

INFORMATIONSKRIGFÖRING eller LEDNINGSKRIGFÖRING?

Förutsättningarna för att hantera information har ökat lavinartat under detta århundrade. I dagens försvarsdebatt förekommer begreppen "informationskrigföring", "ledningskrigföring" och "informationsöverläge" rikligt. Orden bär på ett budskap men har också blivit modeord med en betydelse som inte alltid framstår som helt klar för varken författaren eller läsaren.

Om vi tittar tillbaka, ser vi att förekomsten av ett skriftspråk har varit en faktor av stor betydelse för samhällets administrativa och ekonomiska utveckling. Boktryckarkonsten i dess av Gutenberg utvecklade form var en av de vattendelare som valdes för att skilja Nya tiden från Medeltiden. Det är ett exempel på betydelsen av att kunna lagra och sprida information. Skrivmaskinens utveckling kom i hög grad att påverka samhällsutvecklingen under 1900-talet. Informationsteknologins (IT) utveckling, vilken möjliggjorts av teletekniken och särskilt av halvledartekniken, har gett oss förmåga att förutom att lagra och sprida även automatiskt registrera och bearbeta information på ett sätt som aldrig tidigare varit möjligt. Därmed har också möjligheten att använda informationen som ett instrument för maktutövning och om man så vill som ett vapen utvecklats.

Under 1980-talet dök uttrycket "ledningskrigföring" med den amerikanska förebilden "Command and Control Warfare" (C2W) upp i militär litteratur och uttrycket formligen exploderade i massmedierna i samband med Kuwaitkriget. "Informationskrigföring" (Information Warfare, IW) började också att användas. Liksom inom andra områden med dynamisk utveckling är utvecklingen av terminologin snabb; idag börjar uttrycket "Information Operations" att dominera.

Utnyttja "Fi:s" beroende

Vad betyder nu detta för Försvarsmak-

Text:

Överste Bentil Wennersholm,
HKU/Teleknigsektionen

ten och för flygvapnet? "FV 2000" bygger i hög grad på tillgång till information, på hantering och spridning av den. Därmed är vi också starkt beroende av information och vi måste skydda den. Samtidigt måste vi lära oss att utnyttja en motståndares beroende av sin information. Vi förutsätter att vi kommer att ha en kvalificerad motståndare den dag vi skulle behöva använda våra stridskrafter. En sådan motståndare kommer att uppvisa många parallella drag till vår egen förmåga att hantera information och beroendet av den.

Försvarsmakten startade vintern 1996-97 "Huvudstudie Ledningskrigföring" med uppgift att föreslå hur vår ledningskrigföring ska ledas, organiseras och utvecklas. Vilka insatser kan genomföras inom ramen för ledningskrigföringen? Vilken personal och utrustning, ny eller befintlig, krävs? Studien ska prioritera ledningskrigföring på ÖB- och MB-nivå och avrapporteras i slutet av 1998.

Vi har börjat med att studera syftet med ledningskrigföring och hur det kan kopplas till försvarsmaktens fyra uppgifter. Ledningskrigföring är i första hand riktad mot en motståndares ledning, dvs mot människan/beslutsfattaren i systemet – inte primärt mot de tekniska delarna av hans ledningssystem. Syftet med ledningskrigföring är att påverka motståndarens förmåga att formulera, uttrycka och utöva sin vilja.

För att nå målet att påverka motstån-

darens ledningsförmåga har vi brutit ned ledningskrigföringen i olika delar som ska samverka för att stödja det syftet. Dessa är *vilsledning*, *psykologisk krigföring*, *ledningsbekämpning* och *underrättelseskydd*. Inom ramen för dessa delar kan vi sedan utnyttja olika verktyg. Främst av dessa är våra förband med sina egenskaper och resurser. Exempel på komponenter är maskering, signaturanpassning, skenmål, telekrigföring, informationssystem samt fysisk bekämpning med konventionella vapen och sabotage.

Demokratin bromsar?

Att använda ledningskrigföring är i hög grad att tillägna sig ett nytt sätt att tänka – att spela med informationen som vapen för att påverka motståndarens omvärldsuppfattning på ett sätt som gynnar den egna sidan. Vilsledning och psykologisk krigföring är områden som är svåra att hantera i en demokratisk stat präglad av humanistiska ideal. Även om vi i princip har haft med dem i vår planering, har de i praktiken blivit ganska marginella företeelser. Vi har inte övat dem i någon större omfattning. Vi har exempelvis inte byggt upp några nämnvärda resurser för att rikta psykologisk krigföring mot en motståndares militära organisation. Här föreslår vi i studien en ändring.

Ledningsbekämpning avser åtgärder som syftar till att *förblinda motståndaren* i en viss riktning eller under viss tid, hindra hans förmedling av order eller slå ut systemkritiska funktioner som exempelvis telekommunikationer. Detta är mer välbekant men kräver samordning med övriga delar av ledningskrigföringen och andra delar i operationsplanen, för att vi ska göra en riktig prioritering av mål och få ut så stor verkan som möjligt.

Underrättelseskydd är ett svårt begrepp. Det motsvarar det amerikanska "Operations Security". Vi är inte nöjda med översättningen. (Kom gärna med bättre förslag!) Syftet är att motverka motståndarens insyn i vår gruppering och

våra intentioner. Vi måste därför fastställa vilken information om våra förband och vår verksamhet som det är avgörande att motståndaren inte känner till. Underrättelseskydd har framförallt stor betydelse för att vi ska kunna genomföra vilseledning på ett trovärdigt sätt.

Veta vad "Fi" vet

Vi behöver känna till motståndarens system för underrättelseinhämtning – exempelvis satellitspaning, flygburen radar och signalspaning samt få klart för oss hur en motståndare uppfattar vårt läge och vår verksamhet. Detta innebär att vi såväl måste kartlägga hans underrättelsesystem som följa upp de signaler som vi själva avger. Signalerna utgörs inte endast av aktiva sändare utan även av underrättelser som motståndaren kan erhålla genom olika typer av inhämtning. Vi måste uppmärksamma också annan verksamhet som kan röja operationen; ett exempel är förnödenhetsbeställningar. Vi behöver vidare ha en god uppfattning om motståndarens varseblivning av våra åtgärder; uppfattar han vår vilseledning som en verklig operation? Planering och tillämpning av underrättelseskydd måste vara en kontinuerlig process. En svårighet är att underrättelseskydd också är ett område med ett motsatsförhållande till många faktorer som styr livet i ett öppet demokratiskt samhälle.

Ledningskrigföring innebär flera krav på våra underrättelsefunktioner. För att kunna bedriva effektiv vilseledning och psykologisk krigföring måste vi ha ingående kunskap om motståndarens ledningsprocesser, doktriner, taktik och nyckelpersonal samt om svagheter i hans tekniska system.

Ledningskrigföring innebär ett nytt synsätt vid det operativa utnyttjandet av stridskrafterna. Planering av ledningskrigföring måste ske integrerad med övrig verksamhet. Ledningskrigföring ska därför beaktas redan under bedömandet och ingå i den operativa idén. Vi måste utbilda och öva chefer och stabsmedlemmar i vår operativa ledningsorganisation för att träna in ett nytt beteende. En breddutbildning inom Försvarsmakten krävs också för att få fullt genomslag.

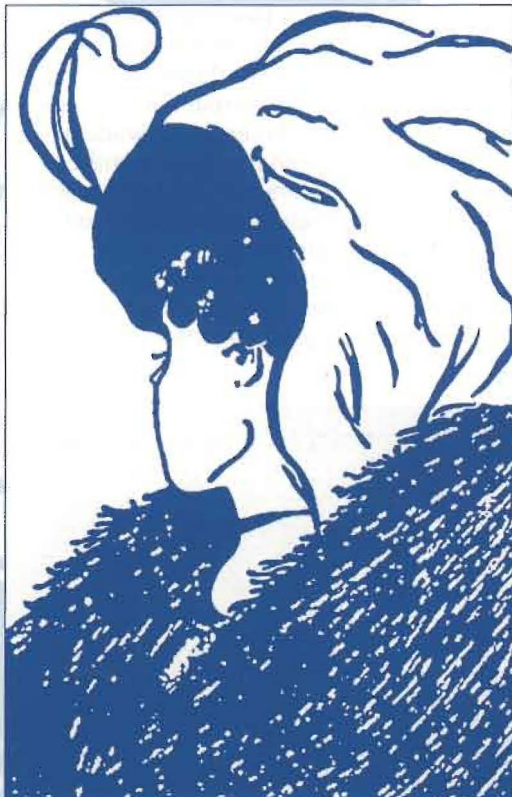
Studien kommer under 1998 att fördjupa sig inom ledningskrigföringens olika delområden. En fråga som kommer att behandlas är *begreppsapparaten*. Studien har i sitt arbete kommit fram till några rekommendationer som strider mot nu fastställda begrepp. Ett viktigt sådant avsteg är slutsatsen att ledningskrigföring bör avse den ena sidans

åtarder för att påverka motståndarens ledning. Skyddet av den egna ledningen mot motståndarens ledningskrigföring är däremot en fråga vid utformningen av det egna tekniska ledningssystemet, ledningsfilosofi och organisation.

Hur påverkas flyget?

Hur kan då ledningskrigföring påverka flygstridskrafterna? En roll för dessa som kommer att bibehållas och har stor betydelse är medverkan i ledningsbekämpning. Behovet av särskilda vapen eller modifiering av befintliga vapen för denna uppgift kommer att studeras. *Underrättelseskydd* och *vilseledning* kommer att vara viktiga faktorer för att understödja våra flygstridskrafter för att de ska kunna utnyttjas så effektivt som möjligt. Inte minst behöver vår basering och våra intentioner vad avser kraftsamling i tid, rum och funktion döljas för motståndaren.

Med en skickligt genomförd ledningskrigföring har vi goda förutsätt-



Vilseledning

I informationskriget kan man dölja det sanna och framhäva det falska.

ningar att uppnå överraskning och för oss gynnsamma styrkeförhållanden.

Ett uttryck som ofta missbrukas är informationsöverlägsenhet. Det har kommit in via det amerikanska begreppet "information superiority" och bör användas med eftertanke. USA har genom sin överlägsenhet såväl kvalitativt som kvantitativt möjlighet att skapa något som närmar sig innebörden av begreppet. Vi torde inte ha samma möjlig-

ter utom i speciella fall och i samverkan med andra nationer. Det är därför viktigt, att vi uttrycker oss så att vi får hanterbara och trovärdiga begrepp. Eftersom frågan rör kampen om omvärldsuppfattningen, bör vi snarare tala om att "*bestrida motståndaren insyn*" respektive att "*säkerställa egen omvärldsuppfattning*" inom ett operationsområde. Det förra kan vi uppnå genom åtgärder som störning, vilseledning och fysisk bekämpning i olika former; det senare genom att sprida och hårdgöra våra sensorer samt att integrera och utnyttja information från flera källor.

... kan vara kriminell ...

Till sist några kommentarer om ledningskrigföringens förhållande till informationskrigföring. Informationskrigföring berör alla sektorer i samhället och kan som aktörer ha enskilda personer, företag eller statliga organisationer. Den kan vara kriminell eller ha åtminstone visst stöd av lagregler. Den kan insättas i fred, i kris och i krig. Den kan ge upphov till kriser och leda till krigstillstånd. Inom begreppet ledningskrigföring har vi begränsat oss till militära åtgärder mot militära system. Det är viktigt att vi tillsammans med berörda civila myndigheter och organisationer gemensamt utnyttjar kompetensen inom landet för att öka samhällets motståndskraft mot informationskrigföring. Försvarsmakten har också deltagit i två studier som har initierats av regeringen.

Försvarshögskolan och Styrelsen för psykologiskt försvar har i uppdrag att studera aktiva åtgärder för att öka skyddet i samband med informationskrigföring (ASTA-studien). Efter avrapportering 1997 har studien fått i uppgift att 1998 lämna förslag om bland annat hur aktiv IT-kontroll av egna system ska genomföras.

Inom regeringskansliet har en arbetsgrupp tillsatts med uppdrag att följa utvecklingen av hot och risker inom området informationskrigföring (Ag IW). Gruppen ska sprida kunskap om detta samt lämna förslag till hur ansvar inom området ska preciseras och hur riktlinjerna för en strategi inom området bör se ut. Resultatet kan sammanfattas

med att ÖCB (Överstyrelsen för civil beredskap) föreslås få ett nytt nationellt sammanhållande ansvar för informationskrigföringsområdet med stöd av Försvarsmakten, varvid särskilt TSA (Totalförsvarets signalskyddssamordning) bör nämnas. Vidare föreslås inrättande av en *särskild statistikenhet* i syfte att kartlägga IT-incidenters omfattning och karaktär inom såväl privat som offentlig sektor. ■