



Undgå spionage
- for din sikkerheds skyld



**FE Forsvarets
Efterretningstjeneste**

Kastellet 30
2100 København Ø

Telefon 33 32 55 66

Telefax 33 93 13 20

E-mail fe@fe-mail.dk

Web www.fe-ddis.dk

Forord

Forud for et fjendtligt angreb har modstanderen typisk indhentet informationer, spioneret, så hans angreb får størst succes for ham - og dermed skader os mest muligt.

Derfor er det afgørende for sikkerheden at gøre det så svært som muligt for vores modstandere at få informationer om lejren, kasernen, operationerne etc.

Formålet med denne folder er at øge bevidstheden om sikkerhed og vise, hvordan spionage udgør en afgørende forudsætning for de trusler, man er udsat for under en udsendelse. Men også i dagligdagen herhjemme er principperne fornuftige at huske på.

Det er i missionsområdet, at man kan blive dræbt som følge af spionage. Husk, udsendelsen begynder allerede ved opstillingen af enheden i Danmark, og det gør risikoen for fjendtlig indhentning af informationer også. Derfor skal sikkerhedsbevidstheden være på plads fra begyndelsen.

Truslen fra spionage er næsten usynlig. Spioner forsøger netop at undgå opmærksomhed. Spionage - indhentning af oplysninger - gennemføres bedst, når man glemmer, at truslen findes. Men spionage er meget udbredt, og spionage rettes også mod 'almindelige' soldater. Spionage udgør en direkte trussel i mange missionsområder.

Derfor er høj grad af sikkerhed (beskyttelse af operativ planlægning, kommunikationslinjer osv.) afgørende - også selv om det nogle gange virker besværligt. Manglende sikkerhed kan i yderste konsekvens koste dig eller dine kammerater livet.

Denne folder bygger på erfaringer, som er gjort af danske og allierede styrker på missioner i Balkan, Irak, Afghanistan og som FN-observatører.

"Formålet med militær sikkerhed er at beskytte forsvaret, herunder personel, materiel, dokumenter, elektroniske informationssystemer, operationer samt etableringer mod den sikkerhedsmæssige trussel med henblik på at opnå den højest mulige grad af sikkerhed." (FKOBST 358-1).

Hvad er spionage?

Enhver aktivitet, gennemført med alle menneskelige og tekniske midler for at tilegne sig de oplysninger, som vi ønsker at holde for os selv, er spionage.

Hvorfor interessere sig for spionage?

Indhentning af oplysninger er en forudsætning for at kunne gennemføre en operation. I februar 2006 i Tonbridge syd for London gennemførte en gruppe personer et røveri mod et pengedepot. Udbyttet blev 53 mio. £. Aktionen blev gennemført ved at kidnappe depotchefens familie og med dem som gidsler tvinge chefen til at få depotvakterne til at lukke gruppen ind.



Røveriet i Tonbridge. Røvernes lastvogn fotograferet af depotets overvågningskamera, da den kørte væk med 53 mio. £. Kilde: *The Guardian* 24. februar 2006.

Forud for operationen er der foregået spionage. Indhentningen er sket gennem overvågning og gennemgang af åbne kilder. Man har fundet ud af, hvem chefen er, fundet hans adresse, afkodet hans families rutiner, noteret tider for vagtskifte, undersøgt vagternes mulighed for at udløse alarmer osv.

Fra eksemplet kan man drage direkte paralleller til en terrorgruppes forberedelse af et angreb. Hvem vil man ramme? Danskere? Hvor kører vi patruljer? Hvornår kommer den næste? Hvordan

beskytter vi os mod angreb aktivt som passivt? Hvilke frekvenser taler vi på? Hvor lang tid går der, før en patrulje under angreb kan få støtte? Og så videre. Disse oplysninger er ikke umiddelbart tilgængelige. Derfor må modstanderen få dem gennem forskellige former for spionage, f.eks. ved overvågning og aflytning af radiokommunikation.

Hvem udfører spionage?

- når stater spionerer...

Staters holdning til spionage er tvetydig: På den ene side er spionage en alvorlig forbrydelse i de fleste lande. På den anden side har de fleste stater organisationer, der har til opgave at spionere mod andre lande eller organisationer for at give statens ledere det bedst mulige beslutningsgrundlag.

Stater har ofte betydelige ressourcer til spionage og har teknisk udstyr som f.eks. satellitter, lyttestationer, udstyr til afkodning (dekryptering) af signaler og avanceret kommunikations- og overvågningsudstyr. Stater kan også have et netværk af spioner - kilder - til at indhente oplysninger og analytikere til at bearbejde informationerne.

Ud over de efterretningstjenester, der har fokus uden for landets grænser, råder de fleste stater militær, politi og lignende sikkerhedstjenester over organisationer, der arbejder mod indre fjender - såkaldt *kontra*etterretningstjeneste - eller på engelsk Counter Intelligence (CI). I mange operationsområder er disse sikkerhedstjenester samarbejdspartnere i arbejdet for at sikre stabilitet og sikkerhed. Men efterretningstjenesterne kan samtidig være præget af korrupsion eller loyalitet over for f.eks. tidligere ledere, etniske grupper eller nationale mindretal. Tjenesternes personel kan endvidere være udsat for trusler. Hvad enten årsagen er trusler, sympati for modstanderne eller simpel korrupsion, kan disse efterretningstjenester altså udgøre en alvorlig risiko for lækager. Det er således en hårfin grænse at samarbejde og være årvågen.

- når andre spionerer...

Terrorister og den organiserede kriminalitet udgør ofte den mest direkte trussel mod den udsendte soldat.

Oprørere og terrorister spionerer blandt andet for at kunne ramme den udsendte enhed og de lokale, der samarbejder med den.

Organiseret kriminalitet spionerer:

- for at kunne omgå vores aktiviteter
- for at kunne udnytte vores tilstedeværelse, f.eks. vores logistik ved at finde 'svage led', åbninger for afpresning, korrupsion osv.
- for at kunne slå igen, hvis vore aktiviteter truer de kriminelle strukturers overlevelse

Der vil ofte være et samarbejde mellem oprørsgrupper og organiseret kriminalitet, hvor man deler oplysninger og varsler hinanden om vores aktiviteter.

Ikke-statslige organisationer har færre resourcer til spionage. Til gengæld er de som regel på hjemmebane, og de er ikke hæmmet af

love og regler. De kan ved mord og trusler mod f.eks. lokalansatte få adgang til alt, hvad de ved. Man skal heller ikke undervurdere kriminelles og terroristers adgang til tekniske midler. Avancerede midler til skjult overvågning, rumaflytning, scanning af mobiltelefoni og almindelig radiokommunikation kan købes på internettet for overkommelige beløb.

Hvem retter spionage sig imod?

Spionage retter sig mod alle!

Modstanderen søger sine oplysninger, hvor han kan. Selvfølgelig er centralt placerede førstehåndskilder med adgang til kommende operationer eller kommunikation højt prioriterede mål. Men den menige soldat, der på velfærdstelefonen fortæller sin kæreste, at de skal patruljere i Geresk i morgen, har i bedste fald advaret de mennesker i Geresk, patruljen skulle overraske. I værste fald har han givet oplysninger, der giver modstanderen mulighed for at angribe patruljen.



Oprørere? Terrorister? Kriminelle? Uanset hvad man kalder dem, indhenter de oplysninger for at kunne ramme os. Dansk køretøj ramt af nedgravet bombe i Afghanistan. Kilde: Forsvarets Mediecenter.

Hvordan gennemføres spionage?



Satellitfoto af tidligere dansk lejr i Bosnien, hentet med Google Earth.

Spionage kan f.eks. ske ved, at lokale er øjne og ører for modstanderen (kaldes HUMINT), ved indhentning og analyse på baggrund af billedmateriale, f.eks. billeder taget fra fly eller satellitter (kaldet IMINT) eller ved at bruge åbne kilder som aviser, internet, statistikker, biblioteker osv. (kaldet OSINT).

Når mennesker spionerer ...

HUMINT er indhentning af oplysninger, der udføres 'på jorden' af mennesker. Her er et par typiske eksempler; alle taget fra missioner med dansk deltagelse.

The screenshot shows the top of a USA Today news page. The navigation bar includes links for Home, News, Travel, Money, Sports, Life, Tech, and World. The main headline reads: "Taliban says it beheads 4 Afghans, calling them spies for U.S.-led forces". Below the headline is a sub-headline: "Taliban says it beheads 4 Afghans, calling them spies for U.S.-led forces". The article is dated "Posted 6/23/2008 3:22 PM ET". There is a small photo of a soldier in military gear. The article text begins: "KANDAHAR, Afghanistan (AP) — A purported spokesman for the Taliban said Friday that the militant group had beheaded four Afghans it accused of spying for U.S.-led forces. The men were abducted at gunpoint by armed men and their headless bodies were dumped in the southern province of Zabul and found Thursday and Friday, said Ali Khail, a spokesman for the provincial governor. Meanwhile, coalition and Afghan forces announced that they had destroyed a bunker used by insurgents, killing 17 of them Wednesday in southern Afghanistan, where the militants have been launching increasingly bold attacks. The fighters were intercepted as they traveled back and forth from their bunker to set up an ambush near Tirin Kot, the"

I missionsområderne myrdes folk af terrorister og kriminelle, hvis de mistænkes for at give de internationale styrker oplysninger. Derfor er kilder og efterretninger, der kan spores "need to know". Kilde: USA TODAY.

Lækagen

En lokal sikkerhedstjeneste skal deltage i en operation. En af de lokale officerer advarer vore modstandere om operationen og angiver ruten frem til målet. Modstanderen planlægger et baghold for kolonnen. Da vi nærmer os, kontakter den lokale officer modstanderen og melder, hvilken bil han selv kører i.

Honey trap'en - den forførende spion

En officer møder en lokal pige og sød musik opstår. Efterfølgende kontaktes officeren med et krav om at spionere for en lokal tjeneste. Hvis ikke han samarbejder, vil hans kone få alt at vide - med billeder. Officeren nægter og konfronteres derpå med en trussel om anklage for voldtægt. Kvinder i forsvaret har også mødt sympatiske, lokale mænd.

Rengøringskonen

Rengøringskonen tømmer skraldespandene. Stabshjælperen sjusker med destruktion af kalender og printede forarbejder til operationsbefalinger, og rengøringskonen tager dem med ud af lejren. Hun noterer sig også listen med underafdelingens køretøjer, der hænger på gangen og ser, hvornår de er afgivet til delingerne, og hvornår de skal vedligeholdes. Hun husker navnene på personellisterne og tegner en skitse over lejren. Hun noterer sig nedslagene fra sidste uges raketangreb på lejren og kan melde, hvor langt og i hvilken retning de lå fra messefaciliteterne. Hun taler med soldaterne om deres liv, familie og indstilling til lokale forhold og melder videre om enhedens moral og mulige svage punkter.

Tolken

Den søde kvindelige tolk er god at snakke med på de lange patruljer. Og hun melder videre. Den dygtige mandlige tolk, der har arbejdet for enheden i årevis, taler dansk. Men han afslører det ikke. Tolken får lov at tage sin mobiltelefon med og advarer sin kontaktperson om målet for patruljen med en SMS. Tolken bliver debriefet af sin kontaktperson efter dagens tjeneste om hvem

Ved indgangen til en lejr, hvor lokalansatte ikke må have mobiltelefoner, blev en lastvogn stoppet og ved en grundig eftersøgning fandt man syv mobiltelefoner gemt på bilen...

patruljen har talt med og hvad de har talt om. Den kriminelle organisation, der debriefer ham, er den samme, der i sin tid sørgede for, at han fik mulighed for at søge arbejde ved den udsendte enhed.

Overvågeren

Ejeren af en af boderne langs vejen op til lejren noterer sig tider og sammensætning af trafikken. Han videregiver oplysninger til en mand, der kommer forbi en gang om ugen. Hvis en patrulje er over en vis størrelse, er af usædvanlig sammensætning eller lignende, ringer han til et bestemt nummer, sender en e-mail eller en SMS. Et andet sted efterlader en gruppe en bil foran lejren. Andre noterer sig, hvor lang tid der går, før vagten reagerer. Den efterfølgende afsøgning af bilen videofilmes.

Lokalansatte optræder flere steder i eksemplerne. Lokalansatte udgør *altid* en sikkerhedsrisiko. Lokalansatte vil altid være oplagte kilder til oplysninger for modstanderen, fordi:

- lokalansatte kan trues til at indhente og videregive oplysninger. Truslen kan rettes mod dem selv eller deres familier
- lokalansatte kan bestikkes til at videregive oplysninger. Deres ansættelse er måske betinget af, at lokale kriminelle overhovedet tillader dem at have jobbet
- lokalansatte kan have sympati for modstanderen og den sag, modstanderen kæmper for.



Vær sikkerhedsbevidst: der kan være nogen, der forstår, hvad du siger. Kilde: FE fototjeneste.

Tolke er oplagte til at varetage modstanderens indhentning. Men rengøringspersonale, folk med boder i lejren og de, der kører affald væk, kan alle komme med værdifulde oplysninger for modstanderen. Som soldat i en mission kommer du og din enhed ud til områder, der er præget af kaos. Det er ofte vanskeligt at kontrollere lokales fortid og identitet. I bedste fald er en lokalansat en loyal medarbejder, der kun modvilligt og under pres videregiver oplysninger. I værste fald er en lokalansat en aktiv spion.

Når vi forærer informationerne...

Vi har alle fået adgang til åbne medier som f.eks. internettet, hvor det er vigtigt at overveje, hvad man eksponerer. Det samme gælder, når man udtaler sig til pressen.

Eksponering er den grad, man giver andre direkte adgang til ens personlige oplysninger - i første omgang ens navn. Prøv at undgå efternavn på navneskilt, ved telefonsamtaler, på internettet, i emails eller i pressen, når du er udsendt.

Fuldt navn gør det let for andre at finde frem til dig og dine pårørende. Står man frem med navn, er man kun et par opslag på internettet fra,

at enhver kan finde ens hjemadresse. Der har været flere tilfælde, hvor udsendtes familier er blevet truet over telefonen.

Man eksponerer sig også ved at have navnelister med fuldt navn hængende fremme i lejren i missionsområdet, hvor lokalansatte kan se dem. Pas generelt på dokumentets sikkerhed. Hemmelige dokumenter skal behandles som hemmelige og må ikke behandles, som var de klassificeret til 'tjenestebrug', som der er set eksempler på i missioner.

Personlige hjemmesider eller uofficielle enhedshjemmesider skal man bruge med omtanke. Læs også folderne "Hold kontakten - men med omtanke" og "Brug internettet - men med omtanke".

Internettet med Facebook, blogs etc. bruges ofte til at holde kontakt med familie og venner. Og det er det rigtig godt til. Men når man bruger nettet, er det vigtigt at tænke sig godt om, da risikoen for at den information man lægger på nettet, falder i de forkerte hænder. Informationer, der umiddelbart kan synes banale, som "I morgen tager vi på patrulje i Greenzone", eller vi kommer tilbage den 17." er i de forkerte hænder

vigtig information, der i værste fald kan bringe sikkerheden for patruljen i fare. Husk, at billeder kan sige mere end ord. Der er flere eksempler på, at udsendte i bedste mening har lagt billeder på nettet eller suppleret mails med billeder, der har

afsløret detaljer fra lejren. Billeder, der i de forkerte hænder kan bringe sikkerheden i fare. For at minimere denne risiko er det vigtigt, at man er bevidst om, hvad man skriver, og hvilke billeder man lægger på nettet.



Hvad står der i Berlingske Tidende? At de danske styrker i Irak ikke har jammere til at beskytte sig mod fjernudløste bomber. En nyttig oplysning for modstanderen?

Når teknikken tages til hjælp ...

SIGINT er enhver indhentning, der bygger på tekniske hjælpemidler. Det typiske er aflytning og evt. efterfølgende afkodning (dekryptering) af kommunikation via radio, telefon, internet osv.

SIGINT på højt niveau kræver kostbart teknisk udstyr og højtuddannede specialister til både indhentning og bearbejdning. Men også aflytning i mindre målestok kan være effektivt. Terrorister og kriminelle kan aflytte almindelig ukrypteret radiokommunikation og mobiltelefoni med relativt billigt udstyr, der kan købes af alle på internettet.

At tale dansk giver ingen beskyttelse, højst en kort forsinkelse til oversættelse. At bruge gamle skjuleord på frekvenser, der er gået i arv fra foregående hold, giver selv sagt ingen sikkerhed.



En soldat fortæller om operationer i Irak på sin hjemmeside. (Siden er ikke længere aktiv.)



SIGINT kan kræve store og kostbare installationer. Men en håndscanner til aflytning af mobiltelefoner koster ikke meget på nettet...

Midler til spionage?

Midler til spionage kan være meget enkle. Et stykke papir og en blyant til skitser, navne og lignende kan bringe en langt.

Vil man have mere avanceret udstyr, kan man gå på internettet og for overkommelige beløb få overvågningsudstyr, der er vanskeligt at erkende.

Men det udstyr, man især skal være på vagt overfor, er det, man ser hver eneste dag og derfor overser. Teknisk udstyr, der for få år siden ville have virket fantastisk i en James Bond-film, kan nu købes i enhver elektronikforretning for få hundrede kroner. Mobiltelefonen kan optage film og billeder. MP-3 afspilleren er også diktafon og kan indeholde store mængder data, hvis man i et ubevogtet øjeblik kan få adgang til en afvore computere.

Hvad kan du gøre?

Alle eksemplerne er reelle hændelser som danske eller allierede styrker har erkendt. Spionage udgør en direkte trussel mod dig, når du er på mission. Sikkerhed er både enhedens og dit ansvar. *Hvad kan du gøre for at støtte din enheds sikkerhed?*

- Tag risikoen for spionage alvorligt. Sæt dig i modstanderens sted. Hvad ville du som lokalansat eller udefrakommende kunne finde ud af om din enhed, jeres bevægelsesmønstre og forestående operationer? Hvad kan du gøre for at mindske modstanderens muligheder for at opnå viden om disse forhold?
- Gør dig ikke sårbar over for afpresning i forhold til f.eks. økonomiske vanskeligheder, utroskab, køb af ulovlige varer, misbrug af stoffer eller alkohol. Dette forhold er altid gældende, uanset hvor du arbejder eller gør tjeneste, og er således ikke kun forbundet med international tjeneste.
- Meld om overvågning eller mistanke om overvågning. Overvågning kan være et varsel om forestående angreb.
- Meld om kompromittering eller risiko for kompromittering. **Send kun klassificeret materiale via sikrede kommunikationsmidler.**
- Kontakt CI/sikkerhedsofficeren ved mistanke om overvågning, mistænkelig opførsel hos lokalansatte, kolleger, der har bragt sig selv i en sårbar position eller en hver anden risiko for at vi udsættes for spionage.

- Brug dine overordnede og CI/sikkerhedsofficeren. Det er banalt, men hellere 10 meldinger for meget end én for lidt.
- Tænk altid på din og din enheds sikkerhed, også når du kommunikerer med dem derhjemme. Velfærdstelefonen, e-mails, chat, mobiltelefon og SMS er alle relativt lette at aflytte.
- Hold din mund med operative forhold og tænk dig om. "Need to know" er en god grundregel. Det er menneskeligt at snakke, og der er ofte meget lidt nyt at tale om under en udsendelse. Men kilder, efterretninger, forstående operationer og så videre er "need to know".
- Tro ikke, at du er for ubetydelig til at udgøre et mål for spionage!

Kan spionage undgås?

Ikke helt - men ved omtanke og rettidig omhu kan vi øge vores sikkerhed ved at minimere modstanderens spionage mod os.



Kommercielt overvågningsudstyr til salg på internettet.

"Telefonen" er en mobilscanner.

"Stjerneskrue" er et tv-kamera.

Genstand til venstre er en mikrofon med tilhørende sender.

Genstanden i øverste venstre hjørne er en key-logger. Den husker de første 30.000 anslag, inklusive passwords.

Der er i alt for ca. 4.000 kr. udstyr.



Husk, mobiltelefoner med kameraer og memorystick-MP3 afspillere med indbygget diktafon er fremragende udstyr til spionage.

