FE har løbende rapporteret om krisens udvikling og parternes hensigter og givet et detaljeret billede af russisk involvering på Krim og i det østlige Ukraine.

Ukraine-krisen har gjort det meget tydeligt, at Rusland prioriterer et håndfast forsvar af landets interesser i det tidligere sovjetiske område højere end samarbejde med USA, NATO og EU, og at Rusland er villig til at løbe betydelige risici i forholdet til

Vesten. Ukraine-krisen har derfor betydet, at forholdet mellem Rusland og NATO er blevet markant forværret, og Rusland vil i de kommende år forblive en væsentlig sikkerhedspolitisk udfordring.

I Danmarks nærområde er især de baltiske lande sårbare over for Ruslands lokale militære overlegenhed, også selv om de er medlemmer af NATO, og det er muligt, at Rusland vil forsøge at intimidere de baltiske lande, ikke mindst for at teste NATO's beslutsomhed og sammenhængskraft.

FE vurderer, at Rusland ikke udgør en direkte militær trussel mod dansk territorium, men FE har et øget fokus på at følge Ruslands strategiske hensigter og militære aktiviteter i Danmarks nærområde tæt. Dette gælder både russiske fly- og flådeaktiviteter i Østersøen og den generelle russiske militære udvikling og opbygning.

ISIL's fremgang i Syrien og Irak

FE har fortsat stort fokus på den langvarige konflikt i Syrien. Konflikten påvirker stabiliteten i hele regionen og har i flere henseender betydning for verdenssamfundet, herunder Danmark. Syrien-konflikten har blandt andet medført en stor humanitær krise med op mod 12 millioner flygtninge og internt fordrevne mennesker. Konflikten har også medført udfordringer i form af tilrejste og hjemvendte ekstremister og terrorister. Konflikten er desuden en stærkt medvirkende årsag til, at urolighederne i Irak er blusset op igen. ISIL har udnyttet ustabiliteten i Syrien og Irak til at erobre et stort territorium på tværs af de to lande og udråbt et islamisk kalifat. ISIL's selverklærede kalifat har ændret dynamikken i området og har fjernet fokus fra kravet om at afsætte den syriske præsident Bashar al-Asad.

Danmark deltager i kampen mod ISIL i en koalition af allierede lande anført af USA. FE har i 2013-2014 bidraget med relevant viden i forbindelse med regeringens overvejelser, folketingsbeslutninger samt Forsvarets planlægning af den danske deltagelse. FE har ligeledes støttet indsatsen mod ISIL ved at levere trusselsvurderinger og militære statusrapporter om udviklingen i kampen mod ISIL samt vurderinger af ISIL's hensigter og angrebsplaner. FE vil fortsat støtte beslutningstagerne og udsendte enheder, så længe Danmark er engageret som en del af koalitionen.

Efterretningsmæssig Risikovurdering 2014

"ISIL står stærkt, primært i områder med en overvejende sunnimuslimsk befolkning, og udnytter ustabiliteten i Syrien og Irak. Det vil derfor være vanskeligt at nedkæmpe ISIL."

Terrorbekæmpelse

Målet med FE's indsats på terrorområdet er at forebygge terrorangreb mod Danmark og danske interesser i udlandet. I løbet af 2013 og 2014 har FE ydet en betydelig indsats i kampen mod terror. FE har blandt andet været med til at afdække trusler fra terrornetværk, inden de er nået frem til Danmark.

Terrortruslen mod Danmark og danske interesser i udlandet fra militante islamistiske grupper er alvorlig. I løbet af de seneste år er al-Qaidas øverste ledelse blevet svækket, mens regionale terrorgrupper er blevet styrket. Det betyder, at terrortruslen på nuværende tidspunkt er mere diffus og kommer fra en lang række forskellige grupper i flere forskellige områder af verden.

I løbet af 2013 og 2014 er terrornetværk i Syrien og Irak blevet væsentligt styrket. Det gælder navnlig terrorgruppen ISIL og al-Qaida-gruppen Nusra-Fronten. Tusinder af vesterlændinge er rejst til Syrien og Irak for at tilslutte sig ISIL, Nusra-Fronten og andre militante islamistiske grupper. Her får de typisk erfaringer fra slagmarken og kommer i kontakt med rutinerede angrebsplanlæggere og bombespecialister, der tidligere har opereret i andre kampområder. I Syrien og Irak er de ofte blevet ideologisk radikaliserede og forråede og har desuden tilegnet sig færdigheder, som gør dem i stand til at udføre angreb i vestlige lande. De udrejste ekstremister udgør derfor en mulig terrortrussel i de vestlige lande, som de eventuelt vender tilbage til.

Ud over fokus på Syrien og Irak har FE i 2013 og 2014 fulgt terrornetværk i Yemen, Nordafrika, Østafrika, Pakistan og Afghanistan, som fortsat truer Danmark og danske interesser i lokalområdet.

FE's arbejde er rettet mod personer og netværk i udlandet, mens Politiets Efterretningstjeneste (PET) fokuserer på trusler, der befinder sig inden for Danmarks grænser. Terrornetværk har dog typisk grene i flere lande og er dermed internationale af natur. FE arbejder derfor tæt sammen både med danske myndigheder og andre landes efterretnings- og sikkerhedstjenester. I Danmark arbejder FE især tæt sammen med PET, herunder Center for Terroranalyse (CTA). CTA består af medarbejdere fra PET, FE, Udenrigsministeriet og Beredskabsstyrelsen og er organisatorisk placeret hos PET. CTA's arbejde er nærmere beskrevet på www.pet.dk.

Som følge af terrorangrebene i Paris og i København i begyndelsen af 2015 vil FE's terrorindsats blive styrket markant. I april 2015 indgik partierne bag forsvarsforliget en politisk aftale om at bevillige FE yderligere 415 mio. kr. frem til 2018, hvilket blandt andet giver mulighed for at styrke FE's indhentningskapaciteter og evne til at opdage og forfølge nye terrortrusler.

Fra politisk side blev der samtidig lagt op til, at FE som led i den forebyggende efterretningsmæssige indsats selvstændigt skal kunne få rettens kendelse til målrettet at indhente oplysninger om især danske "foreign fighters", der rejser til udlandet for at tilslutte sig militante islamistiske grupper. Dette vil kræve en ændring af FE's nuværende lovgrundlag.

Efterretningsmæssig Risikovurdering 2014

"Antallet af hjemvendte vil sandsynligvis stige de næste to til tre år. Dermed får globalt orienterede militante islamister mere direkte adgang til Vesten og Danmark."

ISIL og al-Qaida

ISIL blev dannet i 2003 i Irak og blev hurtigt en del af al-Qaida. Dengang hed gruppen al-Qaida i Irak (AQI). I 2011 fik AQI også fodfæste i Syrien, blandt andet ved at styrke samarbejdet med Nusra-Fronten, som AQI selv havde været med til at grundlægge. I 2013 brød AQI med Nusra-Fronten og skiftede navn til ISIL (også kaldet ISIS). I 2014 brød ISIL også med al-Qaidas øverste ledelse og skiftede igen navn, nu til Islamisk Stat (IS). FE bruger fortsat betegnelsen ISIL, der også anvendes af Forsvaret. I løbet af 2013 og 2014 har ISIL udviklet sig til at være verdens mest omtalte og frygtede terrorbevægelse.

Cybertrusler

FE's efterretningsmæssige opgaver på cyberområdet

- Indhente oplysninger om cyberaktørers evner, hensigter og adfærd: Hvem forsøger at spionere mod eller angribe Danmark, hvad er deres kapacitet, og hvilke danske myndigheder, organisationer og virksomheder er mål for cyberspionage og cyberangreb?
- Videregive oplysninger til Center for Cybersikkerhed med henblik på at levere efterretningsbaseret cybersikkerhed.
- Varsle om cybertrusler fra udenlandske aktører.

Center for Cybersikkerheds hovedopgaver

- Styrke sikkerheden i den ikt-infrastruktur, som samfundsvigtige funktioner er afhængige af, gennem netsikkerhedstjenesten, der opdager, analyserer og bidrager til at imødegå cyberangreb mod myndigheder og virksomheder.
- Fungere som myndighed for informationssikkerhed og beredskab på teleområdet.
- Varetage opgaven som Danmarks nationale it-sikkerhedsmyndighed: oplyse, vejlede og rådgive danske myndigheder og virksomheder om it-sikkerhed.

Cybertrusler har høj prioritet i FE's arbejde, og FE har i 2013 og 2014 opbygget kapacitet til at kunne imødegå den stadigt stigende cybertrussel fra især statslige og statsstøttede aktører. Arbejdet på cyberområdet foregår både i FE's efterretningsorganisation og i Center for Cybersikkerhed. FE's efterretningsorganisation holder øje med de udenlandske aktører, som forsøger at udnytte internettet til at spionere mod og på andre måder angribe danske interesser. Center for Cybersikkerhed er nationalt kompetencecenter for cybersikkerhed og bidrager blandt andet gennem netsikkerhedstjenesten til at beskytte Danmark mod cyberangreb.

Den største cybertrussel mod danske interesser kommer fra statslige eller statsstøttede aktører. Truslen er primært rettet mod danske ministerier og virksomheder. Staterne bruger de stjålne informationer til at fremme deres politiske og økonomiske mål samt militære udvikling. FE indhenter oplysninger om disse aktørers kapaciteter og hensigter for at kunne imødegå og varsle om specifikke trusler såsom mulige forestående cyberangreb og forsøg på spionage rettet mod Danmark. Informationerne er typisk meget sensitive og bliver først og fremmest delt med Center for Cybersikkerhed og FE's hovedkunder.

FE har i 2013 og 2014 leveret en række rapporter til danske myndigheder om cybertrusler mod Danmark på baggrund af egenindhentede oplysninger og efterretninger fra udenlandske samarbejdspartnere. Det har betydet, at flere angreb er blevet afværget eller stoppet.

FE har et tæt samarbejde med udenlandske samarbejdspartnere, hvor vi udveksler oplysninger om spionage og angreb via internettet. FE har i flere tilfælde advaret samarbejdspartnere om konkrete spionageforsøg mod virksomheder inden for blandt andet forsvars-, medicinal- og luftfartsindustrien inden for 24 timer efter, at et cyberangreb var iværksat.

Militære operationer

FE støtter Forsvarets opgaveløsning, både nationalt og internationalt. I 2013 og 2014 har FE leveret efterretninger til Forsvarets øverste ledelse, militære myndigheder samt enheder og personer udsendt i internationale operationer. Efterretningerne skal give de politiske og militære beslutningstagere og enheder det bedst mulige grundlag at agere på under de hjemlige forberedelser og ude i missionerne.

FE's efterretningsstøtte til Forsvaret i 2013- 2014 har blandt andet omfattet de to store igangværende missioner: Afghanistan og NATO's antipirateri-operation Ocean Shield ved Afrikas Horn. I slutningen af 2013 og frem til sommeren 2014 deltog Danmark i transport og eskorte af kemiske kampstoffer ud af Syrien. Operationen blev gennemført af Søværnet, som ledte den maritime operation på vegne af FN. FE støttede med rådgivning, analyser og efterretninger og arbejdede tæt sammen med Forsvarets egne efterretningsenheder og udenlandske efterretningstjenester.

FE støttede ligeledes Forsvaret, da Danmark sendte observatører til Ukraine i 2014 i rammen af OSCE. Senest har FE støttet det danske bidrag til kapacitetsopbygning og Danmarks F-16-bidrag, der deltager i kampen mod ISIL i Irak. Derudover har FE leveret støtte til mindre militære bidrag og danske udsendte i Mali, Sydsudan og Den Centralafrikanske Republik.

FE har samtidig udarbejdet ikke-klassificerede situations- og trusselsvurderinger til brug for Folketinget. Udvalgte vurderinger er tilgængelige på FE's hjemmeside.

Støtte til Forsvaret

FE støtter Forsvaret med rådgivning og efterretninger om operative forhold i missionsområderne. Efterretningerne drejer sig om fjendtligtsindede personers og gruppers hensigter, aktiviteter og kapaciteter.

FE leverer desuden oplysninger om lokale politiske aktører og deres indbyrdes relationer. Kendskab til lokale forhold sætter de udsendte enheder og enkeltpersoner i stand til bedre at forstå de lokale og regionale forhold. Dermed kan de udsendte samarbejde mere hensigtsmæssigt med lokalbefolkningen og de lokale myndigheder. De har også et bedre grundlag for at vurdere den aktuelle lokale trussel i missionsområdet.

Arktis

FE har i 2013-2014 prioriteret Ruslands politiske og militære intentioner i Arktis samt Kinas økonomiske engagement i det arktiske område, herunder Grønland.

I forhold til Rusland har FE især haft fokus på, om Ukraine-krisen og de forværrede relationer mellem Rusland og Vesten ville få afsmittende konsekvenser andre steder i verden, herunder Arktis. Rusland følger dog fortsat FN-sporet om retten til havbunden i Arktis, men samarbejdskursen kan komme under internt pres i den russiske ledelse, hvis Rusland ikke når sine centrale mål ad denne vej. Rusland er samtidig ved at udbygge sin militære tilstedeværelse i Arktis, hvilket er en udvikling, som FE følger nøje.

Kinas primære interesser i Arktis er de kortere sejlruter og adgang til naturressourcer, men kinesiske investeringer i Arktis, herunder Grønland, vil sandsynligvis føre til, at Kina også på mellemlangt til langt sigt vil få politiske og strategiske interesser i regionen. Kinas interesse for investeringer i navnlig strategiske mineraler i Grønland kan desuden indebære risici for Rigsfællesskabet. FE følger derfor denne udvikling.

Masseødelæggelsesvåben

Truslen fra spredning af masseødelæggelsesvåben er fortsat en udfordring. Truslen drejer sig især om kernevåben, men også om biologiske og kemiske våben.

FE informerer og varsler om udvikling og spredning af masseødelæggelsesvåben, som kan være af direkte eller indirekte betydning for Danmarks sikkerhed eller danske interesser. FE arbejder også for at standse fremstilling af masseødelæggelsesvåben og ballistiske missiler. Denne internationale ikke-spredningsindsats foregår i tæt samarbejde med FE's udenlandske samarbejdspartnere.

FE har i 2013 og 2014 fortsat indsatsen mod konkrete handler og aktiviteter relateret til spredning af masseødelæggelsesvåben, ikke mindst i forhold til Iran. FE har i den forbindelse fokus på netværk og firmaer, der ulovligt forsøger at handle med komponenter, udstyr eller materialer, der kan bruges til at udvikle masseødelæggelsesvåben. FE deler efterretninger og analyser med udenlandske samarbejdspartnere med henblik på at forhindre eller forsinke disse handler. Konkrete forsendelser er på den baggrund blevet standset.

Pirateri

Farvandet ud for Somalias kyst var i en årrække plaget af pirateri, men piraternes aktiviteter er aftaget markant siden 2012, og i 2014 har der kun været et enkelt angreb. Det skyldes primært, at handelsskibene efterlever de anbefalede forholdsregler til at imødegå pirateri, samt at den internationale koalition gennemfører antipirateri-operationer på havet. De grundlæggende årsager til pirateriet ved Somalia har imidlertid ikke ændret sig. FE har derfor i 2013-2014 leveret informationer om pirater til danske myndigheder, civile firmaer samt det danske militære bidrag i NATO's antipirateri-operation Ocean Shield ved Afrikas Horn.

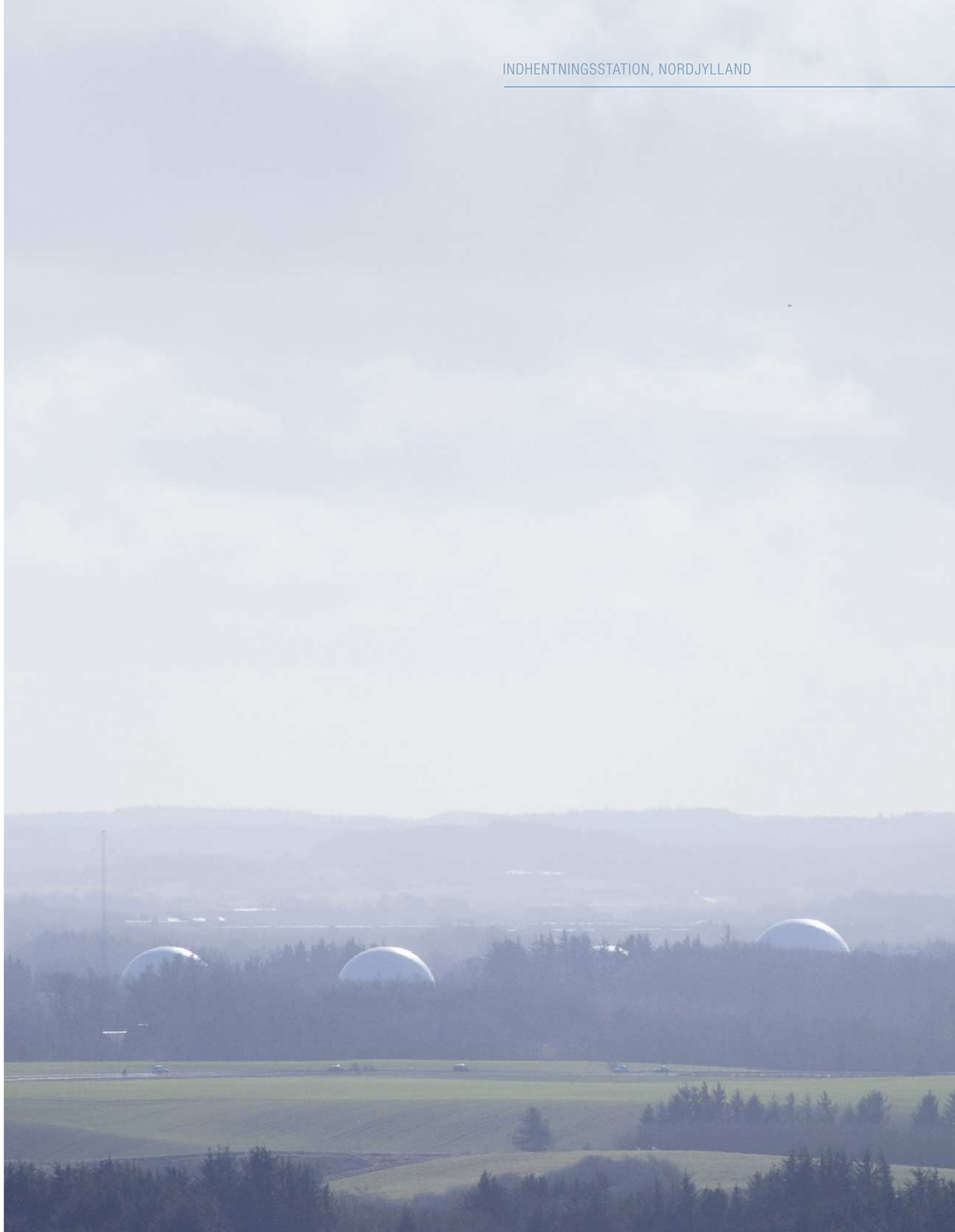
I 2013 og 2014 har der været et stigende fokus på problemet med sørøveri ved Guineabugten i Vestafrika. Skibsfarten er især truet ud for Nigeria. I Guineabugten bliver angrebene typisk udført af velorganiserede kriminelle grupperinger, der stjæler lasten fra primært tankskibe. Besætningsmedlemmer bliver med jævne mellemrum bortført i nogle uger, men længerevarende gidselsituationer som ved Afrikas Horn er dog ikke sandsynlige.

Pirateri og sørøveri

Pirateri foregår ifølge FN's definition i internationalt farvand, mens sørøveri foregår i et lands territorialfarvand. FE har valgt konsekvent at omtale de aktører, der udgør en trussel mod skibsfarten ved Afrika, som pirater, uanset om angrebene sker i eller uden for territorialfarvandet.

Efterretningsmæssig Risikovurdering 2014

"Truslen fra pirateri ved Østafrika er faldet til et meget lavt niveau og vil forblive lav på kort sigt."



Center for Cybersikkerhed og FE

Center for Cybersikkerhed blev oprettet i december 2012 som en del af FE. Placeringen ved FE sikrer, at centeret har adgang til den særlige efterretningsbaserede viden, som FE råder over på cyberområdet.

FE har i mange år haft til opgave at beskytte Forsvarets kritiske it-infrastruktur mod cyberangreb og har dermed fået opbygget stærke kompetencer på netop cyberområdet.

Som udenrigsefterretningstjeneste har FE endvidere stor viden om de udenlandske aktører på cyberområdet samt et veletableret samarbejde med udenlandske efterretningstjenester.

Center for Cybersikkerhed

Center for Cybersikkerheds hovedopgave er at understøtte et højt informationssikkerhedsniveau i den informations- og kommunikationsteknologiske infrastruktur, som samfundsvigtige funktioner afhænger af.

Centerets primære fokus er at håndtere avancerede cyberangreb. Den grundlæggende it-sikkerhed skal myndigheder og virksomheder selv sørge for, typisk i samarbejde med private it-sikkerhedsfirmaer. Den beskyttelse mod de avancerede cyberangreb, som Center for Cybersikkerhed leverer, udgør et ekstra lag af sikkerhed, der supplerer de kommercielt tilgængelige sikkerhedsløsninger samt myndighedernes og virksomhedernes egen indsats.

Center for Cybersikkerhed har i 2014 fået et nyt samlet lovgrundlag. Det nye lovgrundlag har styrket centerets muligheder for at undersøge og forebygge cyberangreb samt sikre, at der er entydige og restriktive regler for centerets behandling af personoplysninger. Lovgrundlaget beskrives nærmere på side 52-53.

Dialog med interessenter

I løbet af 2014 har Center for Cybersikkerhed iværksat en række tiltag, der har udbygget og styrket centerets dialog med både den offentlige og den private sektor. Centeret har blandt andet etableret forskellige samarbejdsfora om cybersikkerhed for en række offentlige myndigheder, brancheorganisationer og samfundsvigtige virksomheder.

For at understøtte Center for Cybersikkerheds arbejde med at beskytte Danmark mod avancerede cyberangreb er der truffet en regeringsbeslutning om, at alle statslige myndigheder fremover skal underrette Center for Cybersikkerhed ved større it-sikkerhedsmæssige hændelser.

Sideløbende med den styrkede dialog med interessenterne prioriterer Center for Cybersikkerhed fortsat den proaktive rådgivnings- og vejledningsindsats, som er en af centerets kerneopgaver. Centeret udgiver løbende trusselsvurderinger, sikkerhedsanbefalinger og vejledninger. Et eksempel er vejledningen ”Cyberforsvar der virker”, som er udarbejdet i samarbejde med Digitaliseringsstyrelsen. Vejledningen indeholder konkrete anbefalinger til, hvordan danske myndigheder og virksomheder effektivt kan mindske risikoen for cyberangreb.

Forsvaret er en vigtig interessent for Center for Cybersikkerhed. Centeret har som Forsvarets it-sikkerhedsmyndighed i 2014 revideret de militære sikkerhedsbestemmelser på informationssikkerhedsområdet, så sikkerheden kan styres efter den internationale ISO/IEC 27001-standard. Derudover har centeret intensiveret samarbejdet med Forsvarets myndigheder med henblik på at opdatere de tilhørende sikkerhedsprocesser.

Avancerede cyberangreb

Center for Cybersikkerhed har fokus på de mest avancerede typer cyberangreb. Den alvorligste angrebstype kaldes APT-angreb (Advanced Persistent Threat-angreb), som er kendetegnet ved at være særligt målrettet og vedholdende. APT-angreb bliver typisk udført af angribere, som har økonomisk og teknisk støtte fra organisationer, der ligger inde med specialviden om målet.

Angriberen benytter sig af denne viden til at tiltvinge sig adgang til ofrets it-systemer ved eksempelvis at udnytte sårbarheder (kendte såvel som ukendte) i den software, som ofret bruger. Her skjuler hackeren sig i ofrets systemer ved hjælp af specialfremstillet software, indtil formålet med angrebet er opnået. APT-angreb bliver ofte brugt til at udøve spionage mod virksomheder og stater.

Ny strategi for cyber- og informationssikkerhed

I december 2014 blev den nationale strategi for cyber- og informationssikkerhed lanceret. Sammen med Digitaliseringsstyrelsen varetog Center for Cybersikkerhed sekretariatsfunktionen i forbindelse med udarbejdelsen af strategien, hvor otte ministerier bidrog. Strategien har fokus på at beskytte udvalgte områder, hvor de cybersikkerhedsmæssige udfordringer vurderes at være særligt store, herunder cyber- og informationssikkerhed i staten og på energi- og teleområdet. Flere initiativer i strategien berører direkte centerets arbejde:

- Der er oprettet en enhed, der skal vurdere cybertrusler. Enheden vil blandt andre bestå af repræsentanter for sektorer, hvis infrastruktur samfundsvigtige funktioner er afhængige af.
- Der er oprettet en enhed til undersøgelse af større cybersikkerhedshændelser. Enheden skal understøtte, at der sker en styrket opsamling af erfaringer fra hændelserne, som skal stilles til rådighed for andre myndigheder og virksomheder.
- Center for Cybersikkerhed opretter et særligt kompetencecenter på SCADA-området (indlejrede industrielle styringssystemer). Kompetencecenteret kan bistå og rådgive både private og offentlige virksomheder i forsyningssektorerne med viden om sårbarheder ved SCADA-systemer.

Center for Cybersikkerheds indsats ved cyberangreb

Hver dag udsættes danske myndigheder og virksomheder for avancerede forsøg på cyberangreb. Center for Cybersikkerheds netsikkerhedstjeneste monitorerer løbende internettrafikken til og fra de myndigheder og virksomheder, der er tilsluttet netsikkerhedstjenesten, for at opdage og analysere ondsindet internetaktivitet. Når Center for Cybersikkerhed bliver opmærksom på et cyberangreb, varsler centeret den organisation, som er blevet udsat for angrebet, og rådgiver om, hvordan det kan stoppes og lignende angreb forhindres.

Hackerangrebet mod CSC

Center for Cybersikkerhed bidrog i 2013-2014 med undersøgelser i forbindelse med efterforskningen og afdækning af konsekvenserne af angrebet på CSC fra 2012, hvor hackere skaffede sig adgang til sensitive systemer og oplysninger.

Centeret udarbejdede to rapporter som opfølgning på sagen. Den ene rapport, der blev udarbejdet i samarbejde med PET, omhandlede hændelsesforløbet og CSC's tiltag på baggrund heraf. Den anden rapport, som blev udarbejdet i samarbejde med Digitaliseringsstyrelsen, indeholdt anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift.

Sidstnævnte rapport er offentliggjort og indgår i grundlaget for den nationale strategi for cyber- og informationssikkerhed.

En vigtig ændring, som er gennemført i forbindelse med den nye lov om Center for Cybersikkerhed, er, at centerets to varslingstjenester for internettrusler – GovCERT og MILCERT – er blevet lagt sammen til en ny netsikkerhedstjeneste. Sammenlægningen har givet en række synergieffekter og øget den samlede kapacitet, som centeret kan indsætte ved avancerede cyberangreb.

Sensornetværket

For at bidrage til at forhindre cyberangreb analyserer Center for Cybersikkerhed de værktøjer og metoder, som hackerne bruger. Centerets netværksanalytikere indsamler løbende den nyeste viden om cyberangreb og finder de digitale spor og mønstre, der identificerer et angreb. Disse digitale fingeraftryk lægges ud i specialkonstruerede alarmenheder, som er placeret på internetforbindelserne hos netsikkerhedstjenestens kunder. Tilsammen danner alarmenhederne et såkaldt sensornetværk, som alarmerer Center for Cybersikkerhed ved tegn på cyberangreb hos de tilsluttede kunder.

THOMAS, MALWAREANALYTIKER

"Når en hacker programmerer malware, forsøger han ofte at snyde med koden, så vi ikke kan analysere den. Det er så min opgave at komme uden om de teknikker og metoder, som hackeren har brugt i sine forsøg på at stoppe mig."

Når Center for Cybersikkerhed rykker ud

Når en alarmenhed genkender en hackers ondsindede internettrafik og alarmerer Center for Cybersikkerhed, undersøger netsikkerhedstjenestens analytikere det potentielle cyberangreb. Her vurderer analytikerne, hvor alvorlig truslen er, og hvad der eventuelt bør gøres for at imødegå det potentielle angreb. På baggrund af Center for Cybersikkerheds vurdering bliver kunden varslet, og i alvorlige tilfælde vil netsikkerhedstjenesten tilbyde at udsende en særlig indsatsgruppe, der kan bistå kunden med umiddelbart at imødegå angrebet.

I tilfælde af større cyberangreb eller ved enkeltangreb af mere generel interesse vil Center for Cybersikkerhed kunne udsende sin undersøgelsesenhed med henblik på at opsamle viden, der kan anvendes til fremtidig beskyttelse af tilsvarende systemer. En undersøgelse vil typisk resultere i udgivelse af en rapport eller et varsel.

Læs mere om Center for Cybersikkerheds opgaver og produkter på www.cfcs.dk.

ØSTBANEGADE, KØBENHAVN

Indgangen flyttes til Holsteinsgade i 2015

Militær sikkerhed

I relation til militær sikkerhed har FE til opgave at forebygge og imødegå, at Forsvaret udsættes for skadelige sikkerhedshændelser.

Hvis de forkerte får indblik i Forsvarets sikkerhedsforhold, planlægning, medarbejderoplysninger og kommunikation eller ved præcis, hvor indsatte styrker befinder sig, øges truslen mod soldaterne og den opgave, Forsvaret skal løse.

Den militære sikkerhedstjeneste skal beskytte Forsvaret mod terrorisme, spionage, sabotage og andre former for kriminalitet. Forsvarets aktiver er meget forskelligartede og omfatter for eksempel medarbejdere, våben, køretøjer, kommunikationsudstyr, skibe, fly, bygninger og informationer.

Sikkerhedstjenesten er opdelt i to hovedområder:

- Sikkerheds- og kontraefterretningstjeneste
- Forebyggende sikkerhedstjeneste

Sikkerheds- og kontraefterretningstjeneste

Det er sikkerheds- og kontraefterretningstjenesten i FE, der er med til at identificere trusler rettet specifikt mod Forsvaret. FE skal med andre ord have viden om og kendskab til mulige modstandere og det trusselsbillede, de tegner.

Sikkerheds- og kontraefterretningstjenesten indhenter og analyserer i samarbejde med resten af FE informationer om truslerne mod Forsvaret i Danmark og i udlandet. Resultatet indarbejdes i FE's skriftlige trusselsvurderinger, der benyttes af de politiske og militære beslutningstagere. Trusselsvurderinger for Forsvaret i Danmark udarbejdes i tæt samarbejde med PET og CTA. På grundlag af trusselsvurderingerne fastsættes der forebyggende sikkerhedsforanstaltninger for i passende omfang at beskytte Forsvaret mod truslerne.

FE yder direkte støtte i missionsområder, hvor danske enheder er indsat. Det sker blandt andet ved udsendelse af medarbejdere, der kan rådgive om sikkerheds- og kontraefterretningsmæssige forhold og deltage i samarbejdet med NATO og andre landes myndigheder.

Forebyggende sikkerhedstjeneste

Forebyggelsesarbejdet sker på baggrund af et opdateret trusselsbillede. Ved at være bevidst om, hvordan Forsvaret bedst beskytter sig, kan risikoen for, at truslerne bliver realiseret, minimeres.

Forebyggelse handler om:

- Sikker håndtering og opbevaring af informationer.
- Fysisk sikring af bygninger, depoter, garager, militære områder mv.
- Håndtering af sikkerhedsbrud og andre hændelser samt efterfølgende rådgivning og undervisning for at forebygge nye brud.
- Sikkerhedsgodkendelse af medarbejdere, der skal håndtere klassificerede informationer.
- Sikkerhedsgodkendelse af virksomheder, der leverer tjenesteydelser til Forsvaret.

FE udarbejder og vedligeholder det regelsæt, der fastlægger minimumskravene til forebyggende sikkerhedsforanstaltninger. Disse kan for eksempel omfatte bevogtning, indhegning, adgangskontrol, tv-overvågning af lokaliteter, alarmer, brug af sikrede opbevaringsskabe og sikre procedurer for håndtering af følsomme oplysninger. Regelsættet gælder for alle dele af Forsvarsministeriets område.

De konkrete sikkerhedsforanstaltninger bliver fastsat lokalt af myndighederne på grundlag af FE's regelsæt, ud fra risikoen og de stedlige forhold. Der er særligt behov for en høj grad af forebyggende sikkerhed for de udsendte soldater i missionsområder og for transport og opbevaring af våben, ammunition, højtklassificerede dokumenter og følsomt udstyr.

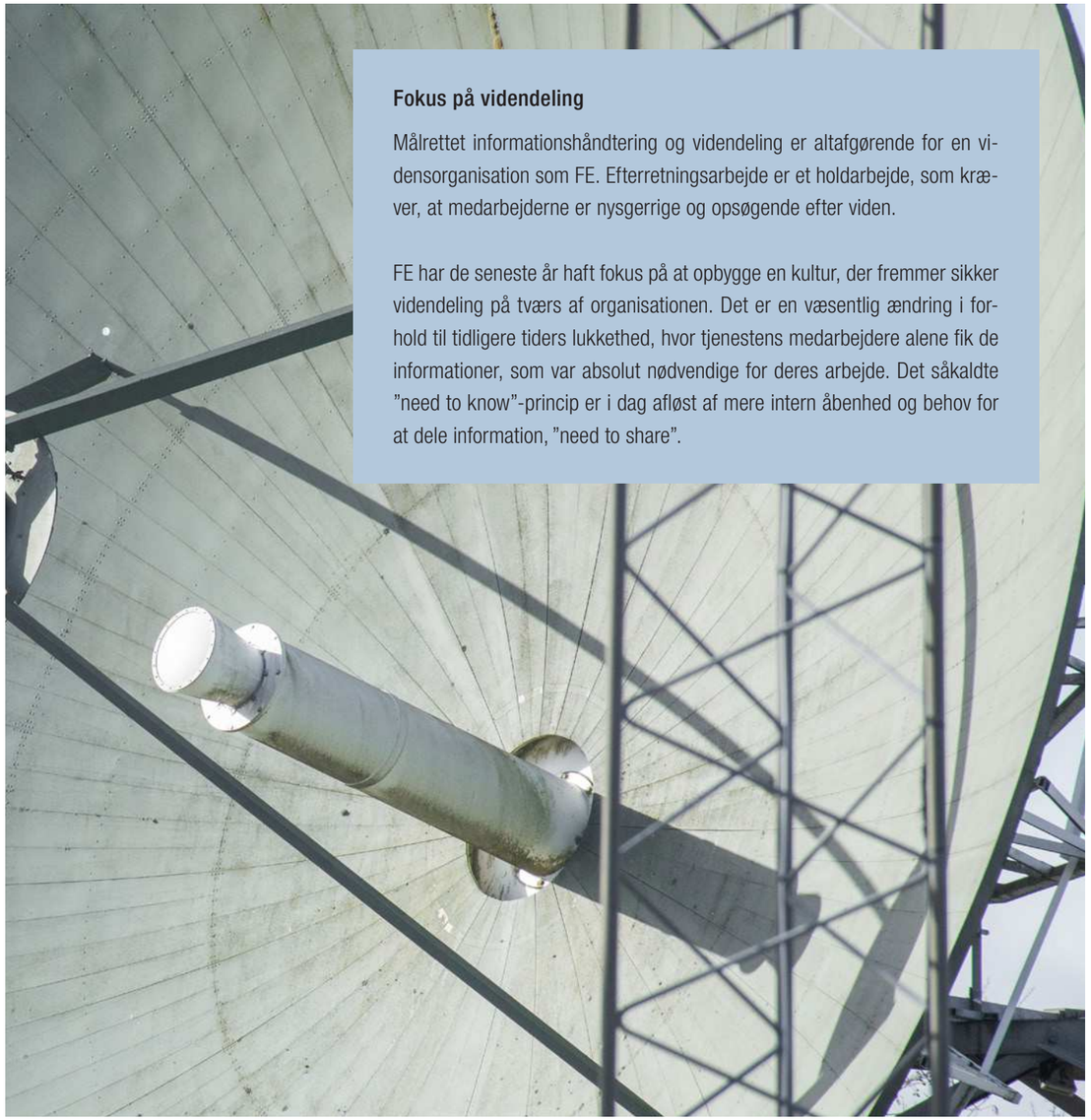
FE har ansvar for, at der regelmæssigt foretages kontrol af sikkerhedstilstanden på Forsvarets tjenestesteder i ind- og udland, og at der rådgives eller pålægges krav om mulige forbedringer.

FE sikkerhedsgodkender ansatte inden for Forsvarsministeriets område og ansatte i private virksomheder, der leverer varer eller tjenesteydelser til Forsvaret. Sager om sikkerhedsgodkendelse behandles efter forvaltningslovens regler, hvilket vil sige, at en person skal give sit samtykke til, at FE kan behandle oplysninger om den pågældende. Derudover gælder reglerne om partshøring, aktindsigt, begrundelse af afgørelser og klagevejledning.

FE træffer afgørelse om sikkerhedsgodkendelser ud fra en konkret vurdering af forskellige personlige forhold. Der lægges især vægt på, om personen har en sådan adfærd og karakter, at der ikke kan være tvivl om, at vedkommende kan håndtere klassificerede informationer. Oplysninger om en ægtefælles eller samlevers adfærd og karakter kan også indgå i vurderingen.

INDHENTNINGSSTATION, NORDJYLLAND

METODER



Fokus på videndeling

Målrettet informationshåndtering og videndeling er altafgørende for en vidensorganisation som FE. Efterretningsarbejde er et holdarbejde, som kræver, at medarbejderne er nysgerrige og opsøgende efter viden.

FE har de seneste år haft fokus på at opbygge en kultur, der fremmer sikker videndeling på tværs af organisationen. Det er en væsentlig ændring i forhold til tidligere tiders lukkethed, hvor tjenestens medarbejdere alene fik de informationer, som var absolut nødvendige for deres arbejde. Det såkaldte "need to know"-princip er i dag afløst af mere intern åbenhed og behov for at dele information, "need to share".

Efterretningsarbejde

Som efterretningstjeneste har FE særlige muligheder for at få adgang til relevante informationer, der ikke er alment tilgængelige, og som andre gerne vil holde hemmelige. Det betyder dog ikke nødvendigvis, at FE kommer frem til andre konklusioner eller vurderinger end dem, som alene er baseret på åbne kilder. Vi benytter forskellige metoder til at indhente vores oplysninger på, såkaldte indhentningsdiscipliner (se side 35-36).

Mulighederne for at indhente data er helt centrale for vores virke og fremgår af lovgrundlaget for FE. FE's indhentning er geografisk neutral, hvilket betyder, at indhentningen kan 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 kan blive opfattet som værende i strid med lovgivningen i det land, hvor indhentningen foregår eller er rettet imod, og det samme kan være gældende for udenlandsk efterretningsvirksomhed på dansk grund.

FE har særlige metoder til analyse af de oplysninger, som indhentes. Når FE modtager en oplysning, skal den først valideres for at afgøre kildens pålidelighed og kildens adgang til oplysningerne. Dernæst vurderer vi oplysningens troværdighed og sandsynligheden for, at det omtalte vil ske. Dette afhænger både af kildens pålidelighed, kildens adgang, oplysningernes troværdighed, og hvordan oplysningerne passer med vores erfaring og andre informationer, vi har kendskab til fra både åbne og lukkede kilder. På denne måde omsættes den rå oplysning til en valideret oplysning, der kan indgå i det videre analysearbejde og den endelige udarbejdelse af efterretninger.

Som efterretningstjeneste er det kun muligt at varsle om fremtidige udviklinger på grundlag af omhyggelig bearbejdning og analyse af de indhentede oplysninger. Efterretningsanalyse er dog ikke en eksakt videnskab, og en vigtig del af varslingen er derfor at gøre det helt klart for FE's kunder, hvor sikre vi er i vores vurderinger. Det gør vi ved at anvende en række faste sandsynlighedsgrader.

Efterretningskredsløbet

Kunderne og deres behov er styrende for FE's indsamling og øvrige efterretningsarbejde, der kan illustreres i det såkaldte efterretningskredsløb.

I efterretningskredsløbet bliver kundernes behov omsat til konkrete, prioriterede efterretningsbehov. På den baggrund beslutter FE, hvordan de efterspurgte oplysninger skal indhentes. Derpå følger den konkrete indsamling eller indhentning af data, som efterfølgende bearbejdes og gøres anvendeligt til analyse og rapportering tilbage til kunderne.

Det er vigtigt at understrege, at efterretningskredsløbet er en stiliseret fremstilling af den måde, vi arbejder på. Der er tale om en dynamisk proces med en række sammenhængende og overlappende delprocesser, hvor nye oplysninger og ændrede behov hele tiden bringes i spil.

Samarbejde i operative teams
Efterretningsarbejdet er en holdindsats, og FE arbejder i stigende grad med operative teams, der er dedikeret til FE's vigtigste indsatsområder. De operative teams er sammensat af specialister på tværs af organisationen, der har til opgave at sørge for, at efterretningskredsløbet på et bestemt indsatsområde virker bedst muligt og løbende udvikles. Dialogen og koordinationen mellem eksempelvis indhentere, bearbejdere og analytikere er med til at sikre, at FE skaffer de rette informationer til at dække de højest prioriterede efterretningsbehov.

Identifikation af behov
Efterretningsprocessen begynder i tæt dialog med FE's kunder for at identificere deres behov for viden. Disse overordnede behov danner grundlag for FE's efterretningsbehov, som konkretiserer de spørgsmål, vi ønsker at besvare gennem indsamling eller indhentning af oplysninger. Efterretningsbehovene prioriteres indbyrdes, da der ikke er ressourcer til at lægge lige meget vægt på alle områder.

Dataindsamling og filtrering
Dataindsamling er en kompliceret proces, der kræver specialiseret teknisk viden inden for vidt forskellige teknologier. Vi skal være i stand til at identificere, hvor den viden eller kommunikation, der efterspørges, er tilgængelig. Dertil kommer udfordringen med at finde præcis den relevante oplysning blandt meget store datamængder. FE foretager derfor filtrering og frasortering af det indhentede materiale, så det er muligt at håndtere og arbejde med materialet.

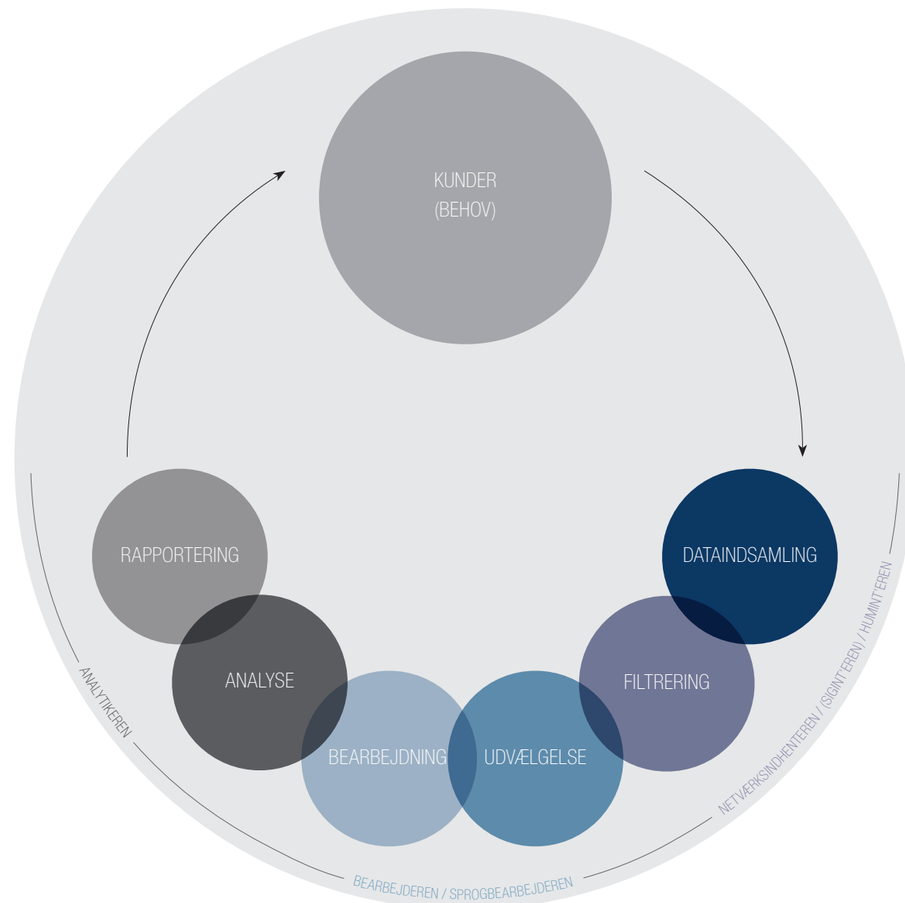
Udvælgelse og bearbejdning
Det potentielt relevante materiale bliver yderligere sorteret og udvalgt, så kun det mest relevante bliver tilgængeligt. Materialet er i stigende grad krypteret, hvorfor arbejdet også forudsætter, at krypteringen brydes, før det kan bruges. Derefter skal det bearbejdes, herunder eventuelt oversættes.

Analyse og rapportering
Herfra kan analytikerne begynde at arbejde med materialet, identificere de mest relevante informationer og validere dem. Ofte består analysen i at samle mange spredte oplysninger fra forskellige kilder til et så samlet billede som muligt. Vi har sjældent alle oplysninger. Analysearbejdet fører på den måde til produkter til kunder og partnere. Men det fører også typisk til behov for ny viden, som igen kræver yderligere indhentning.

KENNETH, OPERATIV TEAMLEDER

"FE er fuld af ambitiøse og dedikerede medarbejdere, som er specialister på hvert sit område i efterretningskredsløbet. Mit arbejde består i at styrke samarbejdet mellem disse medarbejdere om konkrete problemstillinger med FE's prioritering for øje."

EFTERRETNINGSKREDSLØBET



Akademisk samarbejde
Det sidste led i efterretningskredsløbet består af analyse og vurdering af de indhentede oplysninger. Det 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 forskellige 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 2014 har FE blandt andet afholdt seminarer om Iran samt terrorisme.

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

Indhentningsdiscipliner

FE er en såkaldt all-source efterretningstjeneste, der beskæftiger sig med alle typer af informationsindhentning. Særligt større lande har ofte flere efterretningstjenester med hvert sit speciale inden for indhentning. I Danmark er alle indhentningsdiscipliner samlet i FE, herunder opgaven som national elektronisk indhentningstjeneste.

Der er fordele og ulemper ved alle indhentningsdisciplinerne, som indgår i vores overvejelser om, hvilke indhentningsformer der skal anvendes. En helt afgørende faktor er de risici, der er forbundet med brugen af indhentningsdisciplinerne. Overordnet set arbejder FE med fire forskellige indhentningsdiscipliner:

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 at læse nyheder og bruge opslagsværker. Det drejer sig også i høj grad om avanceret og systematisk indsamling af oplysninger fra blandt andet internettet, eksempelvis kommunikation i åbne netfora. Dermed grænser OSINT også som disciplin op til netværksindhentning.

Der er som udgangspunkt ikke særlige risici forbundet med at bruge OSINT.

SIGINT
SIGINT står for Signals Intelligence, som er elektronisk indhentning af forskellige typer af kommunikation som dataoverførsler mellem computernetværk, telekommunikation osv. Den elektroniske indhentning foregår for eksempel via satellitter. Kommunikationen indhentes, mens den er undervejs uden at påvirke transmissionen, og uden at de berørte parter kan se, at deres kommunikation opfanges.

SIGINT-indhentning er derved passiv og forbundet med en forholdsvis lav risiko set fra efterretningstjenestens side. 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, som kommunikationen baserer sig på.

NETVÆRKSINDHENTNING

Netværksindhentning er også kendt som Computer Network Exploitation (CNE). Den er i familie med SIGINT, da der er tale om elektronisk indhentning mod computernetværk. Denne indhentningsform 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.

Netværksindhentning efterlader altid visse spor, som andre efterfølgende kan opdage. Der er dermed en vis risiko for, at aktiviteterne bliver afdækket og indhentningen kompromitteret.

HUMINT

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

HUMINT-indhentning 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 eventuelt personligt komme i fare. Derfor er HUMINT-indhentning forbundet med en betydelig risiko og er en indhentningsform, der kun anvendes, når risici nøje er afvejet i forhold til de mulige gevinster.

"VIKTOR", FØRINGSOFFICER

"Selv i forhold til de allernærmeste venner og familie er det stærkt begrænset, hvad der kan deles. Der er højst tale om meget brede penselstrøg. Det er noget, man skal vænne sig til."

INDHENTNINGSSTATION, AMAGER

Udenlandske partnere

UDENLANDSKE PARTNERE

FE kan som efterretningstjeneste i et lille land ikke dække hele verden. Det er derfor afgørende at have et tæt samarbejde med udenlandske sikkerheds- og efterretningstjenester samt andre staters varslingstjenester for cybertrusler. Det er ikke mindst nødvendigt, da de udviklinger og trusler, som kan have betydning for Danmarks sikkerhed, ofte overskrider landegrænser.

FE arbejder både bilateralt med andre efterretningstjenester og deltager i multilaterale efterretningsmæssige samarbejder i NATO og EU under hensyntagen til det danske EU-forsvarsforbehold.

Partnersamarbejdet handler først og fremmest om udveksling af oplysninger og analyser, men kan også omfatte fælles informationsindhentning og operationer. Det latinske udtryk quid pro quo (noget for noget) bliver ofte brugt til at beskrive samarbejdet mellem efterretningstjenester, hvor udvekslingen af oplysninger går begge veje. Der er med andre ord tale om en byttehandel, hvor FE videregiver oplysninger til en samarbejdspartner, mod at partneren på samme vis stiller oplysninger til rådighed for FE. Samarbejdet kan bidrage til nyttig viden om områder, hvor FE's efterretningsmæssige billede er mangelfuldt.

Da samarbejdet med udenlandske efterretningstjenester er en væsentlig kilde til oplysninger, der bidrager til at dække FE's efterretningsmæssige behov, kan partnersamarbejdet betragtes som en selvstændig indhentningsform, der understøtter den indhentning, FE selv foretager.

FE's partnersamarbejde er opbygget over mange år og er baseret på gensidig tillid og fortrolighed. Det er en central spilleregel, at FE hverken be- eller afkræfter eksistensen af en samarbejdsrelation, heller ikke over for andre udenlandske partnere. Hvis FE's samarbejdspartnere får det indtryk, at FE ikke kan opretholde den fulde fortrolighed, vil konsekvensen typisk være, at relationen skades. 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 partnere foregår inden for rammerne af dansk lovgivning og Danmarks konventionsmæssige forpligtelser. Vi må ikke bede andre landes efterretningstjenester gøre noget, eller hjælpe med at gøre noget, som FE ikke selv må gøre.

FE har interne regler for, hvornår personidentificerbare oplysninger kan videregives til en partner. FE videregiver ikke oplysninger, hvis vi har konkret mistanke om, at de kan blive misbrugt til at danne grundlag for drab, tortur eller anden grusom, umenneskelig eller nedværdigende behandling.

Tilsynet med Efterretningstjenesterne fører blandt andet kontrol med FE's videregivelse af oplysninger om i Danmark hjemmehørende fysiske og juridiske personer til udenlandske partnere. Se mere om FE's lovgrundlag på side 52-53.

INDHENTNINGSSTATION, NORDJYLLAND

Antenner fra indhentningsstationen ved Hjørring. Den hvide kuppel er en radome, der er lavet af et særligt glasfiberstof, der holdes oppe af lufttryk. Radomen beskytter antennerne mod vind og vejr

Tredjelandsreglen

Den såkaldte tredjelandsregel går ud på, at oplysninger fra én efterretningstjeneste til en anden ikke må videregives til et tredjelands efterretningstjeneste eller en tredje part for den sags skyld. Reglen håndhæves strengt af efterretningstjenesterne for at undgå såkaldte falske bekræftelser, hvor forskellige versioner af den samme oplysning fejlagtigt bliver brugt til at bekræfte oplysningens rigtighed. Et brud på tredjelandsreglen kan også være med til at afsløre en efterretningstjenestes metoder og kapaciteter.

SØREN, ANALYTIKER

"Vores udenrigs- og sikkerhedspolitik bliver en gang imellem påvirket af terrorisme. Mit arbejde handler om at opnå en forståelse af, hvad terrorgrupperne vil og kan, og bruge den faglige indsigt til at give vores beslutningstagere et oplyst grundlag at træffe beslutninger på."

Produkter og kunder

Den efterretningsmæssige produktion til kunderne er en af FE's kerneopgaver, og den er det synlige resultat af hele FE's efterretningsarbejde. Produkterne omfatter både skriftlige rapporter, mundtlige briefinger og operative indsatser. Det er vores målsætning, at produkterne indeholder rettidige, relevante og troværdige efterretninger af høj kvalitet.

Flere gange om ugen, og ofte også flere gange om dagen, sender FE efterretningsrapporter til sine kunder. Modtagerne er hovedsageligt Statsministeriet, Udenrigsministeriet, Forsvarsministeriet og PET, herunder CTA. Forsvaret og udsendte styrker er ligeledes blandt FE's hovedkunder. Derudover har Center for Cybersikkerhed en række kunder, både private og offentlige, som det udfører tilsyn for og leverer produkter til på cyberområdet.

FE's produkter kan indgå som del af et beslutningsgrundlag, eksempelvis for folketingsbeslutninger om indsættelse af danske militære bidrag i forbindelse med internationale operationer. Produkterne bidrager også til at orientere den danske regering om udviklinger i udlandet af betydning for Danmarks sikkerhed. FE udarbejder forskellige skriftlige produkter såsom helt korte efterretningsvurderinger, mere detaljerede situations- og trusselsvurderinger og temasignaler om et givent emne. Derudover briefer FE ministre, embedsmænd og soldater, der skal udsendes.

FE lægger vægt på at være i tæt dialog med kunderne på alle niveauer. Det giver kunderne mulighed for at stille spørgsmål og komme med ønsker til FE's rapportering. Dialogen med kunderne foregår direkte med de fagpersoner i FE, der har den specifikke viden. Derudover gennemfører FE kundemøder, hvor samarbejdet og prioriteringen af FE's efterretningsmæssige fokusområder drøftes. Kundernes behov er således afgørende for FE's prioriteringer og bestemmende for efterretningskredsløbet (se side 32).

De fleste af FE's produkter er klassificerede. Vi tilstræber at klassificere produkterne lavest muligt for at sikre størst mulig anvendelighed hos kunderne. FE udfærdiger også enkelte ikke-klassificerede situations- og trusselsvurderinger, som er tilgængelige på FE's hjemmeside.

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

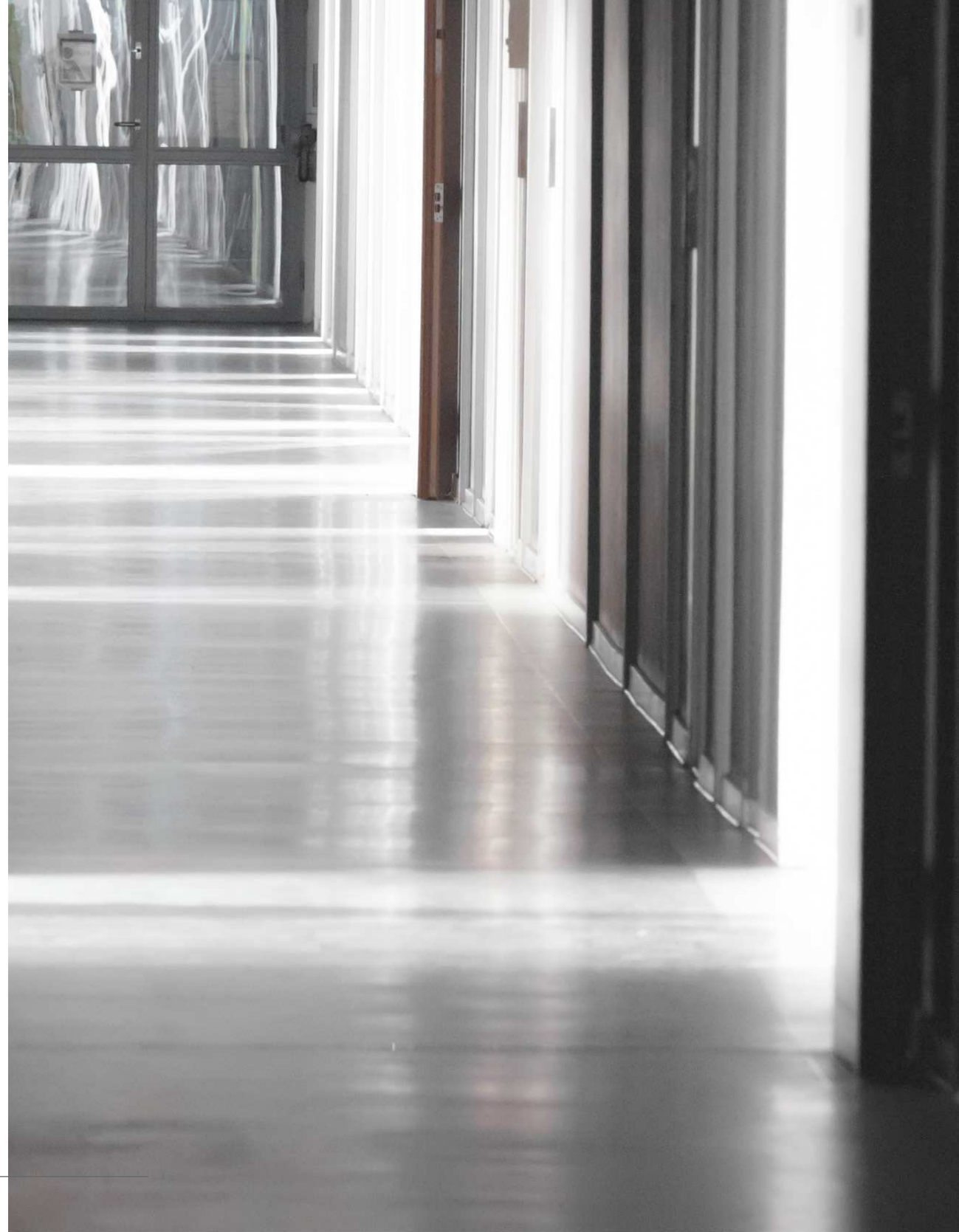
FE i medierne

I de seneste år har der i Danmark og på globalt plan været en øget debat om efterretningstjenesternes måde at arbejde på – og særligt hvilken betydning det har for den enkeltes privatliv. En af årsagerne til debatten er, at den tidligere efterretningsmedarbejder Edward Snowden i 2013 lækkede oplysninger om den amerikanske efterretningstjeneste NSA's arbejdsmetoder. I den forbindelse har der også været en del omtale og diskussion af FE's arbejde. NSA-lækagen har generelt givet anledning til mange spørgsmål og sået tvivl om efterretningstjenesternes virke.

Det er helt afgørende, at der hos beslutningstagerne og blandt borgerne er tillid til en efterretningstjeneste som FE og en tro på, at FE løser sine opgaver inden for specifikke lovmæssige beføjelser. Det kræver så stor åbenhed om vores arbejde som muligt.

FE har derfor flere gange kommenteret de danske mediers dækning af NSA-lækagen uden at gå på kompromis med de særlige forhold og sikkerhedshensyn, der gælder for en efterretningstjeneste. Vi har i den forbindelse søgt at uddybe en række forhold om vores efterretningsmæssige opgaver. Det gælder blandt andet spørgsmål om deling af information med udenlandske samarbejdspartnere og FE's indhentning af store datamængder i udlandet. Alt sker naturligvis i overensstemmelse med dansk lovgivning.

Center for Cybersikkerhed har en mere åben profil over for offentligheden end den efterretningsmæssige del af FE. Centerets arbejde med cybersikkerhed er primært af betydning for danske myndigheder og virksomheder, hvilket forudsætter en langt mere synlig og udadvendt rolle. På den baggrund bidrager og deltager Center for Cybersikkerhed aktivt med sin specialviden i debatten og bliver som nationalt kompetencecenter for cybersikkerhed ofte citeret på området i de danske medier.



SANDAGERGÅRD, AMAGER

RAMMER

INDHENTNINGSSTATION, AMAGER

Ressourcer og medarbejdere

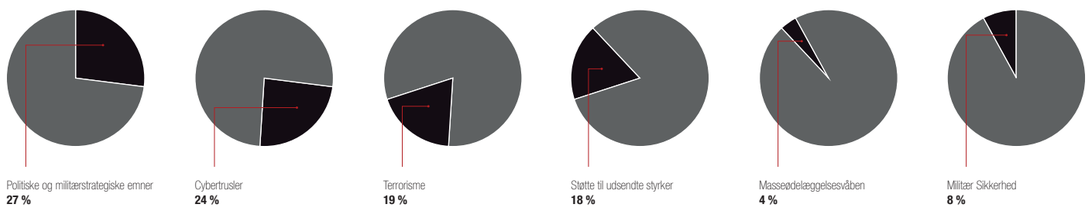
FE er en vidensorganisation, der løser mange typer opgaver inden for en række specialiserede fagområder. Medarbejderne er afgørende for, at FE kan løse sine opgaver, og der er brug for personer med forskellige og ofte helt særlige kompetencer.

Der er i FE stor faglig spændvidde. Den største medarbejdergruppe er akademikerne, som samlet udgør knapt halvdelen af de ansatte. Gruppen af akademikere er steget gennem årene, i takt med at FE har ændret sine opgaver og fokus. De militære medarbejdere udgør 13 procent, hvoraf godt halvdelen er officerer.

En betydelig gruppe af medarbejderne har en it- eller teknisk uddannelse, mens andre medarbejdere udfører administrative opgaver inden for økonomi, sekretærbistand og personaleadministration. Det afgørende er, at medarbejderne er gode til at samarbejde og dele viden på tværs af fagligheder og på tværs af organisationen, for at FE kan opnå de bedste resultater.

MEDARBEJDERE FORDELT PÅ FE'S OVERORDNEDE FOKUSOMRÅDER*

*Fordelingen er ikke sammenlignelig med den angivne fordeling i FE beretning 2011-2012 på grund af ny organisationsstruktur



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 2013 på 621 mio. kr. og i 2014 på 674 mio. kr. I 2015 er FE's bevilling på 675 mio. kr. Stigningen i 2014 og 2015 skyldes forsvarsforligets treårige engangsbevilling på i alt 100 mio. kr. til samling af FE i et nyt domicil. Derudover har partierne bag forsvarsforliget aftalt, at FE i 2015 tilføres yderligere ca. 50 mio. kr. til finansiering af styrkelsen af FE's indsats mod terror.

FE bruger en væsentlig del af bevillingen til lønninger. Derudover er der udgifter til almindelig drift af udstyr og bygninger. Især driften af den elektroniske indhentning er ressourcekrævende, ligesom FE bruger ressourcer på løbende at udvikle sine indhentningskapaciteter, så de er på højde med den teknologiske udvikling.

FE oplyser ikke konkrete tal for medarbejderstab, og hvor mange ressourcer der bruges til almindelig drift. Forklaringen er, at de, der truer Danmark og danske interesser, ikke skal have indblik i omfanget af vores kapaciteter.

FE's personalepolitik adskiller sig ikke fra de fleste andre virksomheders og organisationers. Vi ønsker at være en veldrevet og attraktiv arbejdsplads, der tiltrækker og fastholder de bedste medarbejdere. Både på det analytiske og på det teknologiske felt går udviklingen rigtig stærkt, så forandring er en nødvendighed. Det stiller krav til medarbejderne i FE, som ud over at besidde en stor faglighed også skal være i stand til hurtigt at omstille sig til nye opgaver og arbejdsmetoder.

UDDANNELSESMÆSSIG BAGGRUND

FE's akademikere under kontorchefsniveau, i procent

Medarbejdertyper

FE har mange forskellige typer af medarbejdere. Det kan være teknikere og it-kyndige medarbejdere til FE's elektroniske indhentning og sikkerhed, føringsofficerer med særlige kontaktskabende egenskaber, operative teamledere samt analytikere og bearbejdere med forskellige specialer. Her følger en række eksempler på FE's medarbejdertyper:

DEN ELEKTRONISKE INDHENTER

Elektronisk indhentning (SIGINT) er komplekst og 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, både for at skaffe efterretninger og for at forsvare systemer. Netværksmedarbejderen har et dybt kendskab til internettets struktur, computere, programmer og applikationer. I Center for Cybersikkerhed 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 Center for Cybersikkerhed 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 eller indhenteren skaffer oplysninger fra menneskelige kilder, altså personer, som videregiver ofte følsomme oplysninger til føringsofficeren. Føringsofficeren skal være god til at få alle typer af mennesker i tale og til at håndtere stress og uforudsete situationer. Man 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.

TEAMLEDEREN

Efterretningsarbejdet er en holdindsats. Teamlederen har som hovedopgave at bevare specialisternes fokus på at nå de fælles mål. Det sker i en koordineret og prioriteret rækkefølge, hvor teamlederen skal sikre, at den rette indhentning dækker FE's efterretningsbehov bedst muligt. Teamlederen har oftest en lang videregående uddannelse kombineret med et godt kendskab til efterretningskredsløbet og FE's organisation.

BEARBEJDEREN

Bearbejderen kan typisk et eller flere fremmedsprog på højeste niveau. Ud over gode 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 komplekse data, forstå deres politiske og kulturelle sammenhæng og udvælge og oversætte de relevante oplysninger til analytikerne. Typisk har bearbejderen en lang videregående sproglig og/eller samfundsvidenskabelig uddannelse.

ANALYTIKEREN

Analytikerens arbejdsområde er defineret geografisk (eksempelvis Mellemøsten eller Rusland) eller emnemæssigt (eksempelvis terror- eller cybertrusler). Analytikeren skal foruden et grundigt fagligt kendskab til sit område have forståelse for indhentningens muligheder, blandt andet på det teknologiske område, samt blik for nye efterretningsmæssige mål, der måtte dukke op. 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.

"AYMAN", BEARBEJDER

"Mit arbejde kræver, at man kender sproget på modersmålsniveau, da der kan være mange forskellige dialekter. Jeg skal kunne beskrive situationer mellem folk – også når der ikke bliver sagt noget."

Organisation

FE er overordnet organiseret i fire sektorer samt en juridisk afdeling og et ledelsessekretariat. Hver af de fire sektorer er opdelt i en række afdelinger.

Indhentningssektoren
Sektoren har ansvaret for at indsamle informationer og stille dem til rådighed for FE's analytikere. Indhentningssektoren består af fem afdelinger.

Analysesektoren
Sektoren har ansvaret for at bearbejde og analysere FE's informationer og formidle dem som efterretninger til FE's kunder. Analysesektoren består af fire afdelinger.

Indhentningssektoren og Analysesektoren udgør tilsammen kernen i det såkaldte efterretningskredsløb. Et nært samarbejde på alle niveauer på tværs af de to sektorer foregår både uformelt og formelt gennem operative teams mv.

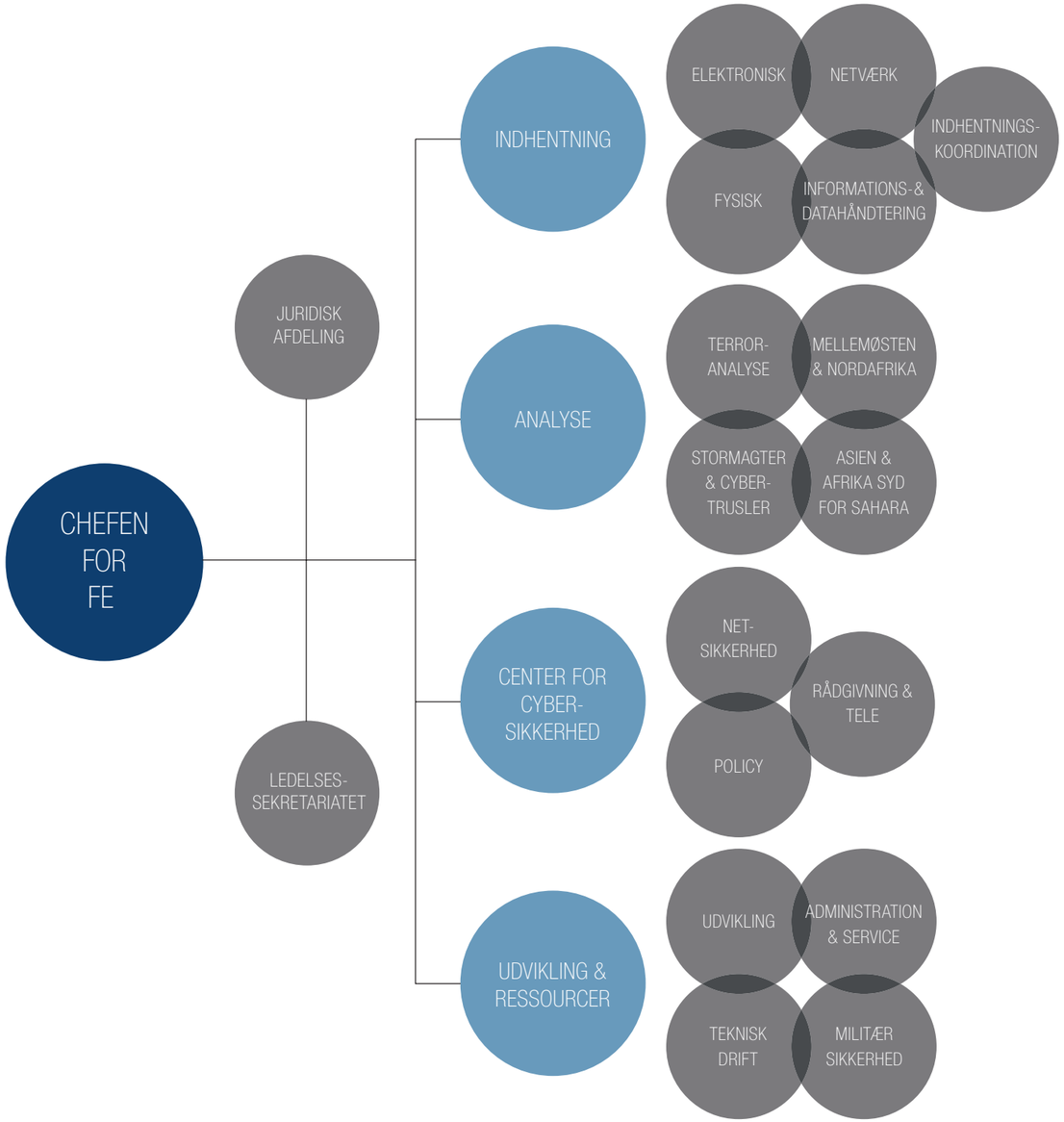
Center for Cybersikkerhed
Centeret varetager opgaverne som national it-sikkerhedsmyndighed, netsikkerhedstjeneste og kompetencecenter på cybersikkerhedsområdet. Centeret varetager desuden FE's kommunikationsopgaver. Centeret udgør samtidig en sektor i FE og består af tre afdelinger.

Udviklings- og Ressourcesektoren
Sektoren har ansvaret for FE's udviklings- og driftsopgaver, herunder teknisk drift og administration, samt for den militære sikkerhedsopgave. Udviklings- og Ressourcesektoren består af fire afdelinger.

Juridisk afdeling
Afdelingen har ansvaret for de juridiske opgaver i FE, herunder Center for Cybersikkerhed, og rådgiver blandt andet FE's ledelse om juridiske spørgsmål i forhold til lov om FE og lov om Center for Cybersikkerhed.

Ledelsessekretariatet
Ledelsessekretariatet støtter chefen for FE og FE's ledelsesgruppe. Afdelingen varetager samtidig forbindelsen til og koordination af samarbejdet med FE's udenlandske samarbejdspartnere.

FE's ledelsesgruppe består af chefen for FE og cheferne for hver af de fire sektorer.



Lovgrundlag

Selvstændigt lovgrundlag for FE's virksomhed
2014 var lovgivningsmæssigt et særligt år for FE. To nye selvstændige love regulerer nu vores virksomhed og opgaver: lov om Forsvarets Efterretningstjeneste og lov om Center for Cybersikkerhed. Tidligere var FE's virksomhed og opgaver reguleret af en enkelt paragraf i forsvarsloven, af retningslinjer og direktiver udstedt af Forsvarsministeriet samt af interne FE-direktiver. Med den nye lovregulering er der skabt større åbenhed om FE's opgaver, metoder og kontrollen med FE.

FE-loven
1. januar 2014 trådte lov om Forsvarets Efterretningstjeneste i kraft (lov nr. 602 af 12. juni 2013), i daglig tale FE-loven. FE-loven beskriver i detaljer FE's opgaver som Danmarks udenrigs- og militære efterretningstjeneste, herunder opgaven som militær sikkerhedstjeneste, og at FE gennem Center for Cybersikkerhed varetager opgaven som Danmarks nationale it-sikkerhedsmyndighed.

FE-loven bygger i al væsentlighed på Wendler Pedersen-udvalgets betænkning og lovudkast fra februar 2012. Et bredt flertal i Folketinget vedtog FE-loven i juni 2013.

De vigtigste elementer i FE-loven:
- En detaljeret beskrivelse af FE's opgaver.
- Regler for FE's indsamling og indhentning af oplysninger, elektronisk såvel som fysisk.
- Regler for, hvornår og hvordan FE må behandle oplysninger om danske statsborgere samt personer og virksomheder, der har en nærmere tilknytning til Danmark. I FE-loven kaldet "i Danmark hjemmehørende fysiske og juridiske personer".
- Regler for, hvornår FE må videregive oplysninger om i Danmark hjemmehørende fysiske og juridiske personer samt retningslinjer for videregivelse af ikke-behandlede data, såkaldte rådata.
- Regler for, hvornår FE skal slette oplysninger om i Danmark hjemmehørende fysiske og juridiske personer.
- Personer kan anmode Tilsynet med Efterretningstjenesterne (tilsynet) om at undersøge, hvorvidt FE uberettiget behandler oplysninger om i Danmark hjemmehørende fysiske eller juridiske personer.
- Etablering af tilsynet som en ny og uafhængig kontrolinstans, der fører tilsyn med FE. Tilsynet kan kræve at få indsigt i enhver oplysning og alt materiale, der kan være af betydning for udøvelsen af kontrollen.

Der er på baggrund af FE-loven udarbejdet interne retningslinjer, der sammen med undervisning af medarbejderne i FE-loven sikrer, at FE efterlever loven.

Lov om Center for Cybersikkerhed
Ved oprettelsen af Center for Cybersikkerhed i 2012 blev det besluttet, at centerets virksomhed skulle reguleres ved lov, hvilket også fremgår af FE-loven. I juni 2014 vedtog Folketinget lov om Center for Cybersikkerhed (lov nr. 713 af 25. juni 2014) eller CFCS-loven, der giver et samlet lovgrundlag for centeret. Loven trådte i kraft 1. juli 2014.

De vigtigste elementer i CFCS-loven:
- Regler for Center for Cybersikkerheds behandling af personoplysninger, der sikrer, at centeret er omfattet af de centrale principper i persondataloven, offentlighedsloven og forvaltningsloven.
- Regler for indsamling og behandling af data ved centerets netsikkerhedstjeneste, som har til opgave at opdage, analysere og bidrage til at imødegå sikkerhedshændelser hos myndigheder og virksomheder tilsluttet netsikkerhedstjenesten.
- Regler for myndigheders og virksomheders tilslutning til netsikkerhedstjenesten.
- Regler for opbevaring, sletning og videregivelse af data, der stammer fra indgreb i meddelelseshemmeligheden i forbindelse med varetagelse af netsikkerhedstjenestens opgaver.
- Et styrket tilsyn med Center for Cybersikkerhed, idet tilsynsopgaven nu er placeret ved tilsynet.

FE har etableret en særlig compliance-funktion, der medvirker til, at Center for Cybersikkerhed efterlever gældende love og regler samt interne procedurer og relevante standarder. Som led i compliance-funktionen underviser centerets jurister også nye medarbejdere i CFCS-loven og sikrer, at centerets interne procedurer lever op til de krav, som følger af loven.

SANDAGERGÅRD, AMAGER

Tilsynet med Efterretningstjenesterne

Landsdommer Ulla Staal, Østre Landsret (formand)
Advokat Pernille Backhausen, Sirius Advokater
Professor Jørgen Grønnegaard Christensen, Aarhus Universitet
Direktør Adam Wolf, Danske Regioner
Bestyrelsesformand Erik Jacobsen, Roskilde Universitet

Kontrol med FE

Der føres på flere områder kontrol med, om FE overholder de gældende regler, som efterretningstjenesten skal arbejde efter. Forsvarsministeren har på regeringens vegne den overordnede kontrol med FE. Derudover har Folketingets Udvalg vedrørende Efterretningstjenesterne (i daglig tale Kontroludvalget) ført kontrol med efterretningstjenesterne siden 1988. Kontroludvalget består af repræsentanter fra de fem største partier i Folketinget.

Ud over den parlamentariske kontrol er FE også underlagt bevillingsmæssig kontrol, som Rigsrevisionen står for. Revisionen gennemføres principielt på samme måde som revisionen af statens øvrige regnskaber.

Tilsynet med Efterretningstjenesterne

Tilsynet med Efterretningstjenesterne har siden januar 2014 ført kontrol med Danmarks to efterretningstjenester: PET og FE. Tilsynet, der har erstattet det tidligere Wamberg-udvalg, udøver sine funktioner selvstændigt og i fuld uafhængighed. Tilsynet har desuden siden juli 2014 ført kontrol med Center for Cybersikkerhed og har erstattet det tidligere GovCERT-tilsyn.

Tilsynets virksomhed og opgaver er forskellige, afhængigt af om tilsynet er rettet mod FE's efterretningsmæssige virksomhed i medfør af FE-loven eller mod Center for Cybersikkerheds virksomhed i medfør af CFCS-loven.

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 eget kontor hos FE, hvorfra det har adgang til alle oplysninger, der kan være af betydning for dets virksomhed. Tilsynet har i den forbindelse blandt andet modtaget detaljerede beskrivelser af FE's og Center for Cybersikkerheds it-systemer og arbejdsprocesser, og medlemmerne er blevet undervist i de relevante systemer, så de selv kan arbejde i systemerne med henblik på at udføre den nødvendige kontrol. Tilsynet er løbende i kontakt med tjenestens jurister, ligesom FE's øvrige specialister deltager i møderne med tilsynet efter behov. Tilsynets sekretariat anvender gennemsnitligt to arbejdsdage om ugen i FE.

Tilsynet kan som led i sin virksomhed afgive udtalelser til FE – det vil sige henstillinger, som FE forventes at følge. Tilsynet kan dog ikke pålægge FE at ophøre med en given aktivitet. Hvis FE helt undtagelsesvis skulle beslutte ikke at følge en henstilling fra tilsynet, skal sagen forelægges for forsvarsministeren. Beslutter ministeren ikke at følge henstillingen fra tilsynet, er regeringen forpligtet til at orientere Folketingets Kontroludvalg. På den måde sikres det, at der også er parlamentarisk kontrol med de forhold, som tilsynet måtte opfatte som kritiske. Tilsynet skal også underrette forsvarsministeren om forhold, som ministeren efter tilsynets opfattelse bør have kenskab til.

Med det nye tilsyn er der sket en markant styrkelse af kontrollen med FE's indhentning, behandling og videregivelse af personoplysninger. Læs mere på tilsynets hjemmeside www.tet.dk, hvor også tilsynets årlige redegørelser om dets virksomhed er offentliggjort.

Tilsynets årsredegørelse 2014

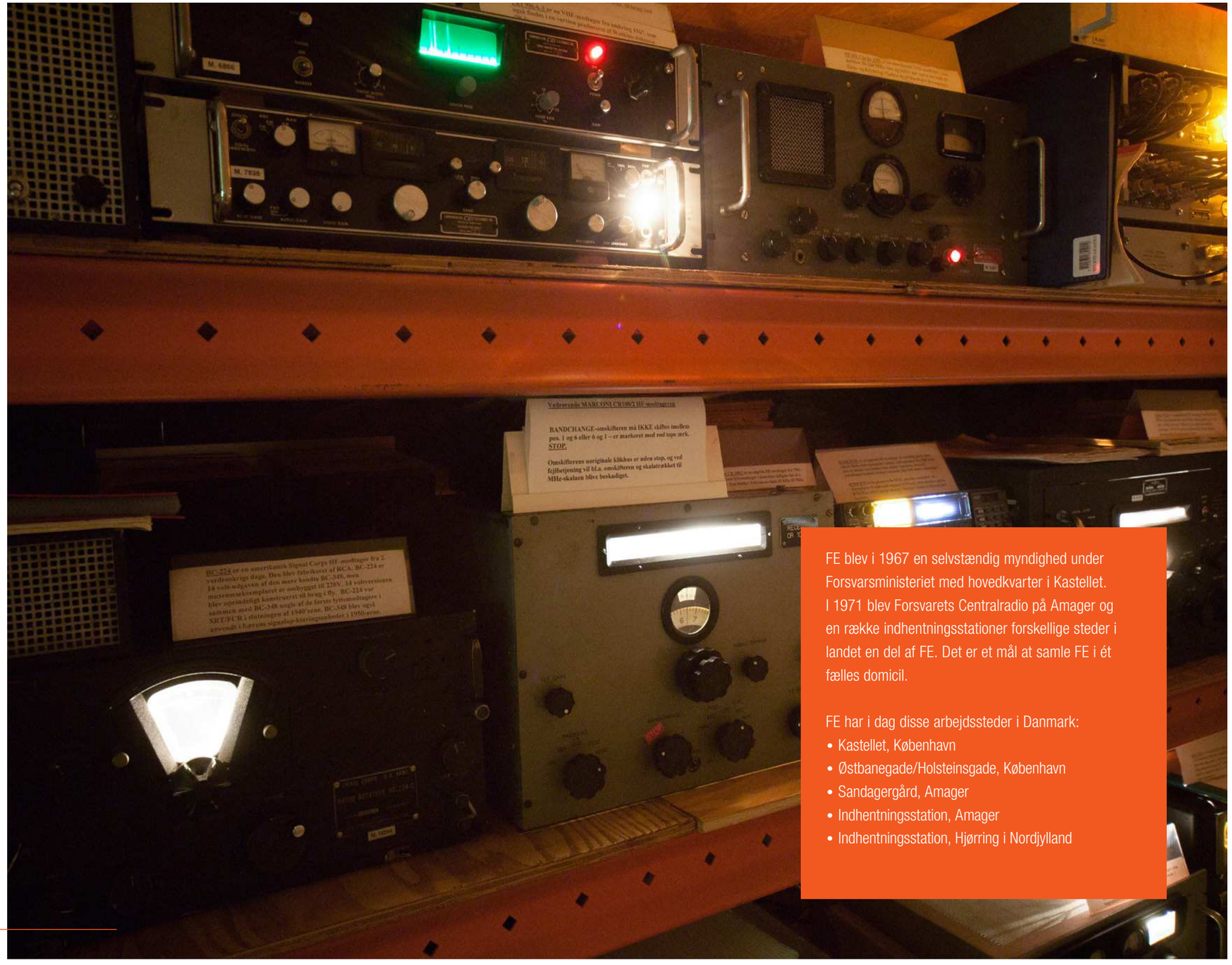
"På baggrund af tilsynets kontroller med FE og tjenestens rettidige udarbejdelse af interne retningslinjer og tilrettelæggelse af procedurer i overensstemmelse hermed er det tilsynets vurdering, at FE har haft betydelig fokus på at sikre implementeringen af FE-loven."

Fælles domicil

Langt de fleste medarbejdere er fysisk placeret i FE's bygninger i Kastellet og i et bygningskompleks på Amager, kaldet Sandagergård, samt i lokaler på Østerbro i København, hvor blandt andet Center for Cybersikkerhed er placeret. Derudover har FE to indhentningsstationer på henholdsvis Amager og i Nordjylland nær Hjørring. FE har også medarbejdere, der arbejder i udlandet i kortere eller længere perioder.

Den meget spredte placering af medarbejderne medfører både store udgifter og er uhensigtsmæssig for samarbejdet på tværs i organisationen. I forsvarsforliget 2013-2017 blev der afsat midler til, at FE's aktiviteter i københavnsområdet kan samles i ét domicil for at styrke FE's virksomhed.

FE har gennem en længere periode arbejdet sammen med Forsvarsministeriets Ejendomsstyrelse og Bygningsstyrelsen om at finde et egnet sted at samle FE. Samling af tjenesten vil skabe yderligere synergi mellem de forskellige opgaver, som FE løser. En mere samlet placering vil gøre FE bedre til at løse sine opgaver og udnytte ressourcerne effektivt.



FE blev i 1967 en selvstændig myndighed under Forsvarsministeriet med hovedkvarter i Kastellet. I 1971 blev Forsvarets Centralradio på Amager og en række indhentningsstationer forskellige steder i landet en del af FE. Det er et mål at samle FE i ét fælles domicil.

FE har i dag disse arbejdssteder i Danmark:
- Kastellet, København
- Østbanegade/Holsteinsgade, København
- Sandagergård, Amager
- Indhentningsstation, Amager
- Indhentningsstation, Hjørring i Nordjylland

GAMMELT UDSTYR FRA FE'S SAMLING

Forsvarets Efterretningstjeneste
Beretning udgivet oktober 2015
Design: Kontrapunkt
Fotos: CphCph
Oplag: 2.500
Trykkeri: PE offset

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