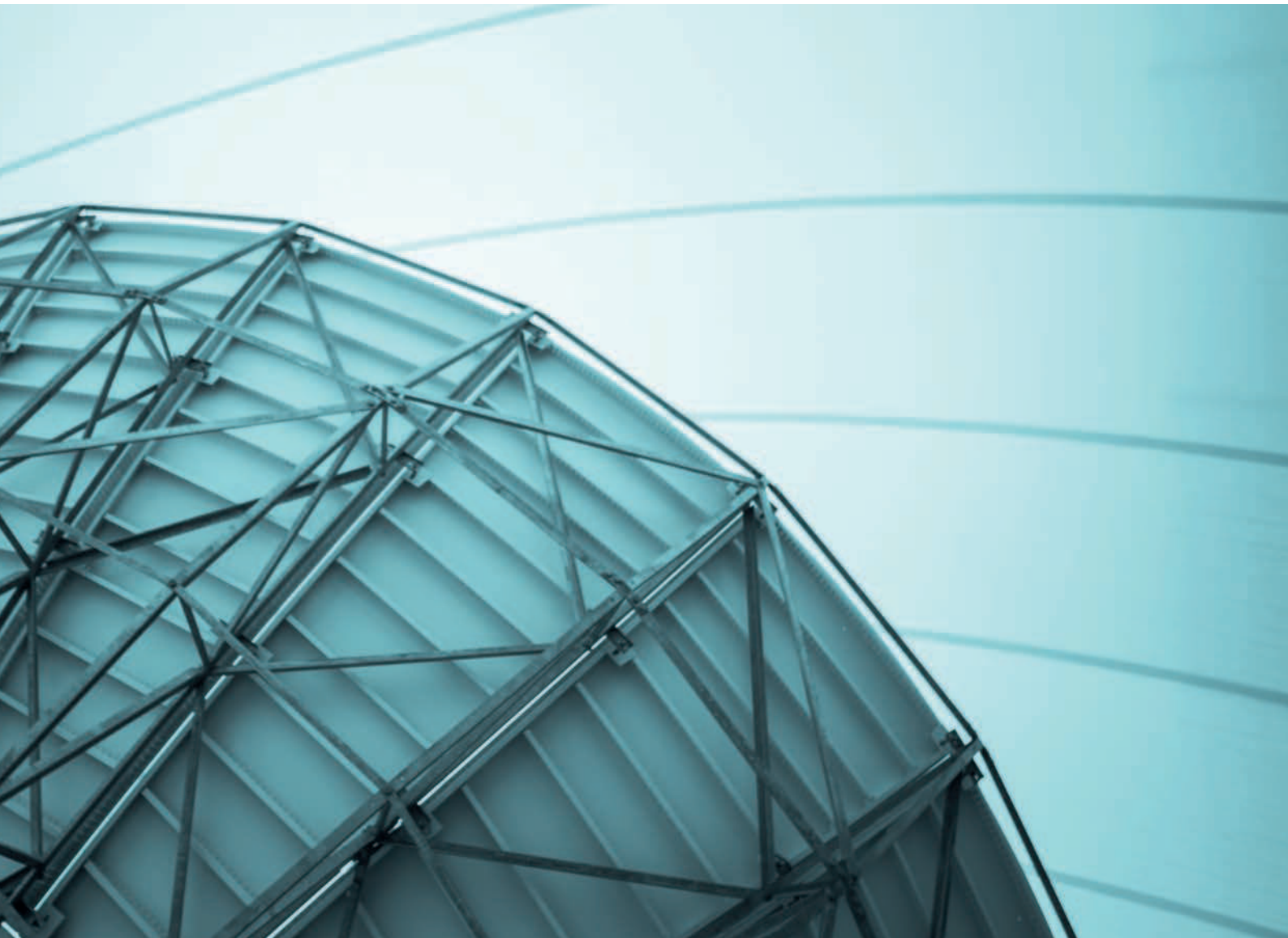
Indhentningsdiscipliner

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 data-overførsler 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.

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.