FOI
TOTALFÖRSVARETS
FORSKNINGSINSTITUT

FOI-R—0294--SE
December 2001
ISSN 1650-1942
Användarrapport

Hans Furustig, Boris Ljunggren, Wilhelm Unge

Skydd mot strategisk vilseledning

Del 1: Definitioner, metoder, diskussioner

Försvarsanalys
172 90 Stockholm

TOTALFÖRSVARETS FORSKNINGSINSTITUT

Försvarsanalys
172 90 Stockholm

FOI-R--0294--SE

December 2001

ISSN 1650-1942

Användarrapport

Hans Furustig, Boris Ljunggren, Wilhelm Unge

Skydd mot strategisk vilseledning

Del 1: Definitioner, metoder, diskussioner

Utgivare	Rapportnummer, ISRN	Klassificering
Totalförsvarets Forskningsinstitut - FOI	FOI-R--0294--SE	Användarrapport
Försvarsanalys	**Forskningsområde**	
172 90 Stockholm	1. Försvars- och säkerhetspolitik	
	Månad, år	**Projektnummer**
	December 2001	I0025
	Verksamhetsgren	
	5. Uppdragsfinansierad verksamhet	
	Delområde	
	11 Försvarsforskning för regeringens behov	

Författare/redaktör	Projektledare
Hans Furustig	Wilhelm Unge
Boris Ljunggren	**Godkänd av**
Wilhelm Unge	Jan Foghelin, Avdelningschef
	Tekniskt och/eller vetenskapligt ansvarig

Rapportens titel

Skydd mot strategisk vilseledning – Del 1: Definitioner, metoder, diskussioner

Sammanfattning (högst 200 ord)

Inom totalförsvaret pågår sedan några år ett relativt omfattande arbete inom områdena informationskrigföring och informationsoperationer. Detta arbete syftar i olika kombinationer både till att skapa skydd mot hot, risker och sårbarheter samt att utveckla egen förmåga att bedriva informationskrigföring. Arbetet syftar bl.a. till att utarbeta en nationell policy för skydd mot informationskrigföring. Skyddet skall omfatta såväl aktiva som passiva åtgärder.

En genomgång av tidigare genomfört arbete uppvisar en kraftig slagsida mot IT-relaterade hot, risker och sårbarheter samt skyddsmöjligheter. Dessa hot, risker och skyddsmöjligheter ligger ofta i realtidsdomänen. Mer subtila och långsiktiga former av informationskrigföring som förutom genom spridning via datoriserade nätverk sprids via diplomater, ekonomiska förhandlingar, politiska utspel, militära och militärindustriella dispositioner m.m. och som på ett mer radikalt sätt syftar till att påverka hela vår verklighetsuppfattning över en längre tidsperiod behandlas inte explicit. Ett balanserat skydd, bör enligt rapportförfattarnas mening, innefatta informationskrigföringens samtliga element, dvs. även vilseledning och psykologisk krigföring.

Föreliggande studie syftar till att medvetandegöra Försvarsdepartementet och övriga totalförsvarsmyndigheter om att vilseledning och skydd däremot bör beaktas i en nationell policy för skydd mot informationskrigföring.

Nyckelord

vilseledning, skydd mot vilseledning, informationskrigföring, nationell policy, fallstudier, omvärldsbevakning, analytiska metoder

Övriga bibliografiska uppgifter	Språk Svenska
ISSN 1650-1942	**Antal sidor:** 137 s.
Distribution enligt missiv	**Pris: Enligt prislista**
	Sekretess

Issuing organization	Report number, ISRN	Report type
FOI – Swedish Defence Research Agency Defence Analysis SE-172 90 Stockholm	FOI-R—0294--SE	User report
	Research area code 1. Defence and Security Policy	
	Month year December 2001	**Project no.** I0025
	Customers code 5. Contracted Research	
	Sub area code 11 Defence Research for the Government	

Author/s (editor/s)	Project manager
Hans Furustig Boris Ljunggren Wilhelm Unge	Wilhelm Unge
	Approved by Jan Foghelin, Head of Division
	Scientifically and technically responsible

Report title (In translation)

Strategic counter-deception – Part 1: Definitions, methods, discussions

Abstract (not more than 200 words)

For several years a relatively extensive work on information warfare (IW) and information operations (IO) has been carried out by various organisations in the Swedish defence sector. The aim of this work is to develop and implement protective measures against threats, risks and vulnerabilities. A second aim has been to develop an offensive Swedish IW capability. An important part of the IW/IO work is the development of a national policy on IW defence. The IW defence should include both active and passive measures.

A review of the Swedish work carried out so far shows a clear bias towards IT-related threats, risks and vulnerabilities. These threats, risks and vulnerabilities are often of an operational and real-time nature. More subtle and long-term forms of IW aimed at distorting our perception of the surrounding world have not been treated in depth. These forms of IW/deception/disinformation are not only spread through computer networks both also by diplomats, economic negotiations, political action, military and military-industrial dispositions etc.

According to the authors of the report, a balanced IW defence should comprise all the elements, which the definition of IW includes. This means that counter-deception and protection against psychological warfare should be put higher up on the agenda than is the case today.

Keywords

Deception, counter-deception, information warfare, national policy, case studies, intelligence, analytical methods

Further bibliographic information	Language Swedish
ISSN 1650-1942	**Pages** 137 p.
	Price acc. to pricelist **Security classification**

FÖRORD

Föreliggande rapport har tillkommit tack vare FOA:s Innovationsråds ekonomiska stöd. 1999 beviljades ett innovationsprojekt rörande omvärldsbevakning och skydd mot strategisk vilseledning. Arbetet förutsattes kunna ske inom en ram av 2 personmånader eller med högst 200 000 kr som totalbelopp.

Motiven till projektet är flera. Det huvudsakliga skälet bakom författarnas initiativ till detta projekt är ett behov av att lyfta upp vilseledning som ett viktigt element i informationskrigföringen. Informationskrigföring handlar per definition inte enbart om IT-relaterade hot och risker ("hackerkriget"). För närvarande pågår vid totalförsvarsmyndigheterna ett arbete som syftar till att utarbeta en nationell policy för skydd mot informationskrigföring. Skyddet skall omfatta såväl aktiva som passiva åtgärder. I Försvarsberedningens rapporter inför de säkerhetspolitiska kontrollstationerna 1999 och 2001, i Underrättelsekommitténs rapport 1999, i *Sårbarhetsutredningen* 2001 samt i några viktiga utredningar från Försvarsmakten, Försvarshögskolan, Försvarets forskningsanstalt och Styrelsen för psykologiskt försvar kan man notera en viss slagsida mot just IT-aspekterna av informationskrigföring. Enligt rapportförfattarnas mening måste ett balanserat skydd beakta informationskrigföringens samtliga element, dvs. även vilseledning, psykologisk krigföring m.fl. element.

Projektledaren vill också rikta ett särskilt tack till Hans Furustig och Boris Ljunggren. Hans Furustig har stått för en mycket stor del av det skrivna underlaget i denna rapport i form av fallstudier m.m. Boris Ljunggren har, med sina kontakter och erfarenheter, på ett oumbärligt sätt bidragit till projektet. Dessutom har vi alla tre ägnat ett stort antal arbetstimmar utöver den givna ekonomiska ramen åt att föra detta projekt i hamn.

Sist men inte minst riktar författarna ett stort tack till Henrik Christiansson, FOI Institutionen för System- och funktionsvärdering, som på ett mycket förtjänstfullt sätt granskat rapporten och kommit med förslag till förbättringar. För eventuella kvarstående oklarheter och felaktigheter är författarna själva ansvariga.

I denna rapport nämns ett antal länder och organisationer i samband med redovisningar av historiska fall av vilseledning. Vissa länder/organisationer förekommer oftare än andra. Detta faktum skall dock inte tas till intäkt för att vi tror att dessa är mer benägna än andra att syssla med vilseledning i framtiden. Att de används som exempel beror helt enkelt på att de historiskt sett varit duktiga i vilseledningens konst i kombination med att de blivit föremål för omsorgsfull dokumentation.

Stockholm, december 2001
Wilhelm Unge
Projektledare

INNEHÅLLSFÖRTECKNING

Sammanfattning

Föreliggande studie syftar till att medvetandegöra Försvarsdepartementet och övriga totalförsvarsmyndigheter om att vilseledning och skydd däremot bör beaktas i en nationell policy för skydd mot informationskrigföring (IW). Dessutom definierar den vilseledning i ett informationskrigföringssammanhang och diskuterar relaterad terminologi. Vår förhoppning är också att vi, genom riklig exemplifiering, kan väcka intresse för vilseledning samt öka förståelsen för vilseledning och dess mekanismer. Sist men inte minst gör rapporten ett försök att strukturera tänkandet kring skydd mot vilseledning på nationell nivå (medel, metoder, organisatoriska frågor m.m.) samt ge underlag för fortsatt arbete.

Inom totalförsvaret pågår sedan några år ett relativt omfattande arbete inom områdena informationskrigföring/informationsoperationer och ledningskrigföring. Detta arbete syftar i olika kombinationer både till att skapa skydd mot hot, risker och sårbarheter samt att utveckla egen förmåga att bedriva informations- och ledningskrigföring. Ovan nämnda arbete syftar bl.a. till att utarbeta en nationell policy för skydd mot informationskrigföring. Skyddet skall omfatta såväl aktiva som passiva åtgärder.

Den bild som framträder vid en genomgång av ovan nämnda departementsskrivelser, offentliga utredningar, rapporter och studier uppvisar en slagsida mot IT-relaterade hot, risker och sårbarheter samt skyddsmöjligheter. Dessa hot, risker och skyddsmöjligheter ligger ofta i realtidsdomänen. Mer subtila och långsiktiga former av informationskrigföring som förutom genom spridning via datoriserade nätverk sprids via diplomater, ekonomiska förhandlingar, politiska utspel, PR-specialister och som på ett mer radikalt sätt syftar till att påverka hela vår verklighetsuppfattning över en längre tidsperiod behandlas inte explicit.

Enligt rapportförfattarnas mening bör ett balanserat skydd innefatta informationskrigföringens samtliga element, dvs. även vilseledning och psykologisk krigföring.

Med vilseledning avser vi i denna rapport medvetna åtgärder av politisk, militär, ekonomisk eller annan art som syftar till att ge en vilseledningsobjektet en felaktig verklighetsuppfattning och därmed ett felaktigt beslutsunderlag i syfte att få honom att agera på ett för deceptörens avsikter gynnsamt sätt. Med begreppet deceptör avses den som planerar och genomför vilseledning. Med vilseledningsobjekt menas den som är målet för vilseledningen. Med strategisk menas att vilseledningen skall beröra svenska intressen och tillgångar av nationell betydelse och att det huvudsakliga vilseledningsobjektet är stats- och militärledningen. Exempelvis skulle avsiktlig vilseledning kunna leda till att den svenska regeringen fattar beslut rörande krigsplanläggning på felaktiga grunder eller att Sverige intar en för landet i ett längre tidsperspektiv skadlig position i internationella förhandlingar. Ett annat exempel skulle kunna utgöras av vilseledning mot försvarsindustrin i syfte att skada den ekonomiskt eller t.o.m. att tvinga den in i ett icke självvalt internationellt samarbete för sin överlevnad (vilket måste särkiljas från övriga affärsbeslut vilka i dag förvisso går mot en internationalisering). Ytterligare ett exempel skulle kunna utgöras av underminerande av svenska statens trovärdighet (allmänt eller i någon speciell fråga).

Ur ett traditionellt underrättelseperspektiv betraktas vilseledning som en av tre komponenter i informationssäkerhetskomplexet. Den första komponenten består av passiva, defensiva åtgärder som syftar till att ta udden av främmande underrättelsetjänsters insamling. Den andra komponenten innebär aktiva försvarsåtgärder för att eliminera motståndarens offensiva underrättelsehot. Den tredje komponenten, vilseledning, syftar till att besegra främmande underrättelseinsamling genom att dölja, vilseleda eller förvirra.

Inom ramen för denna säkerhetsbringande verksamhet kan såväl aktiva som passiva åtgärder utnyttjas. Med aktiv vilseledning avses framhävande av falsk information, medan passiv vilseledning innebär döljande av sann information. I fredstid synes de flesta vilseledningsoperationer vara av intentions- eller förmågedöljande typ (även om undantag från denna generalisering finns). I kris och krig ökar som regel andelen framhävande vilseledning. Detta sammanhänger till del med det faktum att större värden står på spel under dessa tidsskeden och att därför kostnad-risk-kalkylen ser annorlunda ut för vilseledningsobjektet respektive deceptören.

Sett till effekten kan vilseledning delas in i två distinkta typer. Den första typen syftar till att öka osäkerheten genom att för mottagaren presentera flera trovärdiga alternativ. Effekten består i huvudsak i att mottagaren försenar eventuella beslut och åtgärder samt tvingas sprida sina resurser på ett ofördelaktigt sätt. Den andra typen av vilseledning syftar till att minska osäkerheten genom att få mottagaren att låsa på en falsk version av verkligheten. Detta kan göras genom att deceptören bibringar mottagaren bekräftande (men felaktig) information, vilket historiskt är den vanligast förekommande typen av vilseledning. Den mest avancerade och samtidigt mest svårgenomförbara formen är att försöka få mottagaren att tro på det som han a priori uppfattar som falskt. Historiska belägg finns för samtliga dessa typer och former av vilseledning.

Dagens informationssamhälle med ett ständigt ökande informationsinflöde som vida överstiger bearbetningskapaciteten tillsammans med ökade möjligheter att sprida desinformation och möjligheter att snabbt och globalt förändra värderingar underlättar snarare än försvårar deceptörernas arbete.

Föreliggande studie har fokuserat tidsskedena fred och kris. Att krisskedet har prioriterats motiveras av att det mesta som skrivits om vilseledning gäller krigsförhållanden eller åtgärder i nära anslutning till ett krigsutbrott. I en tid då den svenska försvarsförmågan bygger på anpassning synes det vara av intresse att kunna skilja vilseledning från verkligt hotfulla signaler. Att fredsskedet också bör studeras noga beror på att vilseledningen i slutänden inte behöver innebära ett militärt hot utan att den ytterst kan ha ett politiskt eller ekonomiskt mål. Den s.k. *ASTA-studien* föreslår att en nationell policy för skydd mot informationskrigföring utgår från svenska intressen och nationella tillgångar. Med en sådan bred definition omfattas alltså inte bara existensiella hot mot riket, utan även hot mot t.ex. svenska internationella insatser, Sveriges utrikespolitiska anseende och privata svenska företags (i synnerhet försvarsindustriföretags) ekonomiska intressen inom och utom landet.

Kopplat till det svenska försvarets anpassningsprincip finns problematiken med tidig förvarning, s.k. *early warning*, vilken i sin tur sammanhänger med skydd mot vilseledning. Området tidig förvarning handlar i första hand om utvecklandet av metoder för att kunna förutse oväntad och elakartad omvärldsutveckling som hotar det egna landet.

Även om begreppet är allomfattande och metoderna tillämpliga i olika sammanhang avses på nationell nivå oftast tidig förvarning om militära hot mot den egna staten eller dess intressen. Förvarningsmetoderna handlar om att hitta indikatorer som direkt eller indirekt vittnar om förestående hot, kapacitetsuppbyggnad e.dyl.

Vilseledning däremot, handlar om vad som ibland beskrivs som indikatorhantering. Med detta avses att en deceptör försöker kontrollera och samordna de indikatorer som har möjlighet att bidra till den bild deceptören avser att förmedla. Deceptören kan också skapa indikatorer för att understödja sin vilseledning. Relationen mellan förvarnings- och vilseledningsansträngningarna skulle alltså kunna beskrivas som en kamp mellan försök att identifiera och försök att dölja kritiska indikatorer. Problemet för deceptören består i att inte alla indikatorer som vittnar om en viss typ av verksamhet kan kontrolleras eller döljas. Förvarnarens problem är att han som regel har svårt att hantera svaga signaler.

Ag IW skriver att en grundsyn för arbetet med att ge nationen en tillräcklig förmåga att motstå informationskrigföring kan formuleras utifrån den generella säkerhetskedjan *skydda-upptäcka-reagera* (SUR-modellen). Denna modell synes även kunna användas för skydd mot strategisk vilseledning, även om skydd mot vilseledning som regel ses som en tvåstegsprocess: upptäcka och sedan motverka /reagera.[1] Förutom att detektera att man är utsatt för vilseledning är det av stor vikt att klargöra syftet med vilseledningen och att klargöra deceptörens identitet.

Trots att argument för motsatsen ibland hörs pekar vi i denna rapport på det faktum att det teoretiskt finns möjligheter att upptäcka vilseledning. Ett vanligt förekommande sätt är att betrakta vilseledning som en del av en samordnad plan i syfte att få vilseledningsobjektet att göra något som det annars inte skulle göra. Vår utgångspunkt är därför att ett skydd mot vilseledning på motsvarande sätt skall utgöra en **samordnad verksamhet** bestående **av olika metoder för att upptäcka vilseledning samt skyddande åtgärder och aktiviteter** som kompletterar och delvis överlappar varandra. Överlappningen är viktig eftersom den ger en möjlighet att kontrollera uppfattningar mot flera analyser/ källor.

I huvudsak omfattar våra förslag till skydd mot vilseledning

- inkorporerande av skydd mot vilseledning i en nationell policy för skydd mot informationskrigföring,
- olika analytiska förhållningssätt inkl. konkurrerande analys och analys av svaga (kritiska) signaler,
- löpande bevakning av misstänkta fall av vilseledning och
- kunskapshöjande och intresseväckande utbildning inom vilseledningsområdet.

Hur skyddet mot vilseledning skall arrangeras organisatoriskt är en komplicerad fråga. Mot bakgrund av projektets begränsade ramar har organisationsproblemet endast begrundats översiktligt utifrån den litteratur som studerats. En av de mest praktiska lösningarna synes vara att ansluta skyddet mot vilseledning till den organisationsstruktur

[1] I fallet vilseledning skulle man kunna formulera det som Skydd genom Upptäckt och Reaktion (SUR).

som *Ag IW* har föreslagit för ett nationellt skydd mot informationskrigföring.[2] Denna struktur baseras på redan befintliga organisationer, vilket motiveras av kostnadsskäl, och har karaktären av ett nätverk vilket även är den struktur som synes passa för skydd mot vilseledning. Det är dock angeläget att understryka vikten av att en fördjupad analys av ansvarsstrukturen för en eventuell skyddsorganisation görs.

I analogi med *Ag IW*:s förslag anser vi att ett **organ i Regeringskansliet** behövs. Detta organ bör ha flera uppgifter. För det första att formalisera en nationell policy för skydd mot vilseledning. För det andra att övervaka implementeringen av densamma. För det tredje att initiera utbildning rörande vilseledning hos de deltagande myndigheterna, organisationerna och företagen. För det fjärde bör detta organ ha en begränsad bearbetningsförmåga avseende vilseledningshot. Även om huvudansvaret för hotbearbetning m.m. föreslås vara huvuduppgift för ett nationellt funktionsansvar på central nivå (se nedan) har ett organ i Regeringskansliet delvis en annan utblick i säkerhetspolitiska frågor genom sin centrala placering. Och centralisering är av stor vikt såväl vid genomförande av vilseledning som vid skydd mot vilseledning. För det femte bör organet i Regeringskansliet ansvara för egna aktiva motåtgärder för det fall att vilseledning upptäcks. Detta organ skulle i fallet vilseledning företrädesvis kunna vara Regeringskansliets samordningssekretariat för säkerhetspolitiska underrättelsefrågor (Fö/SUND). Motivet till detta är givetvis den nära koppling som finns mellan underrättelseverksamhet och vilseledning. Dessutom bör organet ansvara för inriktning av insamlingsresurserna, en uppgift som redan i dag åligger SUND.

I likhet med *Ag IW:s* struktur bör också ett **nationellt funktionsansvar på central nivå** finnas. Det bör innehålla delar för hotbearbetning, skydd, incidentanalys samt övergripande samordning och inriktning. Denna funktion bör också ha det operativa ansvaret för eventuella aktiva motåtgärder. Det centrala nationella funktionsansvaret bör enligt vår mening ligga på HKV MUST. Motivet till detta är i första hand att MUST är rikets *all source*-underrättelsefunktion.

Även i fallet med skydd mot vilseledning synes ett behov föreligga av en väl fungerande **gränsyta mellan myndighetssfären och den privata sektorn**. Till skillnad mot de IW-relaterade hoten (och en eventuell statistikenhet för att få en uppfattning om omfattning och karaktär av IT-incidenter inom såväl privat som offentlig sektor) skulle detta organ utgöra rapporteringscentral dit misstänkta fall av vilseledning eller misstänkta trender skulle kunna rapporteras. Liksom i fallet med IW skulle Näringslivets säkerhetsdelegation (NSD) kunna utgöra gränsytan mellan myndighetssfären och den privata sektorn.

Möjligheterna till en **aktiv kontrollfunktion** har inte diskuterats i denna rapport. Ett behov av aktiv kontroll synes föreligga även i fallet vilseledning. Men, de praktiska svårigheterna vid genomförandet av sådan aktiv kontroll (där den kontrollerade parten

[2] Föreliggande rapport har till största delen skrivits före SOU 2001:41 Sårbarhet i en ny tid. Författarna är väl medvetna om att en del av Ag IW:s förslag är föråldrade eller kan komma att ges en något annorlunda utformning som ett resultat av Sårbarhetsutredningen; bl.a. kan nya organisationsenheter/ myndigheter komma att upprättas och nuvarande dito att upphöra/förändras. Det förtjänar därför att understrykas att diskussionen i denna rapport i första hand är principiell och rör funktioner och inte konkreta organisationsenheter, även om sådana nämns vid namn. Dessutom kan en del terminologi skilja sig från ordbruket i Sårbarhetsutredningen.

är omedveten om kontrollen) bedöms vara avsevärda eller t.o.m. oöverstigliga av olika skäl. Samtidigt finns det all anledning att i stället peka på möjligheterna att inom ramen för olika övningar vid såväl Regeringskansliet som totalförsvarsmyndigheterna belysa vilseledning och skydd däremot.

En **operativ mediebevakning** bör omfatta alla medier, inte enbart Internet, och ha i uppgift att kontinuerligt och över längre tid bevaka misstänkta fall av vilseledning. Det finns flera tänkbara organisatoriska hemvister för denna mediebevakning; MUST Sök,[3] FRA, SPF eller FOI. Oavsett var den operativa mediebevakningen placeras är det viktigt att denna enhet kan samverka med övriga delar av skyddsorganisationen eftersom mediesignalerna behöver jämföras med andra inkommande signaler. Svenska ambassader utomlands skulle kunna spela en viktig roll genom att bevaka misstänkta fall av vilseledning i respektive målland och regelbundet leverera underlag till det organ som har ansvaret för mediebevakningen. Möjligheten att utnyttja fristående konsulter för bevakning av enstaka frågor bör ej uteslutas.

En viktig del av skyddet mot vilseledning är olika metoder för kritisk (underrättelse-) analys. Med hjälp av alternativa analytiska förhållningssätt kan man skapa ett finmaskigare nät i omvärldsbevakningen genom att olika metoder med olika utgångspunkter, perspektiv och syften tillåts komplettera varandra. I skyddet mot vilseledning blir också sådana analysverktyg som tar hänsyn till människans kognitiva begränsningar viktiga.

Värdet av konkurrerande analys (*competitive analysis*) framhålls ofta som en analytisk metod för att komma till rätta med eventuell vilseledning (och även *early warning*-problemet). Syftet med den konkurrerande analysen är att möjliggöra perspektivbyte vid studiet av datamaterialet. En ensam analytiker/organisation har som regel svårt att göra av varandra helt oberoende analyser av datamaterialet ur olika perspektiv (vilket illustreras av bilden på rapportens omslag). En annan aspekt är att de första intrycken är svåra att ändra och att olika utgångspunkter kan leda till olika slutsatser varför konkurrerande analys kan gynna möjligheterna att upptäcka inkonsistenser i verklighetsuppfattning.

Av särskild vikt är att kontinuerligt bevaka förmodade fall av vilseledning och över lång tid ifrågasätta den information som ens bedömningar ligger till grund för. Särskilt viktigt i vilseledningsskyddssammanhang är att utvärdera tidigare bedömningar i ljuset av ny information som framkommer. En svårighet för en deceptör är bl.a. just att upprätthålla vilseledningen över en längre tid.

En viktig aspekt i analysarbetet är också att analysera egna sårbarheter i form av förutfattade meningar eller koncept som förekommer på såväl expert- som policynivå inom underrättelsesfären och det säkerhetspolitiska etablissemanget. Historien visar att en skicklig deceptör kan utnyttja just sådana låsta uppfattningar. Därför framhålls i analyssammanhang ofta vikten av någon form av institutionaliserat ifrågasättande (djävulens advokat etc.).

[3] Funktionen hette tidigare MUST OSI (Open Source Information/Intelligence). I skrivande stund ingår funktionen i HKV MUSTS:s lägesavdelning och den officiella beteckningen är MUST LÄGE Sök.

Andra näraliggande aspekter av skydd mot vilseledning är att försöka hålla sinnet öppet och att inte dra alltför snabba slutsatser och att försöka titta med deceptörens ögon, förstå hur han tänker och lista deceptörens möjliga handlingsalternativ. En sådan öppen attityd kan också gynnas av ett eget konspiratoriskt tänkande, dvs. skyddsforskning kräver kunskap om hotet.

En egen förmåga till vilseledning framförs ofta som ett sätt att motverka vilseledning. Deceptörens osäkerhet vid utvärderingen av sitt spel ökar om offret kan göra troligt att det självt kan kontra med vilseledning mot deceptören. Förutom att motverka redan pågående vilseledning framhålls att uppvisad förmåga till vilseledning kan ha en avskräckande effekt.

Counter-deception handlar också om att kunna kombinera detaljerad underrättelseanalys med annan, mer övergripande analys (politik, ekonomi, militaria) för att kunna upptäcka inkonsistenser och sätta in dem i ett större sammanhang som beskriver motståndarens mål och medel, förutfattade meningar, vanor m.m. (mikro- kontra makroanalys).

Slutligen beror förmågan till skydd mot vilseledning på kunskap om vilseledningens principer, mekanismer och effekter samt specifik kunskap om potentiella deceptörer. Därför bör utbildning av olika omfattning och djup bedrivas inom Regeringskansliet, på totalförsvarsmyndigheterna, andra eventuellt berörda organisationer samt företag.

Samtidigt finns ett antal svårigheter i samband med försök att skydda sig mot vilseledning. Ett sedan länge välkänt problem är att de flesta informationsbearbetningssystem/-organisationer arbetar med för liten marginal för att kunna klara plötsliga ökningar i informationsvolymen. Erfarenhet visar att svårigheter att klara volymökningar uppstår vid extraordinära händelser utan att vilseledning/desinformation förekommer. För att kunna använda sig av de i föreliggande rapport beskrivna metoderna krävs en marginal i analysresurserna.

Ett annat problem är att försök att göra underrättelseorganisationer känsligare för möjligheterna att vilseledning förekommer kan medföra att man ser vilseledning där det inte finns någon. Man riskerar att få en ökning i falsklarmsfrekvensen med ett vargen-kommer-syndrom som följd, vilket underminerar trovärdigheten hos framtida varning för vilseledning. Även *early warning*-funktionen står inför detta principiella problem.

Ett annat problem som sammanhänger med vilseledningens osäkerheter är att analytikerna p.g.a. att de inte vet vad de kan betrakta som sant eller falskt sätter upp så rigorösa beviskriterier att det undertrycker intuitionens spelrum (vilket är en viktig del i underrättelseanalysen) eller flödet av underrättelser till beslutsfattarna.

Som regel kräver beslutsfattare att en underrättelseorganisation skall kunna skilja på det som är sant och det som är falskt. Det räcker alltså inte för en underrättelseorganisation att ha vaga misstankar om att vilseledning föreligger. Hur beslutsfattarna uppfattar situationen beror sannolikt både av hur indicierna presenteras samt den större (politiska, militära eller ekonomiska) kontexten.

Sist men inte minst talar en större del av mekanismerna i den mänskliga perceptionsprocessen snarare till deceptörens fördel än till dennes nackdel. Ett utmärkande drag för

den mänskliga perceptionsprocessen är t.ex. motståndet mot att omformulera initiala bedömningar trots att enskilda efterkommande intryck uppvisar avvikande mönster. Ett annat stort problem är att människan för att undvika s.k. kognitiv dissonans tenderar att sortera bort avvikande information, medan hon har mycket lättare att ta till sig bekräftande information.

Dessutom förekommer som regel oupplösliga osäkerheter i alla typer av mer komplexa bedömningar utan att desinformation förekommer. Osäkerheten verkar oftast till deceptörens fördel. Förutsatt att den vilseledande informationen inte på goda grunder kan avfärdas helt måste den granskas av offret. Bördan av att reda ut de extra osäkerheter som vilseledningen medför faller därför på offret oavsett om vilseledning sedan accepteras som sanning eller lögn. Deceptören har också en fördel i det faktum vilseledningen nästan alltid medför kostnader för offret medan kostnaden för deceptören ofta är mycket ringa även om planen misslyckas.

Som framgår av det ovan sagda finns det en rad svårigheter av organisatorisk, kommunikativ och kognitiv art förbundna med de föreslagna skyddsmetoderna. Det torde emellertid genom goda kunskaper om dessa svårigheter vara möjligt att eliminera en del av dem samt göra det möjligt att kringgå andra.

Samtidigt bör det påpekas att vilseledning är ett riskfyllt företag som lätt kan omintetgöras av olika omständigheter. För det första måste vilseledningsobjektet nås av de vilseledande signalerna. För det andra måste objektet tolka signalerna på det sätt deceptören avser. För det tredje måsta objektet sedan också agera på ett sätt som verkligen är till fördel för deceptören. I synnerhet den psykologiska perceptionsprocessen och organisatoriska processer hos objektet (objektet utgörs t.ex. av en underrättelsetjänst) gör det svårt att förutse hur objektet kommer att reagera. Andra svårigheter för deceptören sammanhänger t.ex. med sekretess, tidssamordning och integration med andra aktiviteter.

Avslutningsvis kan vi konstatera att skydd mot vilseledning på samma sätt som underrättelseverksamhet lika mycket är en konst som en vetenskap; en konst som bygger på expertbedömningar baserade på omfattande erfarenhet och med ett stort mått av gott omdöme och lyhördhet.

1. Inledning

A growing number of countries utilize disinformation as a regular domestic and foreign policy tool.
Ladislav Bittman[4]

Statsmakternas inriktning mot ett anpassnings- eller ominriktningsförsvar kräver en ökad satsning på omvärldsbevakning och goda beslutsunderlag. Ett hot mot dessa förutsättningar är avsiktlig vilseledning.

Idag förekommer militär, ekonomisk, politisk, teknisk m.fl. former av vilseledning. Olika myndigheter svarar idag inom sitt ansvarsområde för att statsmakterna delges ett korrekt beslutsunderlag. Historien visar dock att aktörer som ägnar sig åt vilseledning kan utnyttja demokratiernas frihetsideal och maktdelning mellan lagstiftare, beslutande högsta statsledning och självständiga myndigheter. Vilseledningen kan avancera ganska långt innan den utsatta parten genomskådar vilseledningen, om han överhuvudtaget genomskådar den. Vilseledning av beslutsfattare kan kombineras med psykologiska operationer i syfte att skapa opinion som ofta ytterligare underblåses av massmedia ("drevet-går-mekanismen"). Denna typ av operationer är det ännu svårare att skydda sig emot, ty även om man genomskådar vilseledningen kan man inte alltid vända opinionen som i ytterlighetsfallet kan begränsa beslutsfattarnas frihetsgrader ("beslutsburar").

I analogi med den s.k. *ASTA-studien* och *Ag IW:s* arbete (se avsnitt 2.1) om skydd mot informationskrigföring synes ett behov föreligga av en övergripande policy för hur skydd mot vilseledning skall organiseras på nationell nivå.

Med omvärldsbevakning avses här såväl inhämtning av information som analys. Med nationell avser vi Sverige som stat och dess intressen i offentliga och privata sektorn.

Med vilseledning avser vi i denna rapport medvetna åtgärder av politisk, militär, ekonomisk eller annan art som syftar till att ge vilseledningsobjektet (motståndaren) en felaktig verklighetsuppfattning och därmed ett felaktigt beslutsunderlag i syfte att få honom att agera på ett för deceptörens avsikter gynnsamt sätt. Med begreppet deceptör avses den som planerar och genomför vilseledning. Med vilseledningsobjekt menas den som är målet för vilseledningen. Med strategisk menas att vilseledningen skall beröra svenska intressen och tillgångar av nationell betydelse och att det huvudsakliga vilseledningsobjektet är stats- och militärledningen. Exempelvis skulle avsiktlig vilseledning kunna leda till att den svenska regeringen fattar beslut rörande krigsplanläggning på felaktiga grunder eller att Sverige intar en för landet i ett längre tidsperspektiv skadlig position i internationella förhandlingar. Ett annat exempel skulle kunna utgöras av vilseledning mot försvarsindustrin i syfte att skada den ekonomiskt eller t.o.m. att tvinga den in i ett icke självvalt internationellt samarbete för sin överlevnad (vilket måste särkiljas från övriga affärsbeslut vilka i dag förvisso går mot en internationalisering). Ytterligare ett exempel skulle kunna utgöras av underminerande av svenska statens trovärdighet (allmänt eller i någon speciell fråga).

[4] Ladislav Bittman, *The New Image-Makers: Soviet Propaganda & Disinformation Today*, Pergamon-Brassey's, 1988, s. 3.

1.1 Projektets syfte

I FOA:s Innovationsråds bifall till vår ansökan specificerades att projektgruppens arbete skulle inriktas mot

- förslag till terminologi inkl. definition av vilseledning i ett informationskrigförings-sammanhang och diskussion av relaterad terminologi och
- strukturering av tänkandet kring skydd mot vilseledning på nationell nivå (medel, metoder, organisatoriska frågor m.m.).[5]

Föreliggande studie skulle då ha kunnat ses som en förstudie. Under arbetets gång har vi emellertid själva valt att utvidga arbetsuppgifterna utöver det Innovationsrådet ursprungligen avsåg finansiera. Studien borde, tyckte vi, även

- belysa hur vilseledning hittills har behandlats inom den svenska utrednings- och studieverksamheten,
- medvetandegöra Försvarsdepartementet och totalförsvarets myndigheter om att vilseledning och skydd däremot bör beaktas i en nationell policy för skydd mot informationskrigföring,
- väcka intresse för vilseledning,
- genom riklig exemplifiering öka förståelsen för vilseledning och dess mekanismer samt
- ge underlag för fortsatt arbete.

Motivet bakom denna utvidgning var att vi, mot bakgrund av det faktum att ingen huvudstudie var planerad efter denna förstudie, önskade skapa ett så fylligt underlag som möjligt för en något så när kvalificerad diskussion inom totalförsvaret kring vilseledning och skydd däremot. Vår ambitionsnivå och projektets begränsade resurser har därför inte stått riktigt i paritet med varandra. Läsaren bör ha detta i åtanke.

1.2 Tillvägagångssätt

För att inte komma i konflikt med statliga organ som eventuellt redan sysslar med skydd mot vilseledning eller närbesläktad verksamhet har föreliggande projekt haft karaktären av oberoende studier. Avsikten var att projektet skulle konstituera en första analysgrupp med uppgift att påbörja metodutveckling inom området nationellt skydd mot (strategisk) vilseledning.

Projekt har till största delen arbetat "in-house" på FOA/FOI. Under projektets gång har dock samtal förts med representanter för Försvarsdepartementet, SÄPO, MUST och försvarsindustrin.

[5] Försvarets forskningsanstalt, Innovationsrådet, protokoll 1999-03-30.

Arbetet har bedrivits i form av ett stort antal arbetsmöten. Mellan mötena har projektdeltagarna läst och skrivit, vartefter strukturen och analysen har växt fram. Studien är i huvudsak en litteraturstudie. En mycket stor mängd litteratur och ett stort antal historiska fall av vilseledning har studerats.

1.3 Underlag och källor

I huvudsak har öppet material från skriftliga källor använts under studiens gång. I enstaka fall har muntliga källor utnyttjats. Vid en eventuell fortsättning av arbetet synes det vara av stor vikt att även utnyttja hemligt material. I synnerhet rör detta utvärdering i samband med fallstudier.

Endast svensk- och engelskspråkigt material har utnyttjats. Underlaget behandlar i första hand svenska, anglosaxiska och sovjetiska förhållanden.

1.4 Rapportens disposition och läsanvisningar

Av användarvänlighetsskäl har rapporten delats upp i två delar. Den första delen omfattar bakgrunden och motivet till varför skydd mot vilseledning bör studeras (kapitel 2). Kapitel 3 omfattar förutom definitioner en allmän beskrivning av hur vilseledning går till i praktiken medan kapitel 5 utgör en teoretisk fördjupning i vilseledningens metoder och mekanismer. Exemplen i kapitel 4 avser att tydliggöra vad som avses med strategisk vilseledning och har av detta skäl placerats efter kapitel 3 men före kapitel 5. En läsare som inte vill fördjupa sig i exemplen eller de teoretiska delarna kan därför med behållning hoppa över kapitel 4 och 5 och gå direkt till kapitel 6 Skydd mot strategisk vilseledning.

I rapportens andra del återfinns en stor mängd fall av vilseledning beskrivna inkl. ett antal fördjupade fallstudier. Dessutom innehåller den andra delen ett stort antal referenser rörande vilseledning som kommenterats för att orientera en intresserad läsare.

I första hand är rapporten avsedd som användarrapport för Försvarsdepartementet (speciellt Regeringskansliets samordningssekretariatet för säkerhetspolitiska underrättelsefrågor (Fö/SUND)), Militära underrättelse- och säkerhetstjänsten (MUST) och Försvarets underrättelsenämnd (FUN). Samtidigt är avsikten att rapporten skall kunna tjäna som en antologi, uppslagsbok eller lärobok avseende vilseledning och skydd mot vilseledning för alla intresserade inom totalförsvaret.

Med hänsyn till att rapporten skall kunna användas som en antologi har vi valt att utforma varje kapitel och bilaga så att den kan läsas fristående utan att läsaren skall behöva söka upp andra ställen i texten. Nackdelen med en sådan presentation är dock att en del upprepningar kan förekomma. Vår förhoppning är dock att fördelarna med den valda dispositionen överväger med hänsyn till rapportens stora omfång.

1.5 Allt är inte vilseledning!

Vilseledning är ett svårstuderat område eftersom det bl.a. finns ett gränsland i vilket egna beslutsfattares, mediers och andra aktörers uppträdande kan skapa effekter liknande dem som är ett resultat av en extern deceptörs vilseledning. Sådan grogrund kan alltid uppstå oavsett om det finns någon bakomliggande extern och avsiktlig vilseledning. Ett sentida svenskt exempel skulle kunna vara debatten kring ubåtskränkningarna under 1980- och 90-talen. Försvarssekretessen i kombination med ryktesspridning, aktörer med särintressen m.fl. ingredienser ingår och skapar en utmärkt grogrund för konspirationsteorier.

Författarna är väl medvetna om denna problematik. Vi har av praktiska skäl valt att avgränsa bort densamma. Föreliggande rapport behandlar således skydd mot verklig och avsiktlig vilseledning iscensatt av en extern aktör. En professionell deceptör kan dock ha hjälp av svenska s.k. inflytelseagenter och oskyldiga offer. Medan den första kategorin är medveten om sin roll fungerar den andra ovetandes som medium för deceptören. Detta problem finns såväl vid utvärderingen av historiska händelser, där ett kvarliggande sediment alltid kan röras upp och skapa grogrund för osaklig debatt (t.ex. främmande ubåtar), som vid utvärderingen av ett pågående skede (t.ex. Echelon-debatten).

2. Motivet till föreliggande studie

Our experience in the invasion of Czechoslovakia has reinforced the opinion long held by warning analysts that the US, at both its intelligence and policy levels, is extremely vulnerable to deception.

Cynthia M. Grabo, CIA 1970[6]

I detta kapitel motiveras varför det synes föreligga ett behov av studier rörande vilseledning och i synnerhet studier rörande skydd mot vilseledning. Efter en genomgång av andra studier inom informationskrigföringsområdet redovisas en översikt av vad de säkerhetspolitiska kontrollstationsrapporterna 1999 och 2001, *Underrättelseutredning* 2000 samt *Sårbarhetsutredningen* 2001 säger om vilseledning och desinformation.

2.1 Studier rörande informationskrigföring

Försvarsmakten (FM), Försvarshögskolan (FHS), Försvarets forskningsanstalt (FOA, numera Totalförsvarets forskningsinstitut (FOI)) och Styrelsen för psykologiskt försvar (SPF) bedriver sedan några år ett relativt omfattande arbete inom områdena informationskrigföring och ledningskrigföring. Detta arbete syftar i olika kombinationer både till att studera egna svagheter och skapa skydd samt att utveckla egen förmåga att bedriva informations- och ledningskrigföring.

I samband med föreliggande studie gjordes sökningar hos registraturerna vid Försvarsmakten,[7] Försvarshögskolan, Försvarets forskningsanstalt och Styrelsen för psykologiskt försvar. Sökorden utgjordes av de centrala begreppen inom informations- och ledningskrigföringen så som de vid söktidpunkten definierades av Försvarsmakten. Därutöver har några associerade termer använts vid sökningarna.[8] När det gäller FM, FHS och FOA avsöktes perioden 1990-2000.[9] Sökperioden för SPF var betydligt längre.[10] Sökresultaten finns samlade i en pärm vid Totalförsvarets forskningsinstituts (FOI) registratur.[11]

I tabell 1 illustreras fördelningen av antalet träffar inom respektive delområde inom ledningskrigföringsområdet. Sökningen avser endast träffar i dokumentens ärendemening,

---

[6] CIA Center for the Study of Intelligence, Studies in Intelligence (kursmateial hösten 2000), Cynthia M. Grabo, *Soviet Decption in the Czechoslovak Crisis*, Internet, http://www.odci.gov/csi/studies/fall00/ch5_Soviet_Deception.pdf, hämtat 9 augusti 2001, s. 86.

[7] Sedan 1990 har Försvarsmaktens högkvarter genomgått ett antal organisationsförändringar. Sökningar har därför genomförts vid myndigheterna ÖB, CA, CFV, CM, FMO, HKV och HKV NY.

[8] Sökorden var: vilseledning, underrättelseskydd, telekrig, psykologisk krigföring, fysisk bekämpning, övrig signalkrigföring, maskirovka, överraskning, vilseledande operationer, desinformation, skydd mot vilseledning, motverkan mot vilseledning, motåtgärder mot vilseledning, psykologiska operationer, informationskrig(föring), informationsoperationer, ledningsbekämpning, lednings-krigföring och skydd mot informationsinhämtning.

[9] Sökningen sträckte sig till februari 2000.

[10] Sökningen resulterade i förteckningar över Beredskapsnämndens/Styrelsen för psykologiskt försvars Meddelanden utgivna fr.om. 1964 och Rapporter utgivna fr.o.m. 1957.

[11] Totalförsvarets forskningsinstitut, Dnr 01-4011.

inte dokumentens innehåll. Tabellen visar endast sökningarna genomförda vid Högkvarteret. Antalet träffar omfattar alla dokument och handlingar rörande respektive delområde, dvs. även kallelser till arbetsmöten avseende studien NN, remisshemställanden osv. Tabell 1 kan därför sägas visa verksamhetsintensiteten kring ett visst delområde snarare än antalet färdiga rapporter eller motsvarande.

Som framgår av tabell 1 har delområdet telekrig kraftigt dominerat verksamheten. Verksamheten avseende vilseledning har varit relativ ringa. Bland träffarna avseende vilseledning finns också ett antal som behandlar vilseledning av tekniska sensorer och verkanssystem o.dyl. I föreliggande studie omfattar termen vilseledning inte denna typ av verksamhet (vilken snarare är att hänföra till området Varnar- och motmedelssystem, VMS).

Tabell 1. ***Antal träffar vid sökning vid Försvarsmaktens högkvarter.***[12]

Sökord	ÖB	CA	CFV	CM	FMO	HKV	HKV NY	*Totalt antal träffar*
Vilseledning	3	23	1		1	58[13]	6	**92**
Underrättelseskydd								
Telekrig	205	107	145	152	55	355	153	**1172**
Psykologisk krigföring						1		**1**
Fysisk bekämpning								
Övrig signalkrigföring								
Maskirovka								
Överraskning								
Vilseledande operationer								
Desinformation								
Skydd mot vilseledning								
Motverkan mot vilseledning								
Motåtgärder mot vilseledning						1[14]		**1**
Psykologiska operationer	1					3		**4**
Informationskrig						10	15	**25**
Informationskrigföring						6	11	**17**
Informationsoperationer								
Ledningsbekämpning								
Ledningskrigföring							13	**13**
Skydd mot informationsinhämtning								

Kommentar 1: Resultatet av ser endast sökning i ärendemeningen.
Kommentar 2: Tom ruta innebär noll träffar.

Vid en genomgång av sökresultaten från FHS och FOA:s registraturer framgår att telekrigsområdet på liknande sätt dominerar inom FHS och FOA:s studie- och forsknings-

[12] Antalet anger summan av hemliga och öppna dokument vid respektive myndighet.
[13] 44 träffar hänför sig till arméns vilseledningsstudie (AL-studie 6: Vilseledning) som genomfördes under denna tidsperiod. 5 träffar rör flygvapnets vilseledningsstudie (VILMA FV) och 2 träffar FOA-rapporten *Marin vilseledning* av Hans Furustig. Därutöver förekommer vilseledning av tekniska system, t.ex. vilseledning av laseravståndsmätare. Föreliggande studie behandlar inte denna typ av vilseledning.
[14] Det enda exemplet på motåtgärder mot vilseledning hänför sig till FOA-rapporten *Motåtgärder och vilseledning avseende laservarnare*.

verksamhet. I SPF:s verksamhet dominerar naturligen psykologisk krigföring, opinionspåverkan och propaganda. Mycket få träffar avseende desinformation och vilseledning i den mening som avses i föreliggande studie förekommer. Dessutom sysslar SPF endast med skyddsaspekten.

Vilseledning av olika former pågår i fred, kris och krig i vår omvärld. En omfattande svensk och internationell litteratur rörande vilseledning finns. Däremot finns mycket lite arbete gjort inom området skydd mot vilseledning. Detta gäller, såvitt författarna är bekant, såväl öppet som hemligt material.

När det gäller studier av informationskrigföring och skydd däremot på nationell nivå skall tre studier nämnas här. Den första är *ASTA-studien – Ett regeringsuppdrag om aktiva åtgärder rörande Informationskrigföring.*[15] Den andra är arbetsgruppen för informationskrigförings (*Ag IW*) rapport.[16] Den tredje är Försvarsmaktens *Huvudstudie Ledningskrigföring.*[17]

ASTA-studien genomfördes gemensamt av FHS och SPF. Studien var ett regeringsuppdrag för studera aktiva åtgärder för att öka skyddet i samband med informationskrigföring. *ASTA-studien* fick en fortsättning där fyra deluppdrag redovisades 1998.[18]

I regleringsbrevet 1997 till FHS, SPF och andra berörda totalförsvarsmyndigheter beskrevs *ASTA-studiens* uppdrag på följande sätt:

> I prop 1996/97:4 (s. 175) framhålls att Sverige måste dels studera och successivt vidtaga åtgärder för att motstå informationskrigföring, dels som en del i möjligheterna att öka kunskaperna om skydd mot informationskrigföring och på sikt utarbeta en nationell policy. Försvarshögskolan och Styrelsen för psykologiskt försvar skall tillsammans och i samråd med Försmakten och Försvarets forskningsanstalt studera möjligheterna till aktiva åtgärder inom informationskrigföring. Studierna bör omfatta
>
> - Utvecklingen i andra länder beträffande debatt, forskning, utbildning/ övning och tillämpning
> - Aktiva åtgärder som Sverige rent tekniskt skulle kunna utveckla och implementera
> - Aktiva åtgärder som Sverige bör begränsa sig till.
>
> Stor öppenhet bör visas vad gäller möjligheter till aktiva åtgärder samtidigt som eventuella folkrättsliga aspekter eller andra inskränkningar av möjligheter till aktiva åtgärder bör anges. Försvarsmakten, Försvarets radioanstalt, Försvarets materielverk och Försvarets forskningsanstalt skall lämna erforderligt underlag och stöd vid studierna. Uppdraget redovisas senast den 30 augusti 1997.

[15] Försvarshögskolan, *ASTA-studien—Ett regeringsuppdrag om aktiva åtgärder rörande Informationskrigföring*, H01710:6014, 1997-06-30.
[16] *Ag IW*, Rapport nummer 2 om åtgärder och skydd mot informationskrigföring från arbetsgruppen för informationskrigföring, 1998-09-01, dnr FO 98 1828/MIL.
[17] Försvarsmakten, *Huvudstudie Ledningskrigföring—Slutrapport*, 21 120:60831, 1999-01-27.
[18] (ASTA 2), FHS/SPF, *ASTA-studien*, 23385:60763.

Den andra studien härrör från *Ag IW*. Regeringen beslöt 1996 att inom Regeringskansliet tillsätta en arbetsgrupp med uppdrag att följa utvecklingen av hot och risker inom området informationskrigföring, sprida kunskap om detta samt att lämna förslag till hur ansvar inom området skall preciseras och hur riktlinjerna för en strategi inom området bör se ut. I arbetsgruppen, *Ag IW*, ingick representanter för Försvarsdepartementet, Kommunikationsdepartementet, Rikspolisstyrelsen, Säkerhetspolisen, Försvarsmakten, Försvarshögskolan, Styrelsen för psykologiskt försvar och Försvarets forskningsanstalt. *Ag IW* lämnade sin första rapport 1997-08-15 till Regeringskansliet. En andra rapport inlämnades 1998-05-29.

Såväl *ASTA-studien* som *Ag IW:s* arbete har till stor del fokuserat på den del av informationskrigföringen som kan relateras till informationsteknologin (datoriserade system) med dess risker och möjligheter. De föreslagna skyddsåtgärderna syftar till att kunna hantera kriser och informationsattacker (ofta i realtid) och har en mycket konkret operativ karaktär.

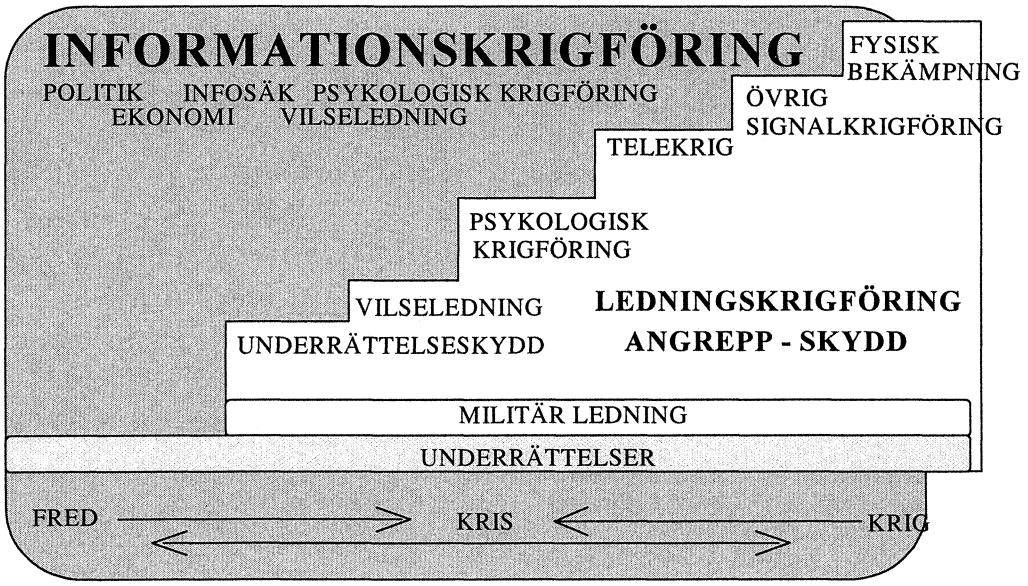

Fig. 1. Sammanhanget mellan informationskrigföringens olika element. Observera dock att terminologin är under förändring och att denna bild inte längre gäller som definition.

I anslutning till *Ag IW*:s arbete kan det vara värt att påpeka att denna arbetsgrupps förslag till del är föråldrade eller kan komma att ges en något annorlunda utformning med hänsyn till senare utredningar, i första hand SOU 2001:41 *Sårbarhet i en ny tid.* Eftersom vår rapport till största delen skrivits före *Sårbarhetsutredningen* kan en del terminologi i vår rapport skilja sig från ordbruket i den senare. Dessutom kan nya organisationsenheter/myndigheter komma att uppstå och nuvarande organisationer/myndigheter att upphöra/förändras.

Den tredje studien, Försvarsmaktens *Huvudstudie Ledningskrigföring*, behandlar Försvarsmaktens egen förmåga till ledningkrigföring, inkl. vilseledning. Studiens slutrapport innehåller viktiga resonemang och definitioner (se vidare avsnitt 3.2.1).

Försvarsmaktens tidigare definition på informationskrigföring framgår av figur 1. Enligt denna terminologi var informationskrigföring det överordnade begreppet. Ledningskrigföring utgjorde den militära delen därav och omfattade skedena kris och krig. Vilseledning kunde förekomma såväl i fred som kris och krig.[19] Även om Försvarsmaktens terminologi för närvarande är stadd i förändring och definitionen enligt figur 1 inte längre är aktuell fyller den här en funktion för att beskriva att vilseledningen är ett fredstida såväl som kris- och krigstida fenomen.

Ett motiv till föreliggande studie utgörs av den snedfördelning med slagsida mot informationsteknologirelaterad informationskrigföring som ovan nämnda studier uppvisar. Snedfördelningen inom hela studieområdet framgick också med all tydlighet av tabell 1. Som framgår av figur 1 är vilseledning ett element i informationskrigföringen. Vilseledning är mer subtil till sin karaktär. Den är ofta också mer långsiktig. Den använder sig också av många inkanaler, inte enbart datoriserade. Vilseledningens subtilitet, långsiktighet och flyktighet gör det om möjligt ännu svårare att skydda sig mot denna form av påverkan än mot "hackerkrig". Icke desto mindre är det författarnas åsikt att man i en nationell policy för skydd mot informationskrigföring måste beakta detta informationskrigsföringselement.

2.2 Vilka är målen för strategisk vilseledning?

Av huvudsakligt intresse för projektets arbete har varit tidsskedena fred och kris. Att krisskedet har prioriterats motiveras av att det mesta som skrivits om vilseledning gäller krigsförhållanden eller åtgärder i nära anslutning till ett krigsutbrott. I en tid då försvarsförmågan bygger på anpassning synes det vara av intresse att kunna skilja vilseledning från verkligt hotfulla signaler. Det är emellertid också klart att vilseledning som avslöjas är en signal i sig. Detta sammanhänger med den s.k. early-warning-problematiken. Att fredsskedet också bör studeras noga beror på att vilseledningen i slutänden inte behöver innebära ett militärt hot utan att den ytterst kan ha ett politiskt eller ekonomiskt mål. Nuvarande samhällsutveckling och trender gör att nationella intressen blir av större vikt samtidigt som vikten av den territoriella integriteten kvarstår som tidigare.

ASTA-studien föreslår att en nationell policy för skydd mot informationskrigföring utgår från **svenska intressen** och **nationella tillgångar**.[20] Även föreliggande studie har detta som utgångspunkt. Med en sådan bred "definition" omfattas alltså inte bara existensiella hot mot riket, utan även hot mot t.ex. svenska internationella insatser, Sveriges utrikespolitiska anseende, statens trovärdighet i medborgarnas ögon och privata svenska företags (speciellt försvarsindustriföretag) ekonomiska intressen inom och utom landet.

[19] *Ledningskrigföring, definition av ny struktur och begrepp*, HKV 21 120:79934, 1995-09-22
[20] Försvarshögskolan, *ASTA-studien—Ett regeringsuppdrag om aktiva åtgärder rörande Informationskrigföring*, s. 2.

2.3 De säkerhetspolitiska kontrollstationerna – systemfel eller korrekta bedömningar

Sveriges nuvarande säkerhetspolitiska situation och omvärldsläge har beskrivits i ett antal skrifter. Se t.ex. Försvarsberedningens rapporter inför den säkerhetspolitiska kontrollstationen 1999 *Förändrad omvärld – omdanat försvar*[21] och kontrollstationen 2001 *Gränsöverskridande sårbarhet – Gemensam säkerhet*,[22] underrättelsekommitténs betänkande 1999 *Underrättelsetjänsten – en översyn*[23] samt *Sårbarhetsutredningen* 2001.[24] Innehållet i dessa skrifter torde vara bekant för en initierad läsare varför vi här nöjer oss med att konstatera att inga existentiella hot mot Sverige synes finnas idag eller under det närmaste decenniet, dvs. det militära läget är gott även om vissa osäkerheter kvarstår. När det gäller andra säkerhetspolitiska delområden som t.ex. ekonomi och information karaktäriseras dock situationen av en hårdnande internationell konkurrens parallellt med förtroendeskapande byggen av typen EU.

I analogi med genomgången i avsnitt 2.1 kan det vara av intresse att redovisa ovan nämnda dokuments syn på vilseledning och relaterade informationskrigföringselement. En genomsökning av dokumenten visar följande förekomst av termerna vilseledning m.fl.:

Tabell 2. ***Förekomsten av vilseledningsrelaterade termer i respektive dokument.***

Term/antal träffar	Försvars-beredningen 1999	Underrättelse-kommittén 1999	Försvars-beredningen 2001	Sårbarhets-utredningen 2001
Vilseledning	0	0	0	0
Vilseledande	0	3	0	0
Desinformation	1	5	0	1
Överraskning	1	0	0	2
Manipulera	1	1	0	1
Ledningskrigföring	0	2	0	0
Informationskrigföring	16	14	13	12
Informationsoperationer	0	0	34	42

På samma sätt som telekrig har dominerat studierna rörande (militär) ledningskrigföring vilket framgår av tabell 1, dominerar informationskrigföring (IW) och infomationsoperationer (IO) i tabell 2. En textundersökning av förekomsterna av dessa begrepp visar att IW/IO tenderar att likställas med den IT-relaterade delen ("hackerkriget") av informationskrigföringen. Mellan 1999 och 2001 kan noteras en förskjutning av terminologin från informationskrigföring (IW) till informationsoperationer (IO). Detta kommenteras också explicit i Försvarsberedningens rapport 2001.[25]

---

[21] Försvarsberedningen, *Förändrad omvärld—omdanat fösvar*, Regeringskansliet, Ds 1999:2, Internet, http://forsvar.regeringen.se/propositionermm/ds/pdf/ds99_2sve.pdf, hämtad 27 februari 2001.
[22] Försvarsberedningen, *Gränsöverskridande sårbarhet—Gemensam säkerhet*, Regeringskansliet, Ds 2001:14, Internet, http://forsvar.regeringen.se/propositionermm/ds/pdf/ds2001_14.pdf, hämtad 9 mars 2001.
[23] Statens offentliga utredningar, *Underrättelsetjänsten—en översyn*, SOU 1999:37, Internet, http://forsvar.regeringen.se/propositionermm/sou/pdf/sou99_37.pdf, hämtad 27 februari 2001.
[24] Statens offentliga utredningar, *Säkerhet i en ny tid*, SOU 2001:41, Internet, http://forsvar.regeringen.se/propositionermm/sou/pdf/sou2001_41a.pdf, hämtad 29 juni 2001.
[25] Försvarsberedningen, *Gränsöverskridande sårbarhet—Gemensam säkerhet*, s. 117.

Gemensamt för tabell 1 och 2 är alltså att ett element (telekrig resp. IW/IO) kraftigt dominerar studie- och utredningsverksamheten trots att definitionerna av lednings- och informationskrigföring omfattar flera element varav vilseledning är ett.

Intressant nog förekommer ordet *vilseledning* inte en enda gång i något av dokumenten. Inte heller ordet *vilseledande* förekommer en enda gång i Försvarsberedningens rapporter eller *Sårbarhetsutredningen.*

Endast Underrättelseutredningen behandlar *vilseledande* och *desinformation* lite mer utförligt. Där påpekas att information inhämtad från såväl mänskliga som tekniska källor kan vara vilseledande och innehålla desinformation.[27] Diskussionerna kring dessa begrepp förs i stort sett i samma anda som i föreliggande rapport, även om utredningens tidsperspektiv tenderar att vara något mer realtidsnära/operativt.

Samtidigt kan det tyckas märkligt att ordet *överraskning* inte förekommer en enda gång i Underrättelsekommitténs 345 sidor långa rapport; en av underrättelsetjänstens viktigaste uppgifter är ju just att förvarna Sveriges politiska ledning så att (militär) överraskning kan förhindras. Och överraskning uppnås bl.a. med hjälp av vilseledning.

När det gäller *överraskning* skriver dock Försvarsberedningen 1999 följande:

> Rysslands offensiva förmåga i området är i dag starkt begränsad. Även Nato saknar utan en omfattande tillförsel av stridskrafter offensiv kapacitet i området. De alltmer förbättrade möjligheterna att uppnå överraskning med strategiskt rörliga insatsstyrkor bör dock observeras.[28]

När det gäller desinformation behandlar Försvarsberedningen 1999 det i avsnittet om att stärka det svenska samhället vid svåra påfrestningar i fred och icke-statliga aktörers eventuella möjligheter att påverka Sverige.[29] *Sårbarhetsutredningen* nämner desinformation i samband med IT-relaterade hot och överraskning i samband med utveckling av elakartade dataprogram samt klimatförändringarnas inverkan på den biologiska mångfalden.[30] Dessa sammanhang är inte de som avses i föreliggande rapport.

Det är inte avsikten att här redogöra för alla textsammanhang i de fyra dokumenten där de sökta orden förekommer. En granskning av de aktuella textavsnitten resulterar i den sammanfattande bedömningen att de bedömningar som görs synes välgrundade och täcker ett brett spektrum av frågor och aspekter när det gäller informationskrigföring och –operationer. Icke desto mindre kvarstår snedfördelningen med slagsida mot IT-relaterade hot.

Mer anmärkningsvärt är kanske att de säkerhetspolitiska kontrollstationerna (Försvarsberedningens rapporter), som ju är till för att kritiskt granska omvärldsutvecklingen och så tidigt som möjligt förvarna om en eventuellt oönskad utveckling i syfte att kunna

---

[26] Försvarsberedningen, *Gränsöverskridande sårbarhet—Gemensam säkerhet*, s. 117.
[27] SOU, *Underrättelsetjänsten—en översyn*, s. 251-252 och 254.
[28] Försvarsberedningen, *Förändrad omvärld—omdanat försvar*, s. 227.
[29] Ibid., s. 95.
[30] SOU, *Säkerhet i en ny tid*, s. 200, 215 resp. 267.

vidta anpassningsåtgärder, inte diskuterar vilseledning och desinformation i ett längre tidsperpsektiv. Hoten, riskerna och sårbarheterna diskuteras nästan enbart ur ett realtidsnära (IT- eller i bland medierelaterat) perspektiv. En titt i tabell 2 ger också intrycket av att världen blivit ännu lugnare sedan 1999.[31] Dessutom sammanfaller Försvarsberedningens rapport 2001 i tiden med det svenska EU-ordförandeskapet. Lite cyniskt skulle man av detta kunna dra slutsatsen att kontrollstationernas ursprungliga syfte (att misstänksamt granska omvärlden) har fått stå tillbaka för en diplomatisk-idealistiskt mer politiskt korrekt bedömning. Tyvärr är det just denna typ av mekanism som en skicklig deceptör kan utnyttja. Ordet *informationskrigföring* som är i frekvent bruk även i internationella forum har dock kunnat användas i de säkerhetspolitiska bedömningarna.

För att återknyta till detta avsnitts rubrik kan vi alltså konstatera att de säkerhetspolitiska kontrollstationerna synes utgöra korrekta bedömningar av omvärldsläget i närtid. I lite mera traditionell realistisk säkerhetspolitisk anda saknar vi dock den mer subtila och långsiktiga hotbilden när det gäller informationskrigföring, nämligen den del som handlar om vilseledning, desinformation i syfte att påverka opinioner över tiden och psykologisk krigföring.

Trots de initiala, något euforiska, förhoppningarna om "fred på jorden" efter att supermaktskonfrontationen upphört kan man konstatera att den tidigare stabila och 'endimensionella' världsordningen har ersatts av en ur policysynpunkt och praktisk hanterbarhetssynpunkt besvärligare 'flerdimensionell' säkerhetspolitisk situation. Den säkerhetspolitiska uppmärksamheten måste vara riktad mot flera håll samtidigt och olika strategier kan komma att behövas för att lösa problemen på de olika fronterna.[32] I dagens multipolära värld finns det fler potentiella motståndare, i synnerhet när det gäller frågor som rör ekonomi, teknik och t.ex. internationellt politiskt inflytande. Förutsättningarna för strategisk analys och "förutsägelser om framtiden" kompliceras också av att vilseledning förekommer, vilket tydligt exemplifieras av t.ex. ett antal länders ansträngningar att dölja sin uppbyggnad av arsenaler av massförstörelsevapen.

[31] Visserligen hade NATO:s operation mot Serbien 1999 avslutats när några av dessa SOU:er och departementsskrivelser skrevs. Samtidigt hade spänningen mellan USA, Ryssland och Kina ökat i samband med de amerikanska planerna på ett nationellt robotförsvar samt NATO:s utvidgningsplaner. Efter den 11 september 2001 har dock framför allt Rysslands relationer med USA och EU väsentligen förbättrats.
[32] Jenny Clevström, Lena Norlander och Wilhelm Unge, *Rysk toxin- och bioregulatorkompetens*, FOA-R—00-01703-170—SE, december 2000, s. 25.

3. Vilseledning – Definition, realiserbarhet och praktik

The greatest derangement of the mind is to believe something because one wishes to do so.

Louis Pasteur[33]

Detta kapitel inleds med några allmänna reflektioner kring vilseledning och resonemang kring varför vilseledning behöver beaktas i säkerhetspolitiska sammanhang. Därefter ger vi en definition av samt en kort översikt över innebörden i begreppet vilseledning.

3.1 Vilseledning – ett kontroversiellt begrepp

Vilseledning är ett kontroversiellt begrepp. Även om hela spektrumet av ståndpunkter återfinns i debatten tenderar ytterlighetsståndpunkterna att dominera, varav den ena ståndpunkten är att vilseledning inte är realiserbart i det moderna och genomskinliga informationssamhället eller på det digitala stridsfältet och den andra är att vilseledning alltid lyckas. Däremellan finns t.ex. ståndpunkten att försök till vilseledning nog förekommer men att de oftast genomskådas eller får otillräcklig effekt. För en diskussion se t.ex. Hans Furustigs rapport *Militär vilseledning – Några grunder*.[34]

Vi försöker i denna rapport presentera en mer balanserad bild. Icke desto mindre kan man konstatera att den historiska statistiken talar ett mycket entydigt språk. Den store auktoriteten på området, Barton Whaley, hävdar att ju högre grad av ansträngning för att vilseleda desto högre grad av överraskning. Han konstaterar att vid en undersökning av 76 fall av strategiska anfall med vilseledande åtgärder uppnåddes överraskning i samtliga fall.[35] Detta rör förvisso krigsfall. Men även i fredstid har vilseledning av främst kapacitetsdöljande karaktär förekommit och varit framgångsrik. Tysk militär upprustning under mellankrigstiden, sovjetisk militärindustriell kapacitet före andra världskriget, de s.k. *bomber gap* och *missile gap* under 1950-talet, det okända sovjetiska offensiva biologiska vapenprogrammet och Saddam Husseins hemliga program för utveckling av massförstörelsevapen och 1998 Indiens framgångsrika döljande av förestående provsprängningar är bara några exempel på att vilseledning förekommer och kan lyckas.

Den mycket erfarne brittiske underrättelsemannen Michael Herman menar t.ex. att

> *Deception applies mainly in war. Its peacetime significance is exaggerated, since the literature about it tends to expand it to include the much more general run of governments' propaganda and news presentation.*[36]

Samtidigt medger Herman att vilseledning under de rätta omständigheterna kan vara ett potent vapen. När det gäller vilseledningens effekt menar Herman att

[33] Citatet är taget från Michael Dewar, *The Art of Deception in Warfare*, kap. 11.
[34] Hans Furustig, *Militär vilseledning — Några grunder*, FOA-R—96-00365-5.2—SE.
[35] Michael Aust, *Strategisk överraskning, varning och beslut*, C-uppsats ht-96 vid Uppsala univ., s. 3.
[36] Michael Herman, *Intelligence Power in Peace and War*, (Cambridge University Press, 1996), s. 170.

> *Its most pervasive effect in the Cold War was however that the deception threat caused all intelligence to be treated with caution, casting doubt on good as well as bad. Humint in particular tends to be devaluated in this way, by users' fears that its reports may have been planted by the opponent.*[37]

Ovanstående problem kvarstår naturligtvis även efter det kalla krigets slut. Det är idag dock svårt att se att fredstida vilseledning skulle kunna hota Sveriges existens. Däremot menar vi att vilseledning exempelvis skulle kunna skada svenska nationella intressen, äventyra svensk trupps säkerhet i samband med internationella insatser eller åsamka Sverige ekonomisk skada. Efter det kalla krigets slut har hotbilden blivit mer diversifierad och antalet uppgifter för såväl Försvarsmakten som övriga totalförsvarsmyndigheter och andra myndigheter blivit mer svårhanterliga samtidigt som hotbilden generellt sett har blivit mer godartad. Flera områden har kommit att omfattas av säkerhetspolitiken, såsom t.ex. ekonomi. Samtidigt som de internationella relationerna och hotbilden blivit mer godartade har antalet potentiella motståndare ökat. I denna situation finns det ett större utrymme för deceptörer. Med begreppet deceptör avses den som planerar och genomför vilseledning.

Ett särskilt problemområde för Sverige som en liten stat med begränsade resurser är behovet av strategisk förvarning, ett behov som accentuerats av den anpassningsfilosofi Sverige för närvarande tillämpar. Om en stat med aggressiva avsikter gentemot Sverige tillämpar kapacitetsdöljande vilseledning för att rusta upp kan Sverige få svårt att upptäcka detta i tid för att vidta lämpliga åtgärder. Optimisterna säger att detta inte kan hända, men historien visar att det kan hända och har hänt.

Wilhelm Agrell beskriver på ett målande sätt i sin bok *Konsten att gissa rätt – Underrättelsevetenskapens grunder* problemen som underrättelseanalytiker ställs inför i samband med vilseledning.

> *Av alla de tolkningsproblem som underrättelseanalytiker ställs inför är de som sammanhänger med vilseledande operationer de mest intrikata. Underrättelsorganisationers inneboende tendens att generera självbedrägerier initieras och underblåses här av en utomstående manipulatör som successivt kan mata in nya uppgifter i underrättelsesystemet för att leda iväg analysen i önskvärd riktning. De vilseledande operationerna är ett spel mellan en medveten spelare och en mer eller mindre omedveten. Ju mer i detalj motståndaren, den medvetne spelaren, förmår indentifiera de intellektuella och systemgenererande svagheterna i offrets underrättelse- och beslutsstruktur, desto mer raffinerat kan dessa svagheter stimuleras så att den vilseledande operationen till sist blir självgående. Vrångbilden har blivit en del av normalbilden.*[38]

[37] Ibid., s. 170.
[38] Wilhelm Agrell, *Konsten att gissa rätt – Underrättelsevetenskapens grunder*, (Studentlitteratur, Lund, 1998), s. 203.

3.2 Definition av vilseledning

I detta avsnitt definieras vad som avses med vilseledning i föreliggande rapport och vilken dess relation till ledningskrigföring är. Dessutom beskrivs vilseledningens principer och förutsättningar. Som jämförelse anges i bilaga 1 ett antal andra definitioner av vilseledning. I det efterföljande kapitlet ges några exempel på strategisk vilseledning för att tydliggöra innebörden i begreppet. Fler exempel återfinns i del 2 av rapporten.

3.2.1 Vilseledning – en del av informationskrigföringen

Enligt nuvarande svensk terminologi är vilseledning en del av ledningskrigföring. I Försvarsmaktens *Huvudstudie Ledningskrigföring* definieras vilseledning som

> *Verksamhet som syftar till att ge motståndaren eller annan aktör ett felaktigt beslutsunderlag för att få honom att disponera sina resurser på ett för våra avsikter gynnsamt sätt.*[39]

Försvarsmaktens *Huvudstudie Ledningskrigföring* definierar vidare ledningskrigföring som:

Militär verksamhet som syftar till att påverka motståndarens eller annan aktörs omvärldsuppfattning och nedsätta hans förmåga att utöva ledning. Ledningskrigföring består av ledningsbekämpning, vilseledning, psykologiska operationer och skydd mot informationsinhämtning.[40]

Kopplingen mellan ledningskrigföringens olika komponenter framgår av fig. 2 till höger. Ledningskrigföring är i sin tur den militära delen av det vidare begreppet informationskrigföring.[41] I bilaga 1 görs en genomgång av ett antal olika definitioner av vilseledning.

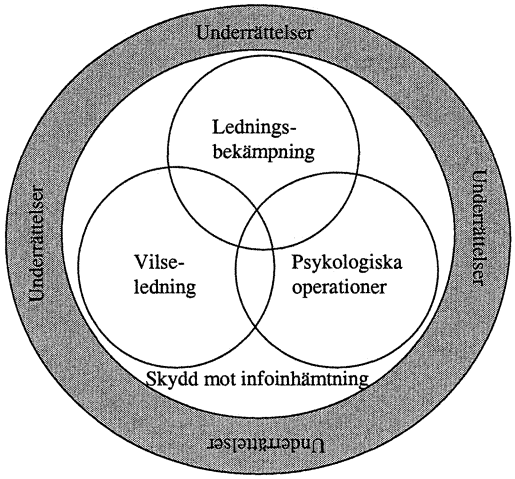

Fig. 2. Definition av ledningskrigföring.

Oaktat att en del av de i bilaga 1 anförda definitionerna ur lexikografisk synpunkt inte är korrekta[42] och oaktat det faktum att de flesta hänför sig till det militära området rymmer

[39] Försvarsmakten *Huvudstudie Ledningskrigföring - slutrapport*, s. 28.
[40] Ibid., s. 28 och 31.
[41] Se t.ex. *Huvudstudie Ledningskrigföring – slutrapport* och Försvarshögskolan, *ASTA-studien—Ett regeringsuppdrag om aktiva åtgärder rörande Informationskrigföring.*
[42] Till exempel är definitionen i *Nomen F 97* ett exempel på en s.k. cirkeldefinition. Ordet vilseledning förklaras med hjälp av ordet vilseleda som inte är definierat. Detta är inte godtagbart enligt lexikografiska principer. För en genomgång av lexikografins grunder och i synnerhet definitioners konstruktion hänvisas till Bo Svenséns bok *Handbok i lexikografi (TNC 85)*. Svensén är verksam vid Tekniska nomenklaturcentralen (TNC).

de de väsentliga elementen som vi i föreliggande rapport menar är centrala för en definition av begreppet vilseledning. Enligt vår mening omfattar vilseledning fem centrala element som därför bör framgå av definitionen. Deceptörens vilseledande åtgärder

- skall vara medvetna och inte resultatet av andra omständigheter,
- skall syfta till att bibringa vilseledningsobjektet en felaktig verklighetsuppfattning och därmed ett felaktigt beslutsunderlag,
- som i sin tur syftar till att få vilseledningsobjektet att agera (eller avstå från att reagera, om detta är deceptörens avsikt), inte enbart tro någonting,
- och helst få vilseledningsobjektet att agera på det sätt deceptören avser och
- åstadkomma en fördel för deceptören.

Med begreppet deceptör avses, som tidigare nämnts, den som planerar och genomför vilseledning. Med vilseledningsobjekt menas den som är målet för vilseledningen.

Sammanfattningsvis kan vi därför anta följande definition av vilseledning:

Med vilseledning avses medvetna åtgärder som syftar till att ge vilseledningsobjektet en felaktig verklighetsuppfattning och därmed ett felaktigt beslutsunderlag i syfte att få honom att agera på ett för deceptörens avsikter gynnsamt sätt.

Ovanstående definition överensstämmer i andemening med den definition som används i *Huvudstudie Ledningskrigföring* och *ASTA-studien* även om den exakta ordalydelsen varierar något. Dessa studiers förslag till terminologi synes därför kunna ligga till grund för en nationell terminologi som bas för det fortsatta arbetet inom informationskrigföringsområdet.

Ett vanligt sätt att betrakta vilseledning är att dela in den i nivåer. Vilseledning kan delas in i strategisk, operativ, taktisk och stridsteknisk vilseledning, varav de tre sista hänför sig till det militära området. Med strategisk avses den nationella nivån. Med t.ex. strategisk vilseledning avses följaktligen att vilseledningen genomförs och/eller får konsekvenser på den strategiska nivån.[43]

Med strategisk vilseledning avses i denna rapport vilseledning som berör ett helt land och dess säkerhetspolitiska sfär eller nationella intressen. I denna vilseledning ingår politiska, militära, ekonomiska, informationsanknutna och andra former av vilseledande åtgärder. Med nationella intressen avses t.ex. för landet betydelsefulla ekonomiska intressen, Sveriges prestige eller trovärdighet i det internationella samfundet eller svensk trupps säkerhet vid internationella operationer.

[43] Det är värt att understryka att någon skarp gräns mellan olika nivåer knappast existerar. En mer begränsad vilseledningsoperation med att specifikt mål skulle t.ex. kunna eskalera och få konsekvenser för hela den utsatta staten vilket skulle medföra att man kan tala om strategisk vilseledning. Situationen skulle också kunna vara sådan att vilseledningen initieras av en främmande makts underrättelsetjänst med syftet att påverka Sverige. Även om operationen inte får nationella konsekvenser gör det faktum att den initierades på den strategiska nivån att den bör klassificeras som (försök till) strategisk vilseledning.

Strategisk vilseledning är tillämplig i alla tidsfaser; fred, kris och krig. I första hand behandlar vi i denna rapport fredstida förhållanden samt krissituationer (jfr avsnitt 2.2).

Avslutningsvis kan det vara på sin plats att placera in vilseledning bland övriga underrättelseaktiviteter. Enligt de flesta betraktelsesätt ses vilseledningens kärnfunktion som ett sätt att dölja något. Sett ur ett underrättelseperspektiv återfinns vilseledning som ett element i informationssäkerhetskomplexet (se fig. 3).

I sin bok *Intelligence Power in Peace and War* diskuterar Michael Herman relationerna mellan "intelligence and security".[44] Han menar att informationssäkerhet består av tre komponenter:

- Protective security
- Detection and neutralization of intelligence threats
- Deception

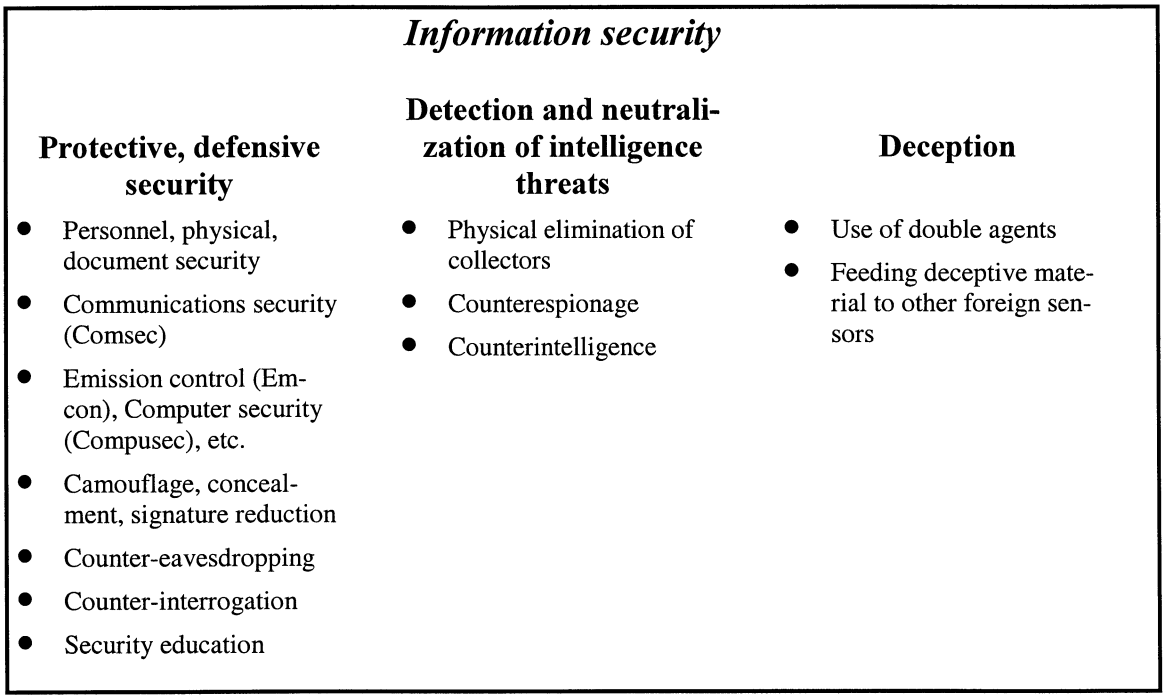

Fig. 3 Informationssäkerhetens komponenter.[45]

Den första komponenten består av passiva, defensiva åtgärder/skydd som syftar till att få bukt med eller ta udden av främmande underrättelsetjänsters insamling. Den andra komponenten innebär aktiva försvarsåtgärder för att eliminera motståndarens

[44] Michael Herman har 35 års erfarenhet av arbete på olika nivåer i den brittiska underrättelseapparaten. I sin välrenommerade bok *Intelligence Power in Peace and War* kombinerar han en teoretisk framställning av underrättelsetjänstens uppgifter, funktionssätt och effekter för en stats ledning, med praktikerns stora erfarenhet. Michael Herman, *Intelligence Power in Peace and War*, kap. 10, s. 165-182.
[45] Bilden tagen från Michael Herman, *Intelligence Power in Peace and War*, s. 169.

offensiva underrättelsehot. Den tredje komponenten, vilseledning, syftar till att besegra främmande underrättelseinsamling genom att vilseleda eller förvirra.

Denna tolkning av vilseledning, som hörandes hemma i en stats defensiva del av underrättelsesfären, sammanfaller till stor del med det traditionella sovjet-ryska begreppet maskirovka. Strategisk maskirovka "omfattar ett komplex av åtgärder för att hemlighålla..." (se vidare definition i bilaga 1 samt avsnitt 3.5), dvs. i huvudsak döljande verksamhet eller åtgärder syftande till att stärka informationssäkerheten.

Inom ramen för den döljande eller säkerhetsbringande verksamheten kan såväl aktiva som passiva eller om man så vill framhävande och döljande åtgärder utnyttjas (se avsnitt 3.3). I fredstid synes de flesta vilseledningsoperationer vara av intentions- eller förmågedöljande typ.[46] I kris och krig ökar som regel andelen framhävande vilseledning. Detta sammanhänger till del med det faktum att större värden står på spel under dessa tidsskeden (t.ex. en stats existens eller en armés avgörande utgång i en militär operation) och att därför kostnad-risk-kalkylen ser annorlunda ut för objektet respektive deceptören. En avslöjad säkerhetspolitisk vilseledningsoperation under fredstid ger upphov till stora politiska kostnader för sändaren, varför mottagarens förväntan om vilseledning torde vara låg. Under krigstid är sannolikt förhållandet omvänt, i synnerhet i militära sammanhang. Kostnaden för beslutsångest är hög, vilket framtvingar mer definitiva och snabba ställningstaganden, vilket i sin tur premierar vilseledningsinsatser. Den politiska kostnaden för sändaren av en vilseledningsoperation är i detta fall låg, därför att den glöms bort snabbare i en kontext av ständigt konkurrerande händelser.

[46] Med förmågedöljande avses här att förmågan framställs som mindre än den verkligen är (jfr fig. 4). Två intressanta exempel på vilseledning, där förmågan framställdes som varandes större än den verkligen var, är Sovjetunionens framhävande i fredstid av de s.k. missil- och bombargapen under 1950-talet. Av dessa exempel kan man lära sig att vilseledning är en riskfylld aktivitet. Trots att dessa raffinerade vilseledningsoperationerna lyckades blev resultatet paradoxalt nog att USA snarare ökade sitt rustningsmässiga försprång än minskade. Fallen beskrivs utförligare i del 2, avsnitt. 3.5.

3.3 Hur genomförs vilseledning?

I sin enklare form består desinformation av rökridåer; falsk eller tillrättalagd information som läggs ut för att skyla verkliga förhållande.
[---]. I sin mer avancerade form är syftet med desinformationen inte bara att, likt sekretessen, förhindra att de faktiska förhållandena klarläggs. Istället tar här desinformationen sin utgångspunkt i betraktaren, dennes observationsmöjligheter och tolkningsmönster. Desinformationen utgör en anti-analys där objektet styr iakttagarens analytiska process utan att denne är medveten om detta.

Wilhelm Agrell[47]

Avsikten med detta avsnitt är att på ett mycket förenklat sätt tydliggöra vad vilseledning handlar om och hur dess principiella funktionssätt ser ut. En utförligare beskrivning görs i kap. 5.

Betraktar man vilseledningsåtgärdernas karaktär kan man dela in dem i aktiva respektive passiva åtgärder.

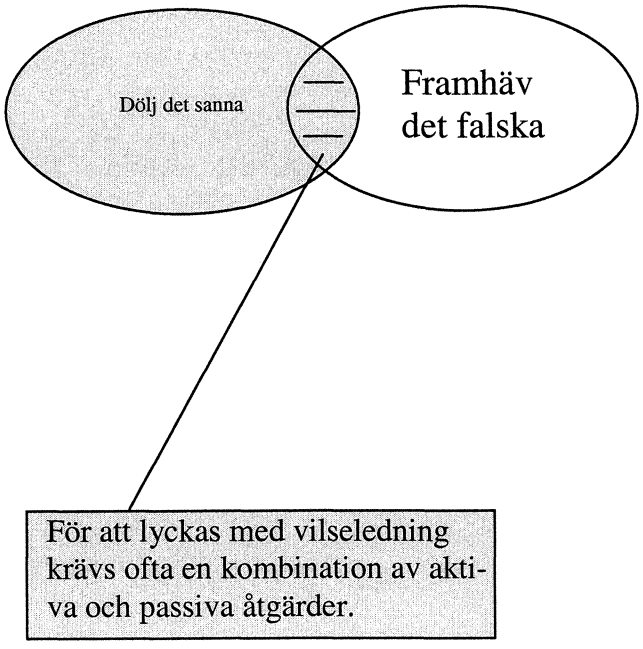

Fig. 4 Vilseledningens grundprinciper.[48]

Med aktiv (framhävande) vilseledning avses framhävandet av falsk information genom att avsiktligt bjuda vilseledande kritisk information för att skapa ett felaktigt beslutsunderlag och därigenom nå verkan hos vilseledningsobjektet.

Med passiv (döljande) vilseledning avses döljandet av sann information genom att eliminera eller undandra kritisk information för att i skyddande syfte försämra vilseledningsobjektets beslutsunderlag.

Med kritisk information avses sådan information som har vital betydelse för att motståndaren ska kunna planera och agera.

[47] Wilhelm Agrell, *Konsten att gissa rätt – Underrättelsevetenskapens grunder*, s. 202.
[48] Försvarsmakten *PM Vilseledning*, 21 120:73579, 1997-12-15.

Ett karaktäristiskt drag hos lyckosamma vilseledningsoperationer är att de innehåller en avsevärd mängd trovärdig och verifierbar information. Med andra ord behövs även olika kombinationer av framhävande av sann information tillsammans med undertryckande av andra delar av dito samt lämpligt döljande av falsk information i syfte att få den att framstå som trovärdig. De döljande åtgärder som döljer falsk information får dock inte vara ogenomträngliga för vilseledningsobjektet. Avsikten är ju att han skall lyckas penetrera skyddet och ta till sig den falska informationen.

Det som historiskt har kännetecknat lyckade militära vilseledningsoperationer är inte att den angripne blivit fullständigt överrumplad, utan trots att förvarning givits har den angripne inte dragit de riktiga slutsatserna och sett konsekvenserna av samt reagerat på de observerade förberedelserna i tid och med tillräcklig kraft. Samma tendens uppträder i andra vilseledningssammanhang där åtgärderna inte har varit av militär natur och syftat till förberedelse för krig.

Människan står i fokus för vilseledning och går att lura trots, och ibland tack vare, den moderna tekniken. Genom att i tid och rum samordna vilseledande åtgärder kan en deceptör:

- förse vilseledningsobjektet med felaktig information
- skapa osäkerhet
- fördröja analysen
- mätta hans bearbetningskapacitet

Därmed kan deceptören få vilseledningsobjektet att fatta felaktiga beslut.

Deceptörens verksamhet resulterar i denna effekt hos vilseledningsobjektet...

Vid planerandet och genomförandet av vilseledningsoperationer kan följande sex principer urskiljas:[49]

Fig. 5 Vilseledningens effekter på vilseledningsobjektet.

[49] Fritt efter Försvarsmakten *PM Vilseledning*, s. 11-12.

- **Fokusering**. Vilseledningen måste fokusera den beslutsfattare som är i stånd att vidta de önskade åtgärderna. Motståndarens underrättelsesystem är normalt inte målet för vilseledningen. Det är bara den primära kanalen genom vilken deceptören förmedlar den vilseledande informationen till beslutsfattaren.

- **Mål**. Målet med vilseledning skall vara att få vilseledningsobjektet att agera (eller att inte agera) på ett visst sätt. Han skall alltså inte bara tro vissa saker. Hans agerande skall också öka deceptörens chanser att nå sina syften.

- **Kontroll**. En vilseledningsoperation måste ledas och följas upp av en instans. Detta krävs för att undvika förvirring och för att säkerställa att de olika elementen i vilseledningen spelar upp samma vilseledningshistoria och att dessa inte står i konflikt med andra politiska, militära m.fl. mål. Genomförandet av vilseledning kan emellertid decentraliseras så länge alla deltagare ansluter sig till en gemensam plan.

- **Säkerhet**. Vilseledningsobjektet måste förnekas kunskap om deceptörens avsikt att vilseleda och om genomförandet av denna avsikt. Framgångsrika vilseledningsoperationer kräver sekretess. Need-to-know-kriterier tillämpas i varje vilseledningsoperation och i varje del av denna. Samma grad av säkerhet omger både verkliga och vilseledande aktiviteter i syfte att undvika anomalier som kan avslöja vilseledningen och samtidigt göra den trovärdig.

- **Tidssamordning**. En vilseledningsoperation kräver noggrann samordning i tiden. Tillräckligt med tid måste avdelas för vilseledningshistoriens olika delar att spelas upp; för vilseledningsobjektets underrättelsesystem att samla in, analysera och rapportera; för de vilseledda beslutsfattarna att reagera och för de egna underrättelseorganen att upptäcka de åtgärder/aktiviteter som vilseledningsobjektets beslut resulterar i.

- **Integration**. Varje form av vilseledning måste vara helt integrerad i den säkerhetspolitik i övrigt som den understödjer. Vilseledningshistorien måste utarbetas i harmoni med övergripande nationella mål. Planering av vilseledning måste ske parallellt med planeringen av övriga säkerhetspolitiska målsättningar och åtgärder.

Den egna underrättelse- och säkerhetstjänsten är av vital betydelse för planerings-, genomförande- och avslutningsfaserna av varje vilseledningsoperation. Underrättelse- och säkerhetstjänsten fyller följande funktioner för deceptörerna:

- Identifierar vilseledningsobjektets beslutsfattare och bedömer deras sårbarhet för vilseledning.
- Gör en bedömning av vilseledningsobjektets uppfattning om deceptörens förmåga och möjliga handlingsalternativ.
- Bedömer vilseledningsobjektets eventuella agerande i olika scenarier och "spelar" igenom möjliga utfall med deceptörerna.
- Upprättar och övervakar återkopplingskanaler för att utvärdera vilseledningsoperationens utfall genom att observera vilseledningsobjektets reaktion.

- Identifierar vilseledningsobjektets informationsinsamlingsförmåga och kommunikationssystem för att fastställa de bästa inkanalerna för den vilseledande informationen.
- Penetrerar de säkerhetsåtgärder som vilseledningsobjektet vidtagit för att skydda sig.

Underrättelseanalytikerna måste leta efter återkopplingar från vilseledningen under det att de försöker identifiera möjliga framtida handlingsalternativ för motståndaren. På grund av den höga sekretessen kan dock som regel endast de underrättelseanalytiker som direkt deltar i genomförandet vara invigda i operationen. Vid en genomgång av verkliga vilseledningsoperationer finner man att dessa ofta inte utvecklas exakt i enlighet med den ursprungliga planen. Man finner också att skickliga deceptörer har förmågan att kontra eventuella mindre bakslag samtidigt som de har förmågan att utnyttja hastigt uppkomna nya chanser att förstärka vilseledningen.

3.4 Är vilseledning realiserbart i dagens informationssamhälle?

> *Informationssamhällets stora utbud av information är både en tillgång och en belastning. Tillgången består i den ökande mängden tillgängligt material i form av öppna källor. Belastningen består i att även bruset ökar – i förhållande till den relevanta informationen. Det betyder att datainsamling i någon mån underlättas, under förutsättning att den inriktas på ett effektivt sätt, men att sovring och analys försvåras. Eftersom tiden ofta är en knapp resurs betyder det därmed att bearbetningskapaciteten riskerar att bli en flaskhals.*
>
> Hans Furustig och Nils-Emil Lindahl[50]

Svaret på frågan huruvida vilseledning är genomförbart i dagens informationssamhälle är ja. Utifrån ett teoretiskt resonemang hävdar Barton Whaley att vilseledning (*deception*) men även skydd mot vilseledning (*counter-deception*) i teorin alltid är möjligt. Whaleys övertygande argumentation återfinns i avsnitt 6.1 och kommenteras därför inte vidare här. Och den tidigare praktiserande deceptören Ladislav Bittman konstaterar att

> *Practitioners of international deception games, regardless of their loyalty, know that deception is easy to perpetrate against anyone willing to be deceived.*[51]

Det har hävdats att den informationstekniska revolutionen skulle komma att omöjliggöra desinformation och vilseledning. Såväl det civila samhället som det digitala slagfältet kommer att bli genomskinligt. Två grundläggande faktum gör att denna utsaga ter sig orealistisk.

För det första ger informationstekniken tillgång till data, som måste bearbetas till relevant underlag för beslutsfattare. De flesta tekniska långtidsprognoser är ense om att en obalans även framgent kommer att råda mellan datainsamlingsförmåga och bearbet-

[50] Furustig, Hans och Lindahl, Nils-Emil, *Omvärldsanalys*, FOA-R—95-00129-5.3—SE, maj 1995, s. 30.
[51] Ladislav Bittman, *The KGB and Soviet Disinformation—An Insider's View*, (Pergamon-Brassey's, USA, 1985), s. 35.

ningskapacitet varför framtagandet av beslutsunderlag knappast kan förväntas gå fortare i framtiden.

För det andra möjliggör informationstekniken inte bara insamling utan även spridande av (des)information. Lars Ulfving pekar på faran med s.k. virtuella samhällen.[52] I den digitala världen kan informationsaktören uppträda med virtuell identitet. Denna virtuella värld saknar geografisk närhet och organisatorisk tillhörighet samtidigt som kommunikationen är tidsoberoende. Vidare har informationsaktören direktkontakt med målgruppen. I en sådan virtuell miljö "är den kulturella processen mycket snabb vilket får till följd att *förändrade värderingar mycket snabbt kan genomsyra målgruppen – detta är kanske det viktigaste i hela informationskrigföringen.*"[53]

Dessutom lever vi västvärlden i ett utpräglat produktivitetsparadigm där allt mer förväntas av varje medarbetare. Allt mindre tid kan ägnas åt varje enskilt ärende. Detta gäller såväl den offentliga som den privata sektorn. Detta medför ett ökande beslutstempo. Därtill kommer internationaliseringen med ytterligare krav på ställningstaganden och beslut.

Sammanfattningsvis kommer alltså såväl framtida underlagsframtagares som beslutsfattares situation sannolikt att karaktäriseras av

- ett ökande informationsinflöde och
- ett ökande beslutstempo

samtidigt som deceptörens situation gynnas av

- en ökande desinformationsspridningsförmåga.

Detta leder i sin tur till att en eventuell deceptörs möjligheter snarare ökar än minskar i det framtida "genomskinliga" informationssamhället. Att statsmakterna insett detta framgår också med all tydlighet av nedanstående citat ur Försvarsberedningens säkerhetspolitiska kontrollstationsrapport 2001 (som visserligen berör samhällets sårbarhetsalstrande teknik i kontexten informationsoperationer).

> *En annan dimension som blivit alltmer framträdande i takt med att informationssamhället vuxit fram är informationsoperationer (---). Den ökade informationsmängden till enskilda medborgare ger detta större vikt. Samhällets beroende av datateknologi skapar möjligheter för en angripare att åstadkomma stora skador utan att använda konventionell krigföring. Informationsoperationer, både defensiva som offensiva, kommer därför att få en allt större betydelse ju viktigare informations- och datateknologin blir för ett samhälle.*[54]

[52] Lars Ulfving, *Den stora maskeraden—Sovjetrysk militär vilseledning: Maskirovka sett i ett historiskt perspektiv*, Försvarshögskolans Acta C8, 2000, s. 92-95.
[53] Ibid., s. 95 (Ulfvings kursivering).
[54] Försvarsberedningen, *Gränsöverskridande sårbarhet—Gemensam säkerhet*, s. 159.

3.5 Hur arbetar deceptörerna? Hur är de organiserade?[55]

Vid ett studium av litteraturen rörande vilseledning kan man urskilja tre olika typer av vilseledningsoperationer:

- Desinformation – falsk information som läcks ut till motståndaren för att vilseleda honom.
- Svart propaganda – propaganda vars avsändare är okänd, dvs. deceptören kan inte spåras ens vid noggranna källundersökningar.
- Inflytelseoperationer – utnyttjande av agenter i motståndarlägret (ofta personer nära beslutsfattare, journalister, vetenskapsmän eller andra inflytelserika personer) för att påverka beslutsfattare och allmänna opinioner.

Som regel har dessa operationer tre typer av deltagare:

- Deceptören – den som planerar och genomför vilseledningsoperationen.
- Vilseledningsobjektet (motståndaren) – ett land, en regering, en grupp, en individ.
- Offret – en oskyldig och ovetande åskådare som utnyttjas av deceptören för att verka mot vilseledningsobjektet.

Deceptörerna använder följande huvudsakliga kanaler för att sprida vilseledande information:

- Agenter utomlands i ställning värdefull för dessa operationer, t.ex. journalister, diplomater, partifunktionärer, riksdagsmän m.fl.
- Dubbelagenter.
- Ideologiska medarbetare i hemlandet på "handläggarnivå" vid tidningar, tidskrifter, radio, TV, fackföreningar, myndigheter, organisationer, resebyråer osv. Deceptörerna är beroende av dem för publikation av artiklar m.m. Själva ändamålet och att det är frågan om underrättelseverksamhet döljs för dem och de får endast de fakta som behövs för att de skall kunna spela sin roll.
- Tekniska kanaler som telefonavlyssning eller avlyssningsanordningar, dvs. man utnyttjar motståndarens avlyssning genom att ge honom falsk information.
- Desinformationsmaterial (förfalskningar[56]) levereras genom anonyma kanaler så att inte ens en noggrann undersökning kan lokalisera vem eller vilka som varit inblandade. I regel skickas materialet med post.

Desinformation är omsorgsfullt konstruerade falska meddelande som läcks eller på andra sätt introduceras i motståndarens kommunikationssystem. Den vilseledande informationen kan vara av politisk, militär, ekonomisk eller teknisk-vetenskaplig art. För att vara framgångsrik måste vilseledning- och desinformationsoperationer åtminstone delvis motsvara verkliga förhållanden eller allmänt accepterade synpunkter. Det behövs

[55] Första halvan av detta avsnitt bygger på ett PM av Boris Ljunggren, daterat 1977.

[56] Viktiga hjälpmedel vid desinformationskampanjer och förfalskningar är: stämplar, officiellt brevpapper, m.m. För att få tillgång till främmande länders statschefers m.fl. befattningshavares namnteckningar skickade sovjetblockets underrättelsetjänster t.ex. ut julkort. I retur fick man oftast både namnteckning och officiellt brevpapper.

också en avsevärd del trovärdig och verifierbar information (fakta) för att övertyga vilseledningsobjektet.

Vilseledning- och desinformationsoperationer har två riskmoment:

- Operativa risker – avslöjande av agenter eller underrättelseofficerare och/eller avslöjandeav deceptörens metoder och syfte.
- Politiska risker – att operationen avslöjas och förövarna får stå till svars inför den allmänna opinionen eller att den egna regeringen nappar på det som är avsett för offret eller motståndaren.[57]

Det minst riskfyllda vid utförandet av vilseledningsoperationer är att undvika levande desinformationskanaler eller agenter och ge skrivbordsoperationer prioritet, dvs. förfalskningar levererade per post eller Internet.

Den avhoppade tjeckoslovakiske deceptören Ladislav Bittman beskriver i sin bok *The Deception Game*[58] en arbetsdag på desinformationsfabriken. Arbetet bestod av studium, analys, diskussioner, möten och byråkratiskt pappersarbete. Huvudändamålet var att notera och dissekera alla motståndarens svagheter och känsliga eller sårbara punkter, och att analysera hans fiaskon och misstag för att kunna utnyttja dem. Underrättelserapporter från utlandet var den huvudsakliga källan till idéer. Individuella förslag till vilseledningsoperationer underkastades först en preliminär bedömning. Redan vid denna preliminära bedömning förkastades en majoritet av förslagen. De förslag som var tänkbara gick vidare till en panel där förslagsställaren mötte många frågor och kritik för att eventuella svagheter skulle upptäckas. Om förslaget gick igenom – eventuellt med justeringar – förelades det därefter chefen för under-rättelsetjänsten för godkännande. För en diskussion om hur resultat eller konsekvenser av vilseledningsoperationer i allmänhet utvärderades se avsnitt 3.6.

Bittman hävdar i sin bok att Sovjetunionen och dess satellitstater i Östeuropa årligen drev 300-400 vilseledningsoperationer under 1960-talet. 1965 ledde och koordinerade enbart den tjeckoslovakiska underrättelsetjänstens desinformationsavdelning mer än 100 operationer.[59]

När det gäller organisatoriska frågor ger litteraturen vid handen att deceptörerna oftast verkar inom ramen för små, mycket hemliga avdelningar inom ett lands underrättelsetjänst. Under krigstid kan även andra lösningar noteras, såsom t.ex. den brittiska vilseledningorganisationen the London Controlling Section och dess placering i The War Cabinet, det politiskt-militära högkvarteret (se avsnitt 4.1).

---

[57] Det sistnämnda kallas för rekyl. Ett exempel på detta ges i de kommenterade referenserna i del 2 (se Woodward (1987), *CIA:s hemliga krig*). Vi förutsätter här att man i demokratisk ordning har beslutat att strategiska vilseledningsoperationer är tillåtna, varvid det också följer att det finns en strikt sekretess, som i praktiken innebär att endast enstaka regeringsmedlemmar informerats på *need-to-know-basis*. Det åligger dessa närmast ansvariga politiker att förhindra landskadliga beslut utan att röja de hemliga operationerna.

[58] Ladislav Bittman, *The Deception Game—Czechoslovak Intelligence in Soviet Political Warfare*, (Syracuse, New York, 1972).

[59] Ibid., s. 16.

I exempelvis f.d. Sovjetunionen var strukturen mycket utbyggd redan i fredstid. Denna struktur omfattade alla aktiva åtgärder, dvs. såväl hemliga vilseledningsoperationer som den öppna statliga propagandaapparaten. Motsvarande strukturer fanns enligt sovjetiskt mönster i de östeuropeiska satellitstaterna. Politbyrån hade det övergripande ansvaret och fattade alla beslut rörande vilka operationer som skulle drivas. Genom kommunistpartiets sekretariat leddes tre parallella enheter:

- Internationella informationsavdelningen IIA (med ansvar för press, radio, böcker och ambassaders informationsverksamhet)
- Internationella avdelningen IA (med ansvar för utländska kommunistpartier, internationella och nationella fröntorganisationer, underjordiska radiostationer och Vetenskapsakademin)
- KGB (Tjänst A inom första huvuddirektoratet, dvs. utrikesunderrättelsetjänsten, med ansvar för svart propaganda, förfalskningar, desinformation, inflytelsagenter, manipulering av utländska medier och paramilitär hjälp)[60]

Enligt en CIA-studie rörande *Covert Action and Propaganda* kunde man i en KGB-manual läsa följande om desinformationens roll och informationsaktörernas uppgifter:

> *Strategic disinformation assists in the execution of State tasks, and is directed at misleading the enemy concerning the basic questions of the State policy, the military-economic status, and the scientific-technical achievement of the Soviet Union; the policy of certain imperialist states with respect to each other and to other countries; the specific counterintelligence tasks of the organs of the State Security...*
>
> *Disinforming on strategic matters falls within the jurisdiction of the government, the appropriate ministries and committees, and the high command of the country's armed forces. The organs of State Security constantly render assistance to the other departments on this matter...*
>
> *Tactical disinformation makes it possible to carry out the individual task of strategic disinformation and, in fact, comprises the principle disinformation work of the organs of State Security.*[61]

Oss veterligt finns det inga öppna källor som anger hur stora finansiella resurser som lades på propaganda och desinformation i vilseledande syfte. Enligt en grov uppskattning av CIA uppgick de sovjetiska ansträngingarna till 3 miljarder USD årligen 1978. Enligt CIA hade denna siffra ökat till 4 miljarder USD årligen 1982.[62]

Som framgår av andra stycket i citatet ovan hade även militärledningen i uppgift att bedriva strategisk desinformation. I den sovjetiska generalstaben var det Överstyrelsen

---

[60] Richard H. Shultz och Roy Godson, *Dezinformatsia—Active Measures in Soviet Strategy*, (Pergamon-Brassey's, USA, 1984), s. 17-34.

[61] *Hearings Before the Subcommittee on Oversight of the Permanent Select Committee on Intelligence*, House of Representatives, 6, 19 februari 1980, U.S. Government Printing Office, s. 63 (citerat i Bittman, *The KGB and Soviet Disinformation*, s. 49-50).

[62] US Congress, House, Permanent Select Committee on Intelligence, "Soviet Covert Action (The Forgery Offensive)", 96th Congress, 2nd Session (Washington, DC: GPO, 1980), s. 60 och US Congress, House, Permanent Select Committee on Intelligence, "Soviet Active Measures", s. 30 citerat i Richard H. Shultz och Roy Godson, *Dezinformatsia*, s. 31.

för Strategisk maskirovka (GUSM) som hade detta ansvar.[63] GUSM var formellt en enhet med samma rang som underrättelsetjänsten GRU eller operationsledningen GUO. GUSM:s huvudsakliga uppgift var sannolikt att dölja verklig krigstida förmåga och kapacitet. Vid ett möte mellan KGB-chefen Jurij Andropov och chefen för den rumänska underrättelsetjänsten, general Ion Pacepa, lär Andropov ha formulerat saken på följande sätt: "The most sacred Soviet-bloc secrets are military, and disinformation is the best way to keep them."[64] (jfr fig. 3).

Medan vissa länder traditionellt inte har gjort någon åtskillnad mellan öppen politisk propaganda och hemlig desinformation och vilseledning, såsom t.ex. Sovjetunionen och dess satelliter, har man i andra, t.ex. USA, varit noga med att särskilja dessa båda verksamheter. Detta har också avspeglat sig i dessa staters informationsstrukturers organisatoriska uppbyggnad. Hemlig desinformation och vilseledning har helt och hållet varit en syssla för underrättelsetjänsten CIA.[65]

Den höga sekretssgraden som i alla länder omger deceptörerna och deras verksamhet har varit och är en nödvändig förutsättning för framgångsrik vilseledning. Även den egna underrättelsetjänstens personal informeras som regel inte annat än i de fall då de skall medverka till operationens genomförande och uppföljning. Den avhoppade chefen för den rumänska underrättelsetjänsten, Ion Pacepa (se vidare avsnitt 4.4), beskriver avdelning D, som i desinformation, mycket målande:

> *It was not until late in the afternoon that I was able to visit the Disinformation Service, as Ceausescu had ordered. Disinformation is one of the most secret activities in any East European country, where the very word is tabu. Thus Service D was known within the Securitate as a small "Documentary Archives" unit, and its headquarters was hidden away on the fourth floor of an out-of-the-way Ministry of Interior building. The normal Securitate officers thought Service D was just an office with three teeler-like windows for receivning documentary requests from different intelligence units and replying with information found in its secret archives – as it did in fact actually do, for cover reasons. When I got there, a duty officer took me inside through an inconspicuous door, punching out a combination on its electronic lock to open it. After crossing a buffer zone that looked like an archives room, we entered the actual Disinformation Service.*[66]

[63] Se t.ex. Lars Ulfving, *Den stora maskeraden—Sovjetrysk militär vilseledning: Maskirovka sett i ett historiskt perspektiv*, s. 77-86.
[64] Ion Pacepa, *Red Horizons*, (Hodder and Stoughton, Sevenaoks, 1989), s. 196.
[65] Richard H. Shultz och Roy Godson, *Dezinformatsia*, s. 14.
[66] Ion Pacepa, *Red Horizons*, s. 121-122.

3.6 Hur utvärderar deceptören effekten av sin vilseledning?

> *Soviet disinformation operatives know that a single covert action, however precisely designed, cannot tip the balance of power between the Western Alliance and the Communist bloc. But they believe that mass production of propaganda and disinformation over a period of several decades will have a significant effect. The strategy seems to work.*
>
> Ladislav Bittman[67]

En viktig del i genomförande av en vilseledningsoperation är successiv utvärdering av dess effekt för att eventuellt kunna anpassa kommande vilseledande inspel till händelseutvecklingen.

Principiellt kan fyra metoder för deceptören att utvärdera effekten av sin vilseledning urskiljas. Den första och samtidigt säkraste metoden är att ha en mänsklig källa i motståndarlägret som kan tala om vilka bedömningar vilseledningsobjektet verkligen gör. En andra men samtidigt osäkrare metod är att anta ett reciprokt beteende. Detta innebär att deceptören sätter sig i vilseledningsobjektets situation och frågar sig hur han skulle (re)agera. Denna metod bygger på det faktum att underrättelse- och säkerhetstjänsters modus operandi (tillvägagångssätt) är relativt universellt, även om mindre avvikelser förekommer. En tredje och närbesläktad metod är att studera vilseledningsobjektets (re)aktion. Även denna metod inrymmer en viss osäkerhet då deceptören inte kan vara helt säker på att objektet inte spelar med i syfte att dubbelbluffa (se vidare kapitel 5).

En fjärde och mycket intressant metod, som framkommit i samband med debriefing av från Sovjetblocket avhoppade underrättelseofficerare som sysslat med vilseledning, är att deceptören litar till en ackumulerad effekt över tiden.[68] Eftersom det är svårt att exakt avgöra vilken effekt en enskild vilseledningsoperation eller desinformationskampanj har upprepas det vilseledande budskapet om och om igen. Dessutom drivs som regel ett antal operationer samtidigt vilka har samma eller näraliggande syften för att skapa synergieffekter. Denna utvärderingsmetod bygger på samma mekanismer som propaganda eller reklam utnyttjar och handlar alltså ytterst om frekvens och kvantitet.

Intressant att notera är också att denna utvärderingsmetod var tvådelad. Förutom den ackumulerade effekten på vilseledningsobjektet utvärderade man i kvantitativa termer det egna genomförandet. Som effektmått användes antalet genomförda operationer, antalet publicerade artiklar eller dylikt samt i vilka medier publiceringarna skedde och dessa mediers status, publiceringarnas innehåll och genomslag i debatten osv.

Som regel försöker sannolikt en deceptör kombinera alla eller flera av ovan beskrivna metoder i syfte att få en så korrekt utvärdering av sin vilseledning som möjligt.

---

[67] Ladislav Bittman, *The KGB and Soviet Disinformation*, s. 2.

[68] Se intervjuerna med den tjeckoslovakiske underrättelseofficeren Ladislav Bittman och KGB-officeren Stanislav Levtjenko i Richard H. Shultz och Roy Godson, *Dezinformatsia*, s. 165-185.

4. Exempel på strategisk vilseledning

Both Western and Soviet intelligence analysts consider the campaign for peace as one of the most successful propaganda campaigns of the last decade.
Ladislav Bittman[69]

I detta kapitel ger vi inledningsvis några exempel från mitten av och andra halvan av 1900-talet för att tydliggöra vad vi avser med strategisk vilseledning. Fler exempel och utförligare fallstudier finns i rapportens del 2.

Ett generellt problem vid redovisning av fall av vilseledning är att man behöver kunskap om både deceptörens verksamhet och vilseledningsobjektets verkliga (underrättelse-) bedömning av den pågående verksamheten, inte bara dennes reaktion. Som framgår av kapitel 5 är ett sätt att kontra vilseledning att spela med fast man i själva verket har genomskådat bluffen. Redovisningarna av fall i denna rapport, såväl del 1 som 2, bygger oftast på kunskap om deceptörens verksamhet och/eller vilseledningsobjektets reaktion. Två mycket intressanta undantag finns: *The bomber gap* och *The missile gap* under 1950- och 60-talen. Av avhemligade amerikanska dokument framgår att USA:s samlade underrättelsesamhälle verkligen blev vilselett avseende sovjetisk kapacitet rörande bombflyg och strategiska robotar. Se vidare del 2.

4.1 Operation Graffham

Inför *Operation Overlord* (landstigningen i Normandie i juni 1944) utformade de brittiska deceptörerna i the London Controlling Section (LCS), en ytterst hemlig grupp placerad i The War Cabinet, flera vilseledningsoperationer som syftade till att förhindra att tyskarna förstärkte försvaret av Atlantkusten i närheten av Normandie, genom att binda tyska styrkor på andra platser.

En sådan vilseledningsoperation var *Operation Fortitude North* vars syfte var att framhäva en allierad invasion i Norge. En deloperation i denna plan var *Operation Graffham* riktad mot Sverige 1944 och indirekt mot Tyskland. Tanken var att en kombination av utspel och signaler mot Sverige skulle uppfattas av den tyska underrättelsetjänsten och på det sättet nå Berlin som i sin tur skulle dra slutsatsen att de allierade verkligen planerade att invadera Norge. Sverige spelade alltså rollen av oskyldigt offer (se avsnitt 3.5) i denna operation.

Detta är ett av de få fallen av vilseledning riktad mot Sverige som projektgruppen har kunnat hitta i den öppna litteraturen. Fallet är relativt väl dokumenterat i flera källor, bl.a. historikern Charles Cruickshanks bok *Deception in World War II*,[70] i memoarer skrivna av en av medlemmarna i LCS[71] och på den svenska sidan av Leif Leifland.[72] De

[69] Ladislav Bittman, *The KGB and Soviet Disinformation*, s. 219.
[70] Charles Cruickshank, *Deception in World War II*, Oxford University Press, 1979. Boken baseras på avhemligade dokument från amerikanska och engelska arkiv.
[71] Dennis Wheatley, *The Deception Planners – My Secret War*, Hutchinson, London, 1980. Boken är skriven mer än 35 år efter händelserna under kriget. Till skillnad från Cruickshank har Wheatley inte använt något arkivmaterial. Boken har därför begränsat värde som exakt historiskt källmaterial. För den

brittiska deceptörerna ansåg denna operation var en av deras mest framgångsrika under kriget. Signalerna nådde mycket riktigt Berlin och två tyska divisioner omgrupperades till Norge för att förstärka försvaret.[73] Huruvida den svenska sidan verkligen blev vilseledd är fortfarande ovisst. En grundlig genomgång av *Operation Graffham* görs i del 2, avsnitt 2.1.

Operation Graffham var en krigstida vilseledningsoperation. De övriga operationer som redovisas nedan rör fredstida förhållanden.

4.2 Operation Neptun

1968 hoppade den tjeckoslovakiske underrättelseofficeren Ladislav Bittman av till USA. Bittman hade bl.a. varit vice chef för den tjeckoslovakiska underrättelsetjänstens avdelning D, desinformationsavdelningen. Han ger i sin bok *The Deception Game*[74] en enastående beskrivning av hur professionella deceptörer är organiserade och hur de arbetar.

En framgångsrik tjeckoslovakisk vilseledningsoperation var *Operation Neptun.*[75] *Operation Neptun*, som var riktad mot den västtyska regeringen, påbörjdes 1964. Den blev en av de mest framgångsrika vilseledningsoperationer som genomfördes under Bittmans tid som deceptör. Operationen hade flera mål.

För det första syftade operationen till att förlänga preskriptionstiden för brott begångna under nazisttiden. Preskriptionstiden skulle löpa ut i maj 1965. För det andra skulle operationen genom att utnyttja krigsförbrytelserna skapa antityska känslor och därmed slå split i det västeuropeiska lägret. För det tredje syftade *Operation Neptun* till att begränsa den västtyska underrättelseverksamheten på tjeckoslovakiskt territorium.[76]

Bakgrunden till operationen var följande. Mot slutet av kriget drog sig nazisterna undan från det centrala Tyskland som blev krigsskådeplats till Böhmen och Alperna. Med sig förde de förutom vapen och ammunition, värdeföremål och dokument/arkiv. Betydande delar av detta nazisternas sista gömställe kom efter kriget att hamna inom Tjeckoslovakiens gränser. Gömda nazidokument/-arkiv spelar huvudrollen i *Operation Neptun.*

---

som är intresserad av hur en vilseledningsorganisation byggdes upp och vilka karaktärsdrag dess medarbetare hade är boken dock av stort värde.

[72] Den brittiske historikern Cruickshank är en av Leiflands sekundära källor till *Operation Graffham.*

[73] Sett till effekten (två flyttade tyska divisioner) är detta knappast att betrakta som strategisk vilseledning. Ser man till syftet framträder ett strategiskt perspektiv; det handlade om de allierades strategi för återkomst till den europeiska kontinenten och därmed strategin för att vinna andra världskriget. Sett ur ett svensk synvinkel var *Graffham* en strategisk operation eftersom den syftade till att vilseleda hela den svenska stats- och militärledningen med de konsekvenser detta skulle ha fått för Sveriges nationella agerande och dispositionen av svenska förband m.m.

[74] Ladislav Bittman, *The Deception Game—Czechoslovak Intelligence in Soviet Political Warfare.*

[75] Avsnitt 4.2 bygger på kapitel 2 Operation Neptun i Bittmans bok *The Deception Game*, s. 39-72.

[76] Eftersom den västtyska underrättelsetjänsten bl.a. utnyttjade tidigare nazikollaboratörer för sin insamling bedömde de tjeckoslovakiska deceptörerna att tyskarna skulle avbryta alla kontakter med sina agenter om tjeckerna hittade gamla naziarkiv. Detta borde vara en elementär försiktighetsåtgärd för varje underrättelsetjänst, resonerade man i Prag; den tjeckoslovakiska underrättelsetjänsten skulle självt ha vidtagit denna försiktighetsåtgärd.

1946 ägde en incident rörande naziarkiv rum i Tjeckoslovakien. Denna incident blev utgångspunkten för *Operation Neptun*. Efter kriget fick de USA:s ockupationsmyndigheterna i Tyskland, genom förhör med krigsfångar, kännedom om en stor arkivgömma i Tjeckoslovakien. I februari 1946 genomfördes en specialoperation in på tjeckoslovakiskt territorium varvid arkivgömman kunde bärgas. Dokumenten lämnades sedermera tillbaka till de tjeckoslovakiska myndigheterna men då hade de allra viktigaste dokumenten tagits bort och resten hade fotograferats. Bland annat saknades alla listor med namn på alla tjeckiska kollaboratörer som samarbetat med nazisterna.

Avdelning D bestämde att en ny arkivgömma med nazidokument som kunde kompromettera västtyska politiker, underrättelsepersonal m.fl. skulle "hittas". I maj 1964 sänkte den tjeckoslovakiska underrättelsetjänsten ner fyra koffertar i Svarta sjön i Böhmen. Koffertarna innehöll hittills okända nazidokument från arkiv i Tjeckoslovakien och Sovjetunionen. Några veckor senare hittades koffertarna av ett tjeckoslovakiskt TV-team som gjorde en dokumentärfilm om trakten kring sjön.

Utöver de tre ovan nämnda målen med operationen tillkom under genomförandet ett fjärde, nämligen att utnyttja den för att hitta riktiga arkivgömmor på tjeckoslovakiskt territorium.

Fyndet blev en stor sensation såväl i Tjeckoslovakien som i omvärlden. Resulatet av *Operation Neptun* blev att preskriptionstiden för brott begångna under nazitiden förlängdes från maj 1965 till 31 december 1969. *Operation Neptun* var en avgörande faktor för det västtyska beslutet även om andra faktorer också spelade in.

I november 1964 vädjade den västtyska regeringen till regeringar, privata organisationer och personer om att inkomma med information som skulle kunna belysa hittills okända nazibrott innan preskriptionstiden löpte ut i maj 1965. Avdelning D upprättade kontakt med den tjeckoslovakiska organisationen *Union of Fighters Against Fascism* vars sekreterare Dr. Volejnik i december 1964 tog kontakt med den västtyska organisationen *Die Nazivervolgten* och överlämnade dokument rörande massakrer på civila i Sovjetunionen under kriget. Vid en gemensam presskonferens överlämnades dokumenten till en representant för *Center for the Prosecution of Nazi War Crimes*. I januari 1965 deklarerades officiellt att Tjeckoslovakien och Polen hade gått med på att samarbeta med de västtyska myndigheterna för att göra hittillls okänt material tillgängligt. I en rapport i febrauri 1965 förklarade den västtyske justitieministern att det material som tillhandahållits vittnade om hittills okända "brottskomplex".

Det tjeckoslovakiska utrikesministeriet hade också till USA, England, Frankrike och Holland överlämnat dokument rörande nazityska brott mot respektive lands medborgare under kriget, framför allt krigsfångar. Dokument rörande judar hade också tillställts judiska organisationer.

Under trycket från euro-amerikanska allierade, sovjetiska och israeliska protester samt uttalande från FN:s generalsekreterare och FN:s kommission för mänskliga rättigheter gav den väststyska regeringen vika i mars 1965 och förlängde preskriptionstiden efter en stormig debatt i förbundsdagen och regeringen.

Förutom en stor mängd artiklar i såväl Väst som Öst publicerade österrikiska, italienska och västtyska förlag böcker baserade på material från Svarta sjön. Den tjeckoslovakiska nyhetsbyrån CPA och den tjeckoslovakiska vetenskapsakademin tillhandahöll i god tro dokumenten och CPA tjänade dessutom pengar på verksamheten.

I detta sammanhang bör också en intressant utlöpare av *Operation Neptun* nämnas. Imponerade av operationens framgångarna skickade de sovjetiska deceptörskollegerna ett dokument rörande Österrikes f.d. kansler Kurt von Schuschnigg till Avdelning D. Von Schuschnigg internerades av Gestapo kort efter Österrikes Anschluss 1938 och tillbringade resten av kriget i ett koncentrationsläger. Det sovjetiska dokumentet var utformat som en deklaration i vilken von Schuschnigg gjorde politisk avbön och uttryckte sin vilja att arbeta för Hitler i utbyte mot nåd för hans egna politiska medarbetare. Han bad också om ursäkt för sina insatser under kanslertiden. De sovjetiska deceptörerma bad sina tjeckoslovakiska kolleger att offentliggöra "Schuschnigg-deklarationen" inför det österrikiska parlamentsvalet i mars 1966. Syftet var att misskreditera *Oesterreichische Volkspartei* och dess historiska traditioner och i synnerhet partiets förgrundgestalt von Schuschnigg. Planen misslyckades emellertid eftersom de tjeckoslovakiska deceptörerna inte hann publicera dokumentet före valet. *Oesterreichische Volkspartei* vann valet övertygande och trängde till och med ut *Sozialistische Partei Oesterreichs* ur koalitionsregeringen. Officiellt förklarades att socialistpartiets stöd till kommunisterna var orsaken till valförlusten.

Först i mars 1968 då den österrikiske socialisten Otto Leichter skrev boken *Zwischen zwei Diktaturen* kom debatten rörande "Schuschnigg-deklarationen" i gång i franska, österrikiska och västtyska medier. I boken återgavs deklarationens fulla text. Även om von Schuschnigg medgav existensen av deklarationen hävdade han att dess slutgiltiga utformning hade åstadkommits utan hans frivilliga samarbete. Hans signatur finns inte på dokumentet. Möjligen kan Gestapo genom omsorgsfull redigering ha givit dokumentet dess utseende. Även om offentliggörandet av "Schuschnigg-deklarationen" och dess påverkan på det österrikiska parlamentsvalet misslyckades förblev åsikterna i pressen delad om huruvida deklarationen var äkta eller falsk. Källkritiska studier lyckades dock aldrig fastställa att dokumentet kommit till offentlighetens ljus som ett resultat av en överlagd vilseledningsoperation.

För spridandet av sin vilseledande information under *Operation Neptun* använde Avdelning D endast officiella kanaler. Av säkerhetsskäl använde man inga inflytelseagenter eller kontaktpersoner inom utländska medier. De huvudsakliga spridningskanalerna var:

- Inrikesminister Strougals presskonferens där fyndet presenterades.
- Rapporter från inrikesministeriet (förberedda av Avdelning D).
- Den tjeckoslovakiska nyhetsbyrån CPA, som fick vinsten från de publiceringar i form av böcker, artiklar m.m. som följde efter fyndet.
- En TV-dokumentär om mysteriet vid Svarta sjön. Filmen uppmärksammades vid filmfestivalen i Leipzig i kategorin dokumentärfilm som ett exempel på extraordinär journalistik.

- Det tjeckoslovakiska utrikesministeriet som till USA, England, Frankrike och Holland överlämnande dokument rörande nazityska brott mot respektive lands medborgare under kriget, framför allt krigsfångar.
- Den tjeckoslovakiska vetenskapsakademin som delgav akademiska kretsar i utlandet material från Svarta sjön.
- Tjeckoslovakiska radion som sände program om den heroiska insatsen av västeuropeiska underjordiska motståndsrörelser mot Hitler (i synnerhet den franska).
- Den tjeckoslovakiska organisationen *The Union of Fighters Against Fascism* som blev kontaktorgan gentemot bl.a. *Center for Prosecution of War Crimes* och *Organization of Nazi victims* i Västtyskland.

Utöver personalen på avdelning D kände endast följande personer till *Operation Neptun*: den grupp officerare vid inrikesministeriet som deltog vid nedsänkandet av koffertarna i Svarta sjön, chefen för underrättelsetjänsten, inrikesministern (som bl.a. höll den första presskonferensen då fyndet presenterades) och president Novotny samt KGB vars kontaktman den tjeckoslovakiska underrättelsetjänsten var tvungen att informera.

Detta innebar att även tjeckoslovakiska myndigheter och allmänhet vilseleddes och utnyttjades som desinformationsspridare. För att öka säkerheten kring operationen spreds desinformation bland dem som skulle komma att bli inblandade i bekräftandet av fyndets trovärdighet. Från de tjeckoslovakiska residenturen i Berlin skickades krypterat en fiktiv rapport som bekräftade att en grupp tyska soldater våren 1945 hade kastat ett antal koffertar i Svarta sjön. Rapporten skickades ut med en bred sändlista så att ett stort antal medarbetare inom underrättelsetjänsten och inrikesministeriet skulle bli bekant med den.

En av de oförutsedda händelser som prövade deceptörernas skicklighet i att anpassa operationen till omständigheter utanför deras inflytelsesfär var reaktiverandet av den tjeckoslovakiska regeringens kommission för åtal av krigsförbrytare. Kommissionens medlemmar, som trodde att dokumenten verkligen kom från Svarta sjön, krävde i början av 1965 att kommissionen skulle tillhandahållas alla dokument innan de fick delges främmande makt, publiceras eller på annat sätt utnyttjas. Inrikesministeriet (avdelning D) ignorerade dock kommissionens begäran och fick vid flera tillfällen utstå protester för detta.

Trots den höga sekretessgraden fanns läckor. Personal inom den tjeckoslovakiska underrättelsetjänsten som inte hade behörighet att ta del av *Neptun* fick på okända vägar kännedom om operationen. Allvarligare var dock att rykten började cirkulera på den tjeckoslovakiska TV:n att den tjeckoslovakiska underrättelsetjänsten hade sänkt ner koffertarna i Svarta sjön. En av officerarna som hade deltagit vid sjön hade anförtrott sig till en god vän som arbetade på TV. Men trots dessa läckor och trots tvivel rörande dokumentens äkthet i vissa kretsar utomlands fick alltså operationen stor effekt.

När *Operation Neptun* summerades fanns den officiellt vara en stor framgång. Bittman och hans närmaste medarbetare nåddes av gratulationer från inrikesminister Strougal. Trots detta noterar Bittman i sin bok att alla mål inte uppnåddes med operationen. Avdelning D:s försök att hos den västeuropeiska allmänheten frammana en bild av 1960-

talets Västtyskland som en praktisk och ideologisk utväxt av Naziregimen misslyckades. När det gäller Västtysklands relationer med sina europeiska partner och allierade åstadkom *Operation Neptun* inte heller något som skulle kunna tolkas som en effekt av operationen. Några fler arkivgömmor hittades inte heller på tjeckoslovakiskt territorium. Och när det gäller det fjärde uppsatta målet – att lamslå den västtyska underrättelsetjänstens aktiviteter på tjeckoslovakiskt territorium blev resultatet en kvarstående osäkerhet. Prag kunde inte få bekräftat inifrån den västtyska underrättelsetjänsten huruvida *Operation Neptun* hade haft effekt. Den tjeckoslovakiska underrättelsetjänsten antog dock att den västtyska underrättelseaktiviteten hade avtagit. Denna slutsats drogs mot bakgrund av hypotesen att den tjeckoslovakiska underrättelsetjänsten skulle ha stoppat all underrättelseverksamhet, åtminstone temporärt, i fall man själv hade råkat ut för samma situation.

Som en finurlig knorr funderar Bittman över huruvida de dokument som de sovjetiska deceptörerna tillhandahöll verkligen var äkta. Även om den tjeckoslovakiska underrättelsetjänstens experter var övertygade om att de var äkta menar Bittman att det ändå finns en teoretisk möjlighet att dokumenten var förfalskade.

Operation Neptun skulle komma att få en efterföljare i *Operation Transfer* som syftade till att överbelasta den västtyska säkerhetstjänsten med improduktivt arbete. Denna operation skulle också komma att till viss del slå mot den västtyska underrättelsetjänsten.

4.3 Operation Transfer[77]

Strax efter andra världskrigets slut förflyttades tre miljoner tyskar från tjeckoslovakiskt territorium. Majoriteten av dessa bosatte sig i Västtyskland. Under 1950-talet följde så en andra tysk emigrationsvåg från Tjeckoslovakien. Denna gång var de tjeckoslovakiska myndigheterna dock mer restriktiva och nekade sådana sökande som var av vikt för landets ekonomi eller statssäkerheten utresa. 1965 deklarerade emellertid den tjeckoslovakiska regeringen att alla tyskar som ville skulle få lämna landet.

Tanken bakom *Operation Transfer* var att hos den västtyska säkerhetstjänsten skapa intrycket av att massimmigrationen också medförde en underrättelseoffensiv mot Västtyskland. Bland alla de tusentals ansökningar om emigration som inkommit till de tjeckoslovakiska myndigheterna sökte underrättelsetjänsten upp alla starkt antitjeckoslovakiska och antikommunistiska personer. Dessa ställdes inför ultimatumet att samarbeta med underrättelsetjänsten eller nekas utresa. I syfte att få lämna Tjeckoslovakien accepterade de flesta samarbetet. Tack vare dessa personers politiska inställning kunde underrättelsetjänsten vara ganska säker på att dessa personer omedelbart skulle avslöja sina kontakter med den tjeckoslovakiska underrättelsetjänsten för de västtyska immigrationsmyndigheterna och därför bli ett fall för den västtyska säkerhetstjänsten och möjligen även underrättelsetjänsten.

Flera hundra fiktiva agenter värvades. För att öka trovärdigheten i operationen gavs dessa fiktiva agenter utbildning i agentverksamhet. Bland annat gavs de fiktiva hemliga kommunikationsvägar för att de skulle kunna kontakta den tjeckoslovakiska underrättel-

[77] Avsnitt 4.3 bygger på sidorna 72-78 i Bittmans bok *The Deception Game*.

setjänsten. Dessa fiktiva agenter fick inte ha någon kontakt med officiella tjeckoslovakiska representationer i Västtyskland för att undvika att kompromettera riktig underrättelsepersonal verksam vid dessa.

Huvudsyftet med *Operation Transfer* var att sysselsätta den västtyska säkerhetstjänsten och rikta dess uppmärksamhet mot denna fiktiva underrättelseoffensiv och bort från den tjeckoslovakiska underrättelsetjänstens verkliga mål och verksamhet.

Samtidigt som *Operation Transfer* alltså var en vilseledningsoperation användes emigrationsflödet för att till Västtyskland infiltrera riktiga agenter. Deras chanser att undgå upptäckt bland tusentals immigranter ökade på detta sätt. Vid inresan kunde de antingen förneka att de blivit kontaktade av den tjeckoslovakiska underrättelsetjänsten före utresan eller avge ett simulerat vittnesmål om samarbete i syfte att vinna den västtyska säkerhetstjänstens förtroende och senare uppta den verkliga underrättelseverksamheten.

Operationen blev en verklig kvarnsten runt halsen på den västtyska säkerhetstjänsten som under trycket av den fiktiva underrättelseoffensiven också kände sig tvungen att undersöka samtliga immigranter (alltså inte bara de fiktiva agenterna). Risken fanns ju att de bland de övriga immigranterna fanns sådana som hade verkliga underrättelseuppdrag.

Säkerhetstjänstens rapporter om den tjeckoslovakiska underrättelseoffensiven i samband med immigrationen tvingade till slut den västtyska regeringen att ändra strafflagstiftningen 1968 så att alla som frivilligt erkände att de hade arbetat för främmande makt var garanterade immunitet. Lagändringen resulterade inte i någon nämnvärd ökning av antalet agenter som gav sig till känna. Därför vädjade inrikesminister Genscher i april 1970 offentligt till alla spioner att ge sig till känna i utbyte mot immunitet.

Operation Transfer var vältimad eftersom den sammanföll med en allmänt svår period för de västtyska underrättelse- och säkerhetstjänsterna. Efter att under perioden efter kriget ha firat många framgångar, inte minst genom den av den f.d. nazigeneralen Reinhard Gehlen ledda underrättelsetjänsten, blev 1960-talet en mörk period som präglades av sovjetiska och östtyska värvningar inom såväl den västtyska säkerhetstjänsten som underrättelsetjänsten vars trovärdighet sjönk. Därmed försämrades också det tidigare så goda ryktet. Många av de västtyska bakslagen blev offentligt kända genom att spioner avslöjades och greps. Det tjeckoslovakiska bidraget till det västtyska lidandet förblev dock okänt fram till Bittmans avhopp.

Bittman sammanfattar själv operationen på ett utomordentligt sätt. Han skriver

> *Operation Transfer was a success. It confused the West German counterintelligence service, keeping it busy with unproductive investigations and thus reducing its effectiveness. The operation was based on logical premises, the fundamental principles, and working methods valid for all counterintelligence services whether Communist or not. The West German counterintelligence service was forced to submit to the procedures imposed by the Czechoslovak service. Its only option was one which victimized it.*[78]

[78] Ladislav Bittman, *The Deception Game*, s. 77.

4.4 Operation Horisont[79]

This was a vast influence operation he [Ceausescu] was personally running to gain Western political support, money and technology.

Ion Pacepa[80]

1978 hoppade general Ion Pacepa av till USA. Hans täckbefattning var vice inrikesminister, men i själva verket var han chef för den rumänska underrättelsetjänsten. Dessutom var han Nicolae Ceausescus närmaste säkerhetspolitiska rådgivare.

Få avhopp har fått sådana konsekvenser som Pacepas. Den rumänska underrättelsetjänsten blev i det närmaste utraderad. Bland det som general Pacepa avslöjade fanns sanningen bakom Rumäniens förmenta bild som oavhängig frifräsare i östblocket.

1972 tog Nicolae Ceausescu personligen över den övergripande ledningen av den rumänska underrättelsetjänsten DIE. Ceausescus idé var att s.k. inflytelseoperationer var en effektivare metod att nå politiska mål och få inflytande i världspolitiken än traditionell underrättelseinhämtning. Med Ceausescu som övergripande chef för DIE blev dess huvudsakliga uppgift inflytelse- och vilseledningsoperationer. Underrättelseinhämtning kom i andra hand.

Vid ett tal inför DIE:s ledningsgrupp i februari 1972 presenterade Ceausescu sin idé, vilseledningsoperationen *Horisont*.

> *Our experience shows that today the West is commendably eager to encourage the slightest sign of independence within the Soviet bloc. Let's take advantage of their eagerness. ...We must make cleverness our national trait... Stop showing a sullen, frowning face and clenched fist to the West. Start making it feel compassion for us, and you'll see how fast Western boycotts change into magnanimity. Let's present Romania as a latin island in the Slavic sea... Our millenia-old traditions of independence are now up against Moscow's political centrism... A pawn between the two superpowers...*[81]

Dagen efter talet för underrättelsecheferna ökade Ceausescu DIE:s nominella personalstyrka från 700 till 2 800 underrättelseofficerare och åttafaldigade dess budget. Budgeten betalades ut i hårdvaluta som genererats genom bl.a. diamant-, vapen- och narkotikasmuggling samt betalning från Västtysklands och Israels regeringar för att tyskar respektive judar bosatta i Rumänien skulle få återvända till sina respektive hemländer.

Pacepa beskriver målande hur Ceausescu hade tänkt sig *Operation Horisont*:

> *The DIE should start an organized influence offensive against the West. It should carefully plant little hints of independence – without affecting the fundamentals of Communism – and then hammer away at them, in order to stir up the West's sympathy for Romainia and gain its political and economic assistance. The DIE's agents of influence should help Romania gain political and economic advantages*

[79] Ion Pacepa, *Red Horizons*, (Hodder and Stoughton, Sevenaoks, 1989).
[80] Ibid., s. 8.
[81] Ibid., s. 8.

> *in the West, turn Third World governments into political allies, transform hostile emigrés into supporters, sway the international news media. These agents should also use Romania's new prestige to unlock doors opening onto highly classified technology prohibited to Communist countries. Romania should make a substantial increase in its contribution to the defense not only of the Warsaw Pact but also of Peking and the whole Communist world.* [82]

Bilden av Rumänien som oavhängigt skulle förmedlas genom olika kanaler. Bland annat skulle DIE utnyttja

- öppen och svart propaganda,[83]
- antydningar i dolda mikrofoner upptäckta i rumänska ambassader i Väst; mikrofoner som inte tagits bort i syfte att kunna sprida vilseledande information,
- dokument "undertecknade" av främmande regeringar, förfalskade i Bukarest och avsiktligt förlorade på något lyxhotell eller på annat sätt läckta till Väst,
- underrättelseofficerare placerade i befattningar som ambassadörer och ärkebiskopar,
- unyttjande av schweiziska bankkonton för att betala högt uppsatta, korrupta västerlänningar som samtyckte till att presentera bilden av Rumänien som en frifräsare i östblocket,
- underrättelseofficerare förklädda till älskare[84] som rekryterade inflytelseagenter i Väst.

Operation Horisont hade flera konkreta mål. För det första att Rumänien skulle erhålla s.k. most-favored-nation-status i den amerikanska utrikeshandelspolitiken. En sådan status skulle tillåta rumänsk export till USA samtidigt som USA skulle kunna ge Rumänien vissa krediter. Rumänien skulle också förbättra sina möjligheter att få tillgång till amerikansk teknologi som annars var undanhållen Sovjetblocket. För det andra skulle Rumänien skapa liknande gynnsamma villkor visavi Västeuropa. Som framgår av citatet ovan skulle *Operation Horisont* öppna de första dörrarna till västvärldens inre ekonomiska och teknologiska rum för att sedermera bana väg för DIE att med traditionella underrättelsemetoder ta sig i det allra heligaste och stjäla framför allt militärindustriellt relaterade hemligheter, men även annan teknologi för t.ex. oljeborrutrustning och personbilstillverkning. För det tredje skulle denna teknologi sedan säljas dyrt till Moskva för att dra in pengar till den rumänska staten. Och för det fjärde skulle denna storslagna vilseledningsoperation i kombination med traditionellt spionage lägga grunden för ett rumänskt ekonomiskt oberoende.

När det gäller den sista punkten var det särskilt kärnkraftsteknologi, mikroelektronik och försvarsteknologi inkl. flyg- och rymdteknologi som låg Ceausescu varmt om hjärtat. Kärnkraften skulle lösa Rumäniens energiproblem och skapa en potential som kärnvapenstat. Mikroelektroniken var grunden till datorrevolutionen med dess inkomstbringande civila och militära applikationer. Och med hjälp av västerländsk försvars-

[82] Ibid., s. 8.
[83] Med svart propaganda menas propaganda vars avsändare falskeligen utger sig för att vara någon annan. Med grå propaganda avses att avsändaren är okänd och med vit propaganda avses slutligen propaganda vars avsändare uppträder öppet.
[84] Denna teknik har använts och används av många underrättelse- och säkerhetstjänster och går ofta under beteckning Romeo och Julia.

teknologi ville Ceausescu bygga upp en parallell försvarsindustri för egen högteknologisk export till framför allt tredje världen, dvs. vid sidan om den ordinarie försvarsindustrin som försörjde Rumänien och övriga Warszawapaktsländer.

Den sista punkten är intressant också eftersom den understryker att Ceausescu, samtidigt som han var en inbiten och cynisk kommunist, ville göra sig (åtminstone delvis) fri från Moskvas strama tyglar. Genom den relativt framgångsrika dupering av Väst blev *Operation Horisont* en plattform för att hävda sitt oberoende gentemot Sovjetunionen. Genom att kunna försörja Moskva med teknologi som Sovjetunionen annars inte skulle kunna komma över höll Ceausescu Kreml på gott humör och slapp även framgent sovjetiska trupper på sitt territorium (ett "privilegium" som de andra östblocksländerna inte slapp undan).[85] Moskva kände till och accepterade *Operation Horisont* och dess primära syfte att genom inflytande få tillgång till västerländsk teknologi m.m. som skulle kunna stärka det kommunistiska lägret. Det sekundära syftet att göra sig mer oberoende av "storebror" kan Moskva ha anat sig till.

Att Moskva inte litade på rumänerna framgår av det faktum att det sovjetiska spionaget mot Rumänien liksom mot övriga satellitstater fortsatte. Enligt uppgifter ur KGB:s arkiv opererade ett drygt tiotal sovjetiska illegalister i Rumänien. Deras uppgifter var bl.a. att inhämta information om Rumäniens relationer med USA och Kina, landets politiska och ekonomiska bas för en eventuell opposition mot Sovjetunionen, personkulten kring Ceausescu och tillståndet i det rumänska kommunistpartiet.[86] En av dessa illegalister var sannolikt vice inrikesminister general Eugen Luchian. Luchian var även den rumänske premiärministerns juridiske rådgivare. Kort tid före Pacepas avhopp hade den topphemliga del av säkerhetstjänsten Securitate som övervakade den rumänska nomenklaturan och som endast rapporterade till Ceausescu, inrikesministern och underrättelsetjänstens chef börjat fatta misstankar mot Luchian då man genom buggning av dennes hem uppfattat ett mycket kort fragment där Luchian talade ryska med sin fru. Luchian var den ende förutom Ceausescu och inrikesministern som kände till DIE:s hela organisation. Luchian och hans fru försvann spårlöst i samband med Pacepas avhopp.

Huruvida *Operation Horisont* var en framgångsrik vilseledningsoperation är svårt att uttala sig om utan tillgång till de bedömningar som gjordes i USA och Sovjetunionen. Och vem var det som vilseleddes? Var det kanske så att operationen sammanföll med den amerikanska strategin att slå in en kil i Sovjetblocket och att USA därför spelade med? Eller vilseleddes den sovjetiska ledningen som förvisso var informerad om Ceausescus strategi med inflytelseoperationer men som inte litade på den rumänske ledaren, som faktiskt tycks ha haft för avsikt att även gå bakom ryggen på Moskva och göra Rumänien mer självständigt inom Östblocket?

Oavsett svaret på ovanstående fråga kan man konstatera att *Operation Horisont* fick ett antal konkreta resultat. Grunden till operation lades egentligen redan tidigt under Ceausescus regeringstid, i slutet på 1960-talet. Bland de politiska framgångarna kan nämnas att Richard Nixon blev den förste amerikanske president som besökte det kommunistis-

[85] Den rumänske ledaren Gheorghiu-Dej lyckades tillsammans med sin sovjetiskutbildade försvarsminister Bodnaras förhandla fram ett tillbakadragande av de sovjetiska trupperna 1958.
[86] Vasili Mitrokhin och Christopher Andrew, *The Mitrokhin Archive—The KGB in Europe and the West*, (Penguin Press, 1999), s. 352-53.

ka Östeuropa. Besöket ägde rum 1969[87] och följdes av Ceausescu-besök i USA 1970, 1973, 1975 och 1978. Sedermera besökte även president Ford Bukarest. Och under sitt besök i USA 1978 blev Ceausescu den förste kommunistledare som satte sin fot på bl.a. Texas Instruments och NASA, vilket lär ha gjort ett stort intryck på Leonid Brezjnev.

Rumänien erhöll statusen som *most-favored-nation* och behöll den till och med efter Ion Pacepas avhopp. Däremot blev det aldrig några flera statsbesök i USA. *Most-favored-nation*-statusen möjliggjorde en export av kvalitetsmässigt undermåliga rumänska produkter inte bara till USA utan även till andra länder. Tvivelsutan behövde Rumänien mer än väl dessa inkomster som knappast hade kunnat genereras utan denna speciella handelstatus.

Genom kombinationen av inflytelseoperationer, handelsförhandlingar och underrättelseinhämtning lyckas DIE komma över bl.a. designen till den kanadensiska kärnkraftsreaktorn CANDU.[88] 1970 skapade Ceausescu den statliga kärnenergikommittén som fr.o.m.1972 lades under hans personliga kontroll och med Ion Pacepa som nationell koordinator. Rumänien skulle bli exportör av kärnkraftsverk, uran och tungt vatten till länder i tredje världen, länder som sannolikt inte ville bli beroende av amerikansk eller sovjetisk teknologi för sitt framtida energibehov och därmed industriella utveckling. Ceausescu spred även Rumäniens kärnteknologiska kunskaper till Pakistans kärnvapenprogram.[89]

Vidare hade *Operation Horisont* genererat Leopard-2-stridsvagnens fulla ritningar, ritningarna till Fokker FK-614, ett civilt flygplan med militära versioner för spaning, bomb och luftlandsättning samt Fokkers VTOL-konstruktion, en stor mängd brittisk, västtysk, fransk, amerikanskt krigsmateriel (inkl. t.ex. brittiska och franska stridsvagnar utsmugglade från Libanon med hjälp av PLO), Kodaks patent för fotografiskt papper och mycket, mycket annat.

Ceausescu startade eller avsåg att starta tillverkning av många av dessa produkter. Dessutom utnyttjade Ceausescu de stulna teknologierna för att bygga egna konstruktioner. Ett exempel var ett samriskprojekt tillsammans med Jugoslavien för att bygga stridsflygplanet YUROM.

En teknik som ofta användes i handelsförhandlingar var att till Bukarest inbjuda eventuella säljare av varor till Rumänien. Alla viktiga utlänningar inhystes på hotell *Athenee Palace*. Hotellet drevs av underrättelsetjänsten och all personal från direktören ner till städpersonalen var anställd av DIE. Under natten kunde gästerna låsa in sina viktiga handlingar i det välrenommerade hotellets kassaskåp. Förhandlingarna drogs sedan medvetet i långbänk (flera år) och de rumänska kraven på teknisk dokumentation öka-

[87] Besöket var ett tack för Ceausescus fördömande av Warsawapaktsinvasionen i Tjeckoslovakien 1968.
[88] Detta var en ny reaktortyp vars bränsle är naturligt uran, i stället för anrikat uran. Detta passade Rumänien mycket bra eftersom landet har egna urantillgångar.
[89] Ion Pacepa, *Red Horizons*, s. 300-301. Redan 1975 hade den rumänska underrättelsetjänsten indikationer på att Pakistan hade ett hemligt kärnvapenprogram. 1978 besökte Ceausescu Pakistans ledare Ali Bhutto och föreslog att de skulle dela med sig av sina nukleära hemligheter. Utbytet blev ingalunda enkelriktat. Bland annat fick Rumänien den kompletta dokumentationen över den kanadensiska reaktorn CANDU (se ovan) något de ännu inte hade. I gengäld fick pakistanierna bl.a. tillgång till franska kärnkraftssäkerhetssystem, något de hett eftertraktade vid denna tidpunkt.

des. Resultatet blev att efter en tid hade DIE kopierat det mesta av dokumenten varvid affärerna antingen kunde avbrytas eller de olika säljarnas offerter kunde spelas ut mot varandra för att sänka priset.

En finansiär, som också var invigd i de stora dragen av *Operation Horisont*, var Libyens ledare Khadaffi vars oljeinkomster skulle användads för att bygga tre oljeraffinaderier i Svarta havet. Tanken var att Rumänien skulle importera modern raffinaderiutrustning från Väst och processa libysk olja och exportera den som rumänsk. Detta skulle vara ett sätt att säkerställa att Libyen inte förlorade sina inkomster i händelse av västerländsk bojkott av libysk olja.

En annan person som var invigd i Ceausescus strategi om inflytelseoperationer var den palestinske ledaren Yasser Arafat. Enligt Pacepa tog Arafat till sig denna metod.[90] En del i *Operation Horisont* var att Ceausescu skulle försöka ta rollen som fredsmäklare i Mellanöstern (från president Carter). Idén var att Arafat genom att gå med på att inta en mjukare linje i förhållande till Israel skulle bli erkänd i Väst. Ceausescus dröm var att ett erkännande av PLO och efterföljande fredsförhandlingar skulle kunna ge honom Nobels fredspris. Även om Ceausescu aldrig fick priset blev planen en framgång. I juli 1979 mottogs Arafat i Wien av Österrikes kansler Bruno Kreisky och Willy Brandt. Detta var första gången en PLO-representant besökte ett västeuropeisk land och sågs som att Österrikes regering och den socialistiska internationalen nu erkände PLO. Noterbart i detta sammanhang är att även de svenska socialdemokraterna haft ett gott förhållande till PLO.[91]

4.5 Programmet Enzym – Det sovjetiska B-vapenprogrammet

Döljandet av det sovjetiska B-vapenprogrammet är ett utomordentlig exempel på kapacitetsdöljande vilseledning som t.o.m. överträffar den maskirovka/ vilseledning som traditionellt omgett det sovjetiska kärnvapenprogrammet (se vidare del 2, avsnitt 3.4).

1969 avsade sig USA ensidigt sina biologiska vapen eftersom den amerikanska debatten kommit fram till att dessa vapen var av ringa strategiskt värde. Sovjetunionen sade sig också göra detsamma. Enligt den tjeckoslovakiske avhoppade deceptören Ladislav Bittman (se avsnittet om *Operation Neptun*) påverkades det amerikanska beslutet av en sovjetisk desinformationskampanj som sökte övertyga Washington om att om USA fortsatte uppbyggnaden av sin biologiska och kemiska arsenal (särskilt nervgas) skulle

[90] Detta framgår av hans memoarbok *Red Horizons* (s. 30-34), där ett exempel på att även PLO ägnat sig åt vilseledning ges. 1974 bröt sig Abu Nidal ur PLO och fick bl.a. stöd från Irak och Östtyskland. Detta var en nagel i ögat på PLO och försvårade deras egen verksamhet. I en sinnrik vilseledningsoperation, som bl.a. omfattade mordet på den egna PLO-representanten i London(!), lyckades emellertid Arafat infiltrera Abu Nidals organisation så att dessa kom att inneha samtliga topposter och därigenom i realiteten ta över hans organisation *Svarta juni*.

[91] Att planen var framgångsrik kan naturligtvis bestridas genom att hävda att den i tiden råkade sammanfalla med ett skeende där västeuropeiska politiker av helt andra skäl hade kommit till slutsatsen att det nu var dags att erkänna PLO som ett steg i riktning mot fred i Mellanöstern. Å andra sidan kan man då hävda att Ceausescu och Arafat genom underrättelseinhämtning skulle ha kunnat veta att detta var den kommande västeuropeiska politiken och att de därför spelade med eftersom det passade deras syften, medan de samtidigt hade andra, dolda avsikter i ett längre perspektiv.

Moskva starta ett omfattande program för att matcha den amerikanska förmågan.[92] Ett sovjetiskt offensivt biologiskt program fanns då sedan lång tid och Sovjetunionen besatt vid denna tid stora arsenaler av såväl biologiska som kemiska agens.

1972 undertecknade Sovjetunionen och 118 andra stater konventionen mot biologiska vapen som förbjuder utveckling, produktion, lagring och anskaffning av biologiska agens i mängder avsedda för vapenbruk. Små kvantititer för laboratoriebruk tillåts dock enligt B-vapenkonventionen.

I hemlighet tog det sovjetiska B-vapenprogammet ånyo fart 1973, främst för att att inkorporera genetikens landvinningar. Sovjetunionen byggde upp ett stort strategiskt-tekniskt övertag inom detta område. Genom två avhoppare 1989 (Pasechnik) och 1992 (Alibekov, som senare tagit namnet Alibek) fick Väst kännedom om hur det verkligen låg till. Sedermera har även en pensionerad, rysk forskare (Domaradskij) talat om programmet. Så sent som 1990 tilldelades den sovjetiska B-vapenforskningen en miljard USD.[93]

Under tiden har Ryssland skrivit under B-vapenkonventionen. Officiellt lades det offensiva programmet ner 1992 och idag sägs endast skyddsforskning avseende biologiska stridsmedel bedrivas. Det finns dock tecken som tyder på att verksamheten fortfarande pågår.

Genom extremt hög grad av sekretess och sektionering av den hemliga informationen har Sovjetunionen/Ryssland lyckats dölja det sanna och framhäva det falska. Officiellt förnekade Sovjetunionen och förnekar Ryssland att landet har biologiska vapen.

Historisk bakgrund[94]

1928 ratificerade Sovjetunionen Genèveprotokollet från 1925 som förbjuder användning av B- och C-vapen. Samma år påbörjade den unga Sovjetstaten utvecklingen av biologiska vapen (tyfus[95]). 1938 lät den sovjetiska regeringen för första gången gången förstå att landet förfogade över en biologisk krigföringsförmåga. Då deklarerade marskalk Vorosjilov att Sovjetunionen avsåg att upprätthålla Genèveprotokollet, men tillade att man var beredd att använda sådana vapen mot en angripare på dennes territorium om en angripare skulle använda biologiska vapen mot Sovjetunionen.[96]

Intressant nog lät Sovjetunionen femtio år senare världen ånyo förstå att landet besatt en god B-vapenförmåga – denna gång i form av genmodifierade biologiska vapen. Den som framförde budskapet 1988 var Valentin Falin, sekreterare i kommunistpartiets centralkommitté och chef för dess internationalla avdelning, den avdelning som bl.a. hade ansvar för s.k. aktiva åtgärder (se avsnitt 3.5).[97, 98]

---

[92] Ladislav Bittman, *The KGB and Soviet Disinformation*, s. 136.
[93] Ken Alibek med Stephen Handelman, *Biohazard*, (Hutchinson, London, 1999) s. 43.
[94] Den historiska bakgrunden är med någon enstaka förändring tagen från avsnitt 3.1.1 i Jenny Clevström, Lena Norlander och Wilhelm Unge, *Rysk toxin- och bioregulatorkompetens*.
[95] Under det Röd-vita inbördeskriget 1918-21 härjade en svår tyfusepidemi. Sjukdomen skördade många fler offer än kulor och granater och Röda Arméns ledning insåg att sjukdomen var ett potent vapen.
[96] Ken Alibek, *Biohazard*, s. 34.
[97] Kommunikation med Roger Roffey, FOI NBC-skydd 2001.

Fram till 1942 ingick biologiska vapen i Sovjetstatens taktiska arsenal, dvs. som ett medel för att inkapacitera motståndarens trupp. Efter en misslyckad insats av B-vapen där man smittade den egna truppen under slaget vid Stalingrad bestämdes att denna typ av vapen endast skulle ha en operativ-strategisk användning.

Under andra världskrigets slutskede kom Röda Armén över delar av det japanska B-programmet i Manchuriet. 1946 påbörjades byggandet av ett B-komplex i Sverdlovsk enligt japanskt mönster. Det nya var B-vapenframställningens industriella skala, inkl. FoU.

Under Stalinepoken paralyserades den biologiska forskningen av utrensningar i kombination med agronomen Lysenkos irrläror. Som ett resultat blev genetisk forskning bannlyst. Men en rad briljanta upptäckter i Väst under 1950-, 60- och 70-talen, varav den sedermera nobelprisbelönade upptäckten av DNA 1953 var den viktigaste, tvingade de sovjetiska forskarna att inse att de låg efter i utvecklingen. En man hade till sist modet att gå emot Lysenkos ideologiskt korrekta lära: Jurij Ovtjinnikov, framstående molekylärbiolog och vice ordförande i den Sovjetiska Vetenskapsakademin. Han förstod den revolutionerande innebörden av gentekniken. Han lyckades övertyga miltärledningen och Leonid Brezjnev om vikten av nya satsningar inom bioteknikområdet.[99]

I ett försök att komma ikapp Väst beordrade Brezjnev 1973 en stor satsning inom bioteknik och genteknik. Dessa satsningar fokuserades emellertid till den militära applikationen av de nya teknologierna; teknologier som inte kom det civila samhället till godo. Satsningarna omfattade en modernisering av existerande och utveckling av nya B-vapen samt av genetiskt förändrade B-stridsmedel resistenta mot antibiotika och som kunde överkomma vaccinationsskydd. Detta beslut togs alltså samtidigt som Sovjet ratificerade B- och toxinvapenkonventionen 1972.

Det hemliga programmet fick namnet *Enzym*. Navet i verksamheten var det statliga farmaceutiska företaget *Biopreparat* med många anläggningar som utvecklade nya B-stridsmedel och förfinade produktionsmetoder. I detta program ingick utveckling av B-vapen (artilleri, flygbomber och robotar) för storskalig användning mot strategiska mål. Ungefär 50 anläggningar och 60 000-70 000 personer var involverade i B-vapenprogrammet i mitten av 1980-talet. B-stridsmedel producerades i industriell skala (hundratals ton) bl.a. antrax- och pestbakterier samt smittkoppsvirus avsett för laddning av bl.a. interkontinentala robotar. Ett stort antal olika B-stridsmedel standardiserades för vapenändamål. Förutom försvarsministeriets och Biopreparats anläggningar fanns anläggningar inom hälsovårdsministeriet och jordbruksdepartementet för utveckling av B-stridsmedel mot boskap och grödor.[100]

Syftet med den offensiva biologiska forskningen var, som nämnts ovan, att kunna framställa förbättrade och nya stridsmedel i form av bakterier, virus och toxiner för användning i strategiska vapen. Men även KGB var intresserade av att ta del av de stridsmedel som utvecklades, framför allt av toxiska ämnen. Inom programmen *Flute* och *Bonfire*

[98] Vadim Bakatin, *Att bli kvitt KGB*, (Förlags AB Wiken, Falun, 1993), s. 72-73.
[99] Ken Alibek, *Biohazard*, s. 39-41.
[100] Kommunikation med Roger Roffey, FOI NBC-skydd, 2001.

utvecklades toxiner och andra toxiska substanser för att användas mot bl.a. "individual human targets".[101]

I det ryska arbetet utnyttjades inte bara den kunskap som fanns inom de offensiva instituten utan även framsteg som gjordes inom civila forskningsinstitut. All forskning vid dessa institut samordnades – organisatoriskt och finansiellt – av den ryska vetenskapsakademin. *Interdepartementala rådet för teknik och vetenskap* (bildat 1970) verkade som en vetenskaplig och industriell rådgivande instans till det offensiva programmet. I detta råd ingick bl.a. chefer för de ledande civila forskningsinstituten vilket innebar att forskningsframsteg inom instituten direkt kunde överföras till den offensiva verksamheten.

4.6 Sovjetisk militärindustriell kapacitet inför andra världskriget

> *Many years ago I came to the conclusion that it is futile and a waste of time to try to find an exact or even relative share of the Soviet defense burden in terms of GNP, national budget and so forth. (---) From my point of view, the Soviet economy was militarized by 100 per cent. But it can't be proved by budgetary calculations.*
> Dr. Vitalij Sjlykov[102]

Under det kalla kriget pågick i Väst en intensiv debatt om hur stora de sovjetiska ekonomiska försvarsansträngningar var. Sovjetunionen själv hävdade att de uppgick till 2 procent av BNP. Amerikanska CIA hävdade fram till 1976 att de utgjorde 6 procent och efter 1976 att de uppgick till 12 procent av BNP. NATO beräknade dem till 13-16 procent av BNP. Senare har siffrorna reviderats till ca 25 procent. Även högre uppskattningar har förekommit. Samtliga dessa uppskattningar bygger på antagandet att den sovjetiska ekonomin kunde jämföras med marknadsekonomier.[103]

Senare tids forskning har emellertid visat att den sovjetiska ekonomin uppvisade en alldeles egen särpräglad strukturell militarisering och ett system för militärindustriell mobilisering vars tre huvudsakliga karaktäristiska drag var följande:

---

[101] Belagda fall av användning av toxin som stridsmedel finns. Den bulgariske avhopparen Markov mördades 1978 i London genom att en mycket liten kula fylld med toxinet ricin sköts in i hans ben från ett paraply. Den bulgariska underrättelsetjänsten låg bakom attentatet. KGB-chefen Andropov var mycket noga med att hans organisation inte skulle kunna förknippas med dådet varför han inte ville ha något aktivt deltagande i själva utförandet. Däremot tillät han att materiell assistans i form av amerikanskt paraply (för att dölja KGB:s inblandning), kula och toxin lämnades av KGB. Paraplyspetsen byggdes om till en ljuddämpad avfyrningsmekanism av KGB:s avdelning för operativ teknik OTU. Uppgifter om mordet har tidigare lämnats av olika avhoppare, men först genom Vasilij Mitrochin som under 20 års tid kopierade akter i KGB:s första huvuddirektorats arkiv och sedermera exfiltrerades från Ryssland 1992 av den engelska underrättelsetjänsten, har uppgifterna kunnat beläggas. *The Mitrokhin Archive—The KGB in Europe and the West*, Vasili Mitrokhin och Christopher Andrew, s. 506-508.

[102] Vitalij Sjlykov, *The Real Defense Burden in Russia*, paper förberett för FOA-konferensen "Russian Military Prospects" i Stockholm 12-13 mars 1998, s. 8.

[103] Se t.ex. Wilhelm Unge, *The Russian Military-Industrial Complex in the 1990s – Conversion and Privatisation in a Structurally Militarised Economy*, FOA-R—00-01702-170—SE, december 2000, s. 21-23 och Carl G. Jacobsen (ed.), *The Soviet Defence Enigma: Estimating Costs and Burden*, (SIPRI, Stockholm, 1987).

- För det första var det fredstida militärindustriella komplexet (MIK) tvunget att ha en sådan storlek att det skulle kunna ställas om till krigstida produktion med fastställda produktionsvolymer. Detta innebar en omfattande fredstida produktion för att hålla produktionsbasen "varm". Detta var i sin tur en av anledningarna till den stora sovjetiska krigsmaterielparken och den omfattande exporten. Mobiliseringskraven förklarar också filosofin bakom att ersätta utsliten materiel med ny i stället för att underhålla den.

- För det andra innehöll MIK både en civil och en militär del. De civila företagen inom MIK tjänade två syften. Dels var de en omedelbart gripbar resurs avseende arbetskraft, maskinutrustning och produktionslokaler för att påskynda mobiliseringen. Dels finansierade inkomsterna från de civila företagen den militära produktionen och bidrog till att hålla priserna på en artificiellt låg nivå.

- För det tredje var företagen tvungna att upprätthålla en oavbruten produktion som vida översteg de fredstida behoven. I synnerhet gällde detta mineral-, bränsle- och energisektorerna.[104]

Detta innebar dock inte med nödvändighet att alla fysiska resurser gick till MIK, utan att MIK hade första tjing på allt och de kvalitativt bästa resurserna gick dit. Den lågkvalitativa resterande delen gick till det civila samhällets behov eller slängdes på skrothögen. Och det var i själva verket här som det abnorma slöseriet ägde rum vilket till slut ledde till Sovjetunionens undergång.

En viktig del av den sentida forskningen kring MIK är historiska studier av hur det sovjetiska militärekonomiska systemets byggdes upp och hur dess funktionsmekanismer utformades. Här bör särskilt doktor Lennart Samuelsons arbete uppmärksammas. Genom arkivstudier har han kunnat studera MIK:s födelse och utveckling fram till 1941.[105]

En mycket viktig del av det militärindustriella mobiliseringssystemet var den höga graden av sekretess. Formellt såg inte den sovjetiska industrin ut att vara så militariserad som den i själva verket var. De flesta civila fabriker hade omfattande produktionsvolymer av krigsmateriel som mål i händelse av krig. Den enorma produktionsförmågan avseende krigsmateriel doldes till stor del bakom de socialistiska satsningarna på tung industri och utvinning av naturtillgångar. Endast ett mycket litet fåtal sovjetmedborgare hade överblick över och insikt i detta system.

Enligt Lennart Samuelson hade inte alla länder i omvärlden inför andra världskriget klart för sig vilken krigstida produktionsförmåga Sovjetunionen i själva verket besatt. Genom tysk vilseledning blev förvisso Stalin överraskad av det tyska anfallet i juni 1941, men den sedermera mycket berömda omflyttningen av stora delar av industrin till öster om Ural på mindre än ett år vittnar tydligt om den mobiliseringskapacitet som fanns. Omställningen till krigsproduktion och även geografisk förflyttning var väl övade

[104] Wilhelm Unge, *The Russian Military-Industrial Complex in the 1990s*, s. 23-29.
[105] Lennart Samuelson, *Röd koloss på larvfötter – Rysslands ekonomi i skuggan av 1900-talskrigen*, (SNS förlag, Stockholm, 1999) och Lennart Samuelson, *Plans for Stalin's War Machine: Tukhachevskii and Military-Economic Planning, 1925-1941* (London, Macmillan, 1999).

innan kriget. Det sovjetiska systemet, som baserades på teorierna om det framtida totala kriget där personell och materiell (industriell) numerär till slut fäller avgörandet, visade sig vara framgångsrikt. Hitler kunde inte i längden hålla jämna steg i krigsmaterielproduktionen.

Vad visste då omvärldens underrättelsetjänster om den sovjetiska militärindustriella förmågan? Lennart Samuelson skriver så här:

> *Den officiella statistiken för 1937, 1938 och 1939 pekade på sjunkande tillväxttakt inom industrin som helhet. Därför var försvarsindustrins utbyggnad och expansionsplaner i händelse av krig svår att förutse. Rapporter från de tyska militärattachéerna i Moskva underskattade hur väl planlagd den sovjetiska industriella mobiliseringen var. Den sovjetiska krigsmakten hade anammat metoder ur den hemliga industriella mobiliseringen som Tyskland genomförde trots Versaillesfördraget. När samarbetet mellan Röda armén och Reichswehr pågick lärde sovjetiska officerare och administratörer på kurser i Berlin hur industriell beredskap kunde organiseras. Den sovjetiska förvaltningen hade sedan bl.a. infört standardisering för att kunna skifta från civil till militär produktion och avsatt verkstadsutrymme för testproduktion. Detta maskerades dock noggrant. Tyska bedömare rapporterade i slutet av 1930-talet att den sovjetiska industrin arbetade på 70-80 procent av sin fulla kapacitet. De tyska observatörerna förbisåg att krigsproduktionen efter en industriell mobilisering skulle kunna flerdubblas genom att civila industrier hade förberetts för vapenproduktion i händelse av krig. Detta skulle visa sig vara ödesdigra felbedömningar. Först efter ett par års krig började den tyska underrättelsetjänsten få en mer verklighetsförankrad uppfattning om den sovjetiska industrins faktiska potential.*
>
> *Det är en annan historiens ironi att det var först när man från sovjetisk sida genom sin underrättelsetjänst i början av 1941 förstod att den tyska generalstaben förberedde ett anfall mot Sovjetunionen som man började lätta på den totala sekretess som omgärdade krigsindustrin. Tyska experter på besök inbjöds att besöka flygplansfabriker utanför Moskva där man öppet pekade på vilka produktionsmöjligheter som fanns. De tyska experterna förstod snabbt vad vissa nyckeltal betydde och rapporterade till Berlin om felkalkyler i de tidigare tyska underrättelserna. Men deras rapporter kom för sent eller blev misstrodda; inga ändringar i den tyska anfallsplanen gjordes.*[106]

På samma sätt som Tyskland före och under andra världskriget fick erfara vilken effekt den sovjetiska kapacitetsdöljande vilseledningen hade, kämpade Väst under det kalla kriget med att försöka se igenom dimman. Denna dimma som var medvetet skapad i syfte att dölja Sovjetunionens verkliga militärindustriella kapacitet. De döljande åtgärderna omfattade allt från manipulering av ekonomisk-industriell statistik, döljande av militärrelaterade utgifter under andra poster i statsbudgeten till fysiskt döljande av krigstida produktionsanläggningar och teknologier. Som framgår av västvärldens föga framgångsrika ansträngningar att få grepp om de sovjetiska försvars- och försvarsindustriella ansträngningarna (se första stycket i detta avsnitt) var denna vilseledning mycket framgångsrik.

[106] Lennart Samuelson, *Röd koloss på larvfötter*, s. 239-240.

Sammanfattningsvis kan alltså konstateras att den sovjetiska militärindustriella vilseledningen haft både en kapacitetsdöljande och en kapacitetsframhävande karaktär. Före andra världskriget underskattade väst Sovjetunionens militärindustriella kapacitet och efter detsamma överskattade man systemets styrka och uthållighet. Dessa två felbedömningar utgör hörnstenarna Lennart Samuelsons analys av Sovjetunionens ekonomiska historia. Jfr vidare del 2 om Tysklands hemliga upprustning under mellankrigstiden.

4.7 Mitrochins arkiv

KGB-officeren Vasilij Mitrochin hoppade av mentalt redan på 1960-talet, men stannade kvar i organisationen. Under 20 års tid kopierade han akter i KGB:s första huvuddirekatorats arkiv.[107] 1992 exfiltrerades han från Ryssland av den engelska underrättelsetjänsten. Tillsammans med professor Christopher Andrew har han sedermera skrivit boken *The Mitrokhin Archive – The KGB in Europe and the West.* Boken är en rik källa vad gäller sovjetiska aktiva åtgärder, desinformation och vilseledningsoperationer. Vi nämner endast ett intressant fall här: Polenkrisen 1980-81.

Fallet är mycket instruktivt eftersom militära maktmedel fanns att genomföra en sovjetiskledd intervention. Vilka intentioner Moskva verkligen hade var den stora osäkerhetsfaktorn. Vi har nedan valt att betrakta Polenkrisen ur ett vilseledningsperspektiv, även om krisen lika gärna kan sägas utgöra ett klassiskt exempel på hot. Denna typ av situation är kanske den allra besvärligaste ur ett skyddsperspektiv.

4.7.1 Operation X – Framtvingandet av undantagstillstånd i Polen 1981

> *As early as 1980 the Soviet Politburo had been forced into the reluctant recognition that the only effective defence against a Polish counter-revolution was the fear of Soviet military intervention. That fear, however, was a dwindling asset based on memories of Budapest in 1956, Prague in 1968 and Kabul in 1979. Once the Politburo secretly turned against the idea of invading Warsaw in 1980, its policy was based on a bluff which could not be sustained indefinitely.*
>
> Vasilij Mitrochin och Christopher Andrew [108]

Mycket har sagts och skrivits om Polenkrisen 1980-81. Det flesta bedömare menar att Sovjetunionen och ett antal Warszawapaktsländer var beredda att invadera Polen för att stoppa ett maktövertagande av Soldaritet. Totalt fanns 18 stridsberedda divisioner runt Polens gränser i slutet av 1980.[109] Ett år senare bedömde den svenska underrättelsetjänsten att 30-35 divisioner skulle kunna påbörja inmarsch inom 24 timmar.[110]

---

[107] Den del av KGB som bedrev utrikesunderrättelsetjänst.
[108] Vasili Mitrokhin och Christopher Andrew,*The Mitrokhin Archive*, s. 704-705.
[109] Ibid., s. 676.
[110] En sammanfattande bild av det läge den svenska underrättelsetjänsten hade återfinns i Boris Ljunggren, *Militärt relaterade tidiga indikatorer på en utveckling i Ryssland som kan bli ett hot i närområdet och mot Sverige*, outgiven FOA-rapport, hösten 1997, s. 15-18. Här framgår också med all tydlighet svå-

Vid ett extraordinärt möte med Warszawapaktsländernas ledare i Moskva den 5 december 1980 visades den nytillsatte generalsekreteraren i det polska kommunistpartiet Stanislaw Kania invasionplanerna. Kania blev också vittne till hur talare efter talare talade om den polska regeringens handfallanhet och krävde att den omedelbart skulle slå ner på Soldaritet och den katolska kyrkan. Efter mötet följde en diskussion på tu man hand mellan Kania och Brezjnev. Kania framhöll att en intervention skulle innebära en katastrof för både Sovjetunionen och Polen. Enligt Mitrochin lär Brezjnev ha svarat att

> *OK, we don't march into Poland now, but if the situation gets any worse we will come.*[111]

Mitrochin och Andrew kommenterar hotet så här:

> *Brezhnev's threat was propably a bluff. With Soviet forces already at war in Afghanistan and the propability that military intervention in Poland would result in a blood bath, Western economic sanctions and a global public relations disaster, the Kremlin's strategy was to pressure the Poles into using martial law to end Solidarity's challange to the Communist one-party state. Ultimately the most effective way of exercising pressure was to threaten invasion by the Red Army. Memories of Hungary in 1956, Czechoslovakia in 1968 and Afghanistan in 1979 meant that very few in either Poland or the West failed to take the threat seriously in 1980.* [112]

Den sovjetiska politbyrån ansåg att ett dylikt hot var den främsta återhållande faktorn på de anti-socialistiska krafterna i Polen. Av avhemligade dokument från den sovjetiska politbyrån framgår att

> *The Politburo agreed, 'as a deterrent to counter-revolution', to 'exploit to the utmost the fears of internal reactionaries and international imperialism that the Soviet Union might send its troops into Poland'. It also decided to maintain 'support for Comrades Kania and Jaruzelski, who despite their well-known waffling, are in favour of defending Socialism'. They must, however, be put under 'costant' pressure to pursue more significant and decisive actions to overcome the crisis and preserve Poland as a Socialist country friendly to the Soviet Union'.*[113]

I mitten av 1980 tillsattes den s.k. Suslov-kommissionen av den sovjetiska politbyrån för att bevaka Polenkrisen. Suslov-kommissionen rekommenderade att hotet om militär intervention från andra Warszawapaktsländer hela tiden måste finnas i sinnet hos alla polska politiska krafter.[114]

Att generalsekreteraren Kania och försvarsminister Jaruzelski (fr.o.m. februari 1981 tillika premiärminister) famlade i mörkret och befann sig i en mycket svår situation

---

righeten att rätt tolka varningssignaler, göra riktiga bedömningar och fatta rationella beslut mot bakgrund av ofullständig, motsägelsefull och oriktig information samt desinformation.

[111] Ibid., s. 676.

[112] Ibid.s. 676-677.

[113] Mark Kramer (ed.), "Declassified Soviet Documents on the Polish Crisis", *Cold War International History Project Bulletin*, no 5, 1995, s. 130-131, citerat i Vasili Mitrokhin och Christopher Andrew,*The Mitrokhin Archive*, s. 680.

[114] Vasili Mitrokhin och Christopher Andrew,*The Mitrokhin Archive*, s. 682.

framgår av Mitrochins arkiv. Enligt dokument från KGB:s arkiv (en polsk politbyråmedlem informerade KGB) skall Kania ha sagt att

In spite of the pressure from Moscow, I don't want to use force against the opposition. I don't want to go down in history as the butcher of the Polish people. [---] and I'll never ask the Russians for military assistance.[115]

Enligt samme informatör skall Kania hade tagit invasionshotet på största allvar.[116] För att ytterligare späda på Jaruzelskis beslutsvånda avbröt de sovjetiska representanterna under sommaren 1981 de dagliga kontakterna. Detta gällde t.ex. den hetlevrade marskalk Viktor Kulikov, chefen för Warszawapaktens samlade styrkor, som tidigare levererat förolämpande omdömen vilka Jaruzelski tvingats svälja. Både Kania och Jaruzelski lär ha insett att sovjetiska intriger pågick emot dem vilket ytterligare försvårade vändan.

Vad som också talar för versionen att något verkligt invasionshot aldrig förelåg är det faktum Moskva inte utnyttjade erbjudandet från nio polska generaler att genomföra en militärkupp. Generalerna, som vände sig till KGB, föreslog att de skulle avlägsna Jaruzelski och ersätta honom med en ny försvarsminster, arrestera resten av regeringen, besätta strategiskt viktiga punkter och gripa 3 000 kontrarevolutionärer. En aktionsgrupp ledd av den nye försvarsministern och inte innehållandes någon medlem från den tidigare regeringen eller politbyrån skulle sedan vända sig till Warszawapakten med förfrågan om militär hjälp för att bevara socialismen i Folkrepubliken Polen.[117]

Efter ett års vånda gav dock Jaruzelski vika för sovjetiska påtryckningar och den 5 december 1981 fattade den polska politbyrån enhälligt beslut att införa undantagstillstånd. Natten mellan de 8 och 9 december informerade Jaruzelski marskalk Kulikov, som noterade att även om planen verkade resolut var Jaruzelski inte det. Den 9 december beklagade Jaruzelski sig inför bl.a. inrikesminister Milewski, som var Kremltrogen och rapporterade direkt till Moskva, att han kände sig sviken av Moskva.

> *They pressured us to take firm and decisive action, and the Soviet leaders promised to provide all the assistance and support needed. But now, when we have made a firm decision to take action and we would like to discuss it with the Soviet leaders, we cannot get a concrete answer from the Soviet comrades.*[118]

Att Jaruzelski tolkade signalerna rätt framgår av anteckningarna från den sovjetiska politbyråns möte den 10 december 1981. KGB-chefen Andropov (sedermera Leonid Brezjnevs arvtagare som sovjetledare) skall där ha sagt att

> *If Comrade Kulikov actually did speak about the introduction of troops, then I believe he did this incorrectly. We can't risk such a step. We don't intend to introduce troops into Poland. That is the proper position, and we must adhere to it until the end. I don't know how things will turn out in Poland, but even if Poland falls under the control of Solidarity, that's the way it will be.*[119]

[115] Ibid., s. 678.
[116] Ibid., s. 679.
[117] Ibid., s. 682.
[118] Ibid., s. 690.
[119] Ibid., s. 690.

Lördagen den 12 december 1981 ringde Jaruzelski till Brezjnev och fick dennes tillstånd att påbörja *Operation X* (införandet av undantagstillstånd).[120] Resultatet av den sovjetiska vilseledningen blev en framgång för Moskva. Enbart hotet om sovjetisk invasion var lika effektivt för att krossa oppositionen som den militära interventionen hade varit 13 år tidigare i Tjeckoslovakien.[121] Antal döda och skadade blev dock mycket lägre än både den polska och sovjetiska underrättelsetjänsterna hade räknat med.[122]

Huruvida detta är den riktiga tolkningen av Polenkrisens utveckling återstår sannolikt att se. Historieskrivningen fortsätter i frågan. Under 2001 har bl.a. *US Intelligence and the Polish Crisis 1980-1981* skriven av en f.d. chef för CIA:s Directorate for Intelligence och baserad på avhemligade dokument givits ut.[123] Boken behandlar bl.a. överste Ryszard Kuklinskis roll. Kuklinski arbetade i den polska generalstaben. Han var agent för CIA från 1972 till november 1981 då han lyckades fly från Polen. Kuklinksi ingick i en liten grupp som utarbetade planerna för ett överraskande införande av undantagstillstånd. På grundval av den information han försåg CIA med kontaktade president Carter sovjetledaren Brezjnev och varnade för konsekvenserna av en Warszawapaktintervention i Polen.

4.8 Några dagsaktuella exempel

I kapitel 5 i rapportens andra del diskuteras kortfattat ett antal dagsaktuella fall av misstänkt karaktär. Det är inte vår avsikt att där djupare analysera eventuella pågående fall av vilseledning och desinformation. Syftet är endast att peka på några aktuella fall där man kan urskilja olika aktörer med speciella särintressen som skulle kunna tänkas ligga bakom händelseutvecklingen.

[120] Ibid., s. 691.
[121] Ett intressant material för att jämföra denna beskrivning av Polenkrisen med sovjetisk vilseledning i samband med invasionen i Tjeckoslovakien 1968 hittas på CIA:s hemsida, Center for the Study of Intelligence, http://www.odci.gov./csi/studies/fall00/ch5_Soviet_Deception.pdf, hämtad 9 augusti 2001.
[122] Vasili Mitrokhin och Christopher Andrew,*The Mitrokhin Archive*, s. 694.
[123] Douglas MacEachin, *US Intelligence and the Polish Crisis 1980-1981*, Internet, http://www.odci.gov./csi/books/poland/index.htm, hämtad den 9 augusti 2001.

5. Vilseledningens teori, principer och metoder

Innan vi övergår till att diskutera möjligheterna att skydda sig mot vilseledning är det av vikt att på ett mer teoretiskt förankrat sätt än i avsnitt 3.3 beskriva vilseledningens anatomi. Detta kapitel beskriver därför hur vilseledning fungerar och vilka grundläggande mekanismer, principer och metoder deceptören kan utnyttja. Kapitlet är, med vissa förändringar, hämtat från arméns *Vilseledningsstudie 1995-97* som behandlar militär vilseledning på taktisk nivå.[124] Emellertid är principerna och metoderna tänkta att kunna tillämpas oberoende av nivå (strategisk, operativ eller taktisk).

Med teori i samband med vilseledning menas här *dels* principer för hur vilseledning kan förstås och tillämpas utgående från mänskliga psykologiska mekanismer, *dels* principer och riktlinjer för vilseledningens genomförande. Avslutningsvis berörs även de risker som finns vid genomförandet av vilseledningsoperationer.

5.1 Vilseledningens mekanismer

Följande psykologiska principer för hur människan arrangerar och behandlar inkommande information har betydelse för anpassningen till en komplex och informationsrik tillvaro.

Inkommande information till våra sinnen bearbetas i en aktiv process, som kallas varseblivning. Denna process pågår från det enskilda sinnet i steg till hjärnan. Det betyder att vad vi ser, hör, känner eller luktar inte är något objektivt återgivande av entydiga fysikaliska eller kemiska data genom kroppens mätinstrument, utan det är filtrerad och bearbetad information som slutligen hamnar i långtidsminnet. Detta kan utvecklas på olika sätt.

Förutfattade meningar. Genom minnet (erfarenheten) jämför vi våra sinnesintryck med vad vi tidigare upplevt, dvs. vi ser och hör i viss mån vad vi förväntar oss. Genom att skapa "likhet" kan felaktiga associationer induceras hos mottagaren.

Önsketänkande. Om de förutfattade meningarna verifieras uppfattas situationen vara under kontroll, medan om det uppstår oklarheter och tolkningssvårigheter skapas osäkerhet. Vi tenderar att reducera osäkerhet och försöker därför aktivt tolka och bearbeta en situation så att osäkerheten minskar. Därvid finns det en påtaglig risk att vi omedvetet väljer en tolkning som skapar "säkerhet", även om den är falsk, därför att vi gör någon form av subjektiva sannolikhetsbedömningar. Det kan innebära att *en chef hör vad han gärna vill höra*, eller att vi tenderar att dra förhastade slutsatser om osäkerheten därmed reducerats. Det är frågan om olika sätt att lura sig själv.

Förändringar och regelbundenheters betydelse. Vi har en förmåga att filtrera bort konstanta signaler och detektera det avvikande. Det gör att det är lätt att se alla myror som rör sig men svårt att se de som står stilla. Vi tenderar även att lägga till information

[124] Försvarsmakten *PM Vilseledning*, s. 16-28.

(som inte finns) för att därmed skapa symmetri eller regelbundna mönster. Regelbundenheter och små eller gradvisa förändringar undertrycks, varför de kanske inte uppmärksammas.

Kognitiv dissonans. Eftersom individen upplever motsägelser och oklarheter som obehagliga, de skapar spänning (dissonans), strävar individen att reducera dessa spänningar genom olika mekanismer och omtolkningar. En person som har fattat ett felaktigt beslut eller begått en felaktig handling kan omtolka situationen, eller ändra sina värderingar, så att beslutet eller handlingen kan motiveras. Genom att erbjuda en person ett olämpligt handlingsalternativ och samtidigt en ursäkt att välja detta alternativ kan personen förmås att välja detta alternativ.

Varseblivningen är en aktiv process. Gränsen mellan att varsebli (perception) och att tänka (kognition) är flytande, på grund av att människans informationsbehandling sker i ett stort antal steg från kroppens sensorer (exempelvis ögat) via nervbanorna och deras olika omkopplingsstationer till hjärnans olika delar. Informationen från omvärlden via sensorerna till hjärnan passerar olika typer av filter, och påverkas av minnesbilder och förväntningar. Det är med konkret kännedom om dessa förhållanden som illusionisten kan lura sin publik (som dessutom gärna vill bli lurad). Även det "enkla" maskeringsnätet lurar sin "publik", genom att betraktaren fås att manipulera sina egna synintryck.

Nytillkommande information anpassas till gamla modeller. En förändring i perspektiv kräver antingen ett mycket stort informationstillskott på kort tid eller kontinuerligt tillskott under mycket lång tid. Det enklaste sättet att lura en person är att erbjuda den information han vill ha eller den han förväntar.

Kunskap om motståndarens kulturella förhållanden och sociala dispositioner kan utnyttjas både i syfte att luras och att påverka. Om en nation har tilltro till (informationsberoende) eller övertro på (okritisk auktoritetstro) sina myndigheter innebär detta förhållanden som kan exploateras.

Mer konkreta handlingsregler kan härledas från dessa och liknande resonemang och återges längre fram. Tills vidare konstateras att vilseledning kommer till stånd genom att i lönndom dölja något verkligt förhållande eller genom att på ett trovärdigt sätt exponera något som är felaktigt eller missvisande, dvs. genom att dölja det sanna och framhäva det falska.

Det går att räkna upp ett stort antal metoder för att vilseleda. Eftersom en sådan uppräkning lätt blir svåröverskådlig och osystematisk har Barton Whaley presenterat en strukturering av vilseledningens metoder. Den presenteras i något överarbetad form i figur 6.

Barton Whaley menar att varje vilseledningsakt omfattar simulerande och dissimulerande åtgärder. Med dissimulerande åtgärder avses att dölja det sanna. Med simulerande åtgärder menas framhävande av det falska (jfr figur 4 och avsnitt 3.3). Enligt Barton Whaley finns det endast tre sätt att dölja det sanna och tre sätt att framhäva det falska, vilket framgår av figur 6.[125]

[125] Barton Whaley, "Toward a General Theory of Deception", s. 178-92.

VILSELEDNINGENS STRUKTUR

DÖLJA	FRAMHÄVA
MASKERA – Dölja egenkaraktär – Anpassa omgivningen – Osynliggöra – Undertrycka information	*IMITERA* – Kopiera omgivningskaraktär – Härma
FÖRÄNDRA – Lägga till kända egenskaper – Dra ifrån kända egenskaper – Förklä	*NYSKAPA* – Nya mönster – Skapa nya egenskaper
FÖRVIRRA – Öka osäkerhet – Otydliggöra mönster	*LOCKA* – Skapa falsk säkerhet – Skapa nyfikenhet

Fig. 6. Vilseledningens struktur.[126]

5.2 Tillvägagångssätt

Det är möjligt att med utgångspunkt från angivna principer för vilseledning något mer konkret svara på frågan "hur man gör för att luras". Exempel:

- Förkläd det nya till det gamla vanliga.
- Förändra i små steg.
- Bluffa genom att utnyttja vad motparten vet och förväntar sig.
- Ny information måste erbjudas på ett trovärdigt sätt över flera kanaler.
- Ge motståndaren en ursäkt för att lura sig själv!
- Utnyttja mänskliga svagheter: fåfänga, avundsjuka, lättja.
- Låt motståndaren på egen hand komma fram till felaktiga slutsatser!

⇒ **Det är lättare att förstärka förutfattade meningar än att ändra motpartens uppfattning**. Genom att med olika ledtrådar uppmuntra förutfattade meningar och

[126] Fritt efter Barton Whaley. Figuren hämtad från Hans Furustig, *Militär vilseledning—Några grunder*, FOA-R—96-00365-5.2—SE, november 1996, s. 13.

skapa förväntan avleds motpartens uppmärksamhet från alternativa tolkningar eller handlingssätt.

⇒ Erbjud motståndaren ett skenbart fördelaktigt handlingsalternativ, genom vad som verkar vara ett "naturligt tillfälle". Ett sådant naturligt tillfälle måste skapas artificiellt och handlingsalternativet grunda sig på information som kan bekräftas över flera kanaler.

⇒ Kritisk information kan göras tillgänglig genom skenbart mänskliga misstag. Sättet att erbjuda betet på måste nämligen vara trovärdigt, liksom den falska informationen. Trovärdigheten måste vara hållbar inom ramen för motståndarens kontrollmöjligheter och förväntningar, så att vilseledningen inte avslöjas i förtid.

⇒ Det är möjligt att under lång tid exponera falska rutiner för motståndaren. I ett skarpt läge blir handlingssättet ett helt annat. Det är inte ovanligt att systematiskt "göra sig bättre än man är", exempelvis i alltför tidig marknadsföring av nya vapensystem. Det motsatta sättet är också möjligt, "att göra sig sämre än man är", exempelvis vid demonstrationer av kapacitet och prestanda hos vapensystem som inte ska exporteras.

⇒ Tillvänjning eller acklimatisering åstadkoms genom upprepning eller kontrollerad långsam förändring. Genom att upprepa ett konstlat agerande så att motståndaren kan identifiera handlingsmönstret, skapas uppfattningen att det föreligger en "rutin", ett mönster. Detta kan leda till minskad vaksamhet och möjliggör överraskning i en skarp situation eftersom mönstrets ledtrådar är falska. Motståndaren kan förväxla status quo och långsam förändring eller vänjs till falska indikatorer på att "vargen kommer" ända tills vargen faktiskt kommer på samma indikatorer.

⇒ Efter att avsiktligt låtit motståndaren avslöja skenmål byter man ut objekten mot skarpa mål, eller omvänt. (Det förutsätter att t.ex. avslöjande signaturer inte röjer falsariet under den tid som vilseledningen, det falska "företaget", är av betydelse).

⇒ Genom att avslöja "sanningen" så att motståndaren tror det är en bluff, eller genom att återupprepa en bluff så att motståndaren utgår från att "den här gången kan det inte vara en bluff". "Sanningen" kan avslöjas så att information avsiktligt överförs till motståndaren så att det verkar vara ett oavsiktligt men mänskligt misstag, eller att det orsakats av olycksaliga omständigheter.

⇒ Det som inte kan döljas exponeras (som något annat) eller om det är ett handlingsmönster, upprepas. Högvärdiga mål som inte kan döljas kan falskkopieras (artificiella signaturer skapas), mångfaldigas och spridas ut på lämpligt sätt. Det som inte, enligt motståndaren, är värt att följas upp/kontrolleras/bekämpas "döljs" på ett sådant sätt att det genom ledtrådar drar på sig kostsam uppföljning/kontroll/bekämpning.[127]

[127] Ett militärt exempel på taktisk nivå är skenspårning.

⇒ För att skapa överraskning krävs originalitet, att göra det oväntade eller att demonstrera nya vapen eller motmedel. Därigenom skapas en informationschock som tillfälligt kan överstyra och blockera motståndaren.

Vilseledning kan appliceras i fred, kris och krig mot olika typer av mål och processer. Vilseledning behöver emellertid inte alltid vara fullständig, det räcker många gånger om den är temporär och lokal.

5.3 Informationsförädling och informationsdegradering

Om syftet med vilseledning är att förmå motpartens beslutsfattare att agera på ett visst förutbestämt sätt gäller det att presentera ett därtill preparerat beslutsunderlag. Det är därför önskvärt att veta hur motpartens beslutsprocess ser ut, och hur hans underrättelsetjänst fungerar.

Figur 7 nedan ger en struktur för diskussionen. Siffrorna 1-10 i figuren svarar mot punkterna i diskussionen nedan.

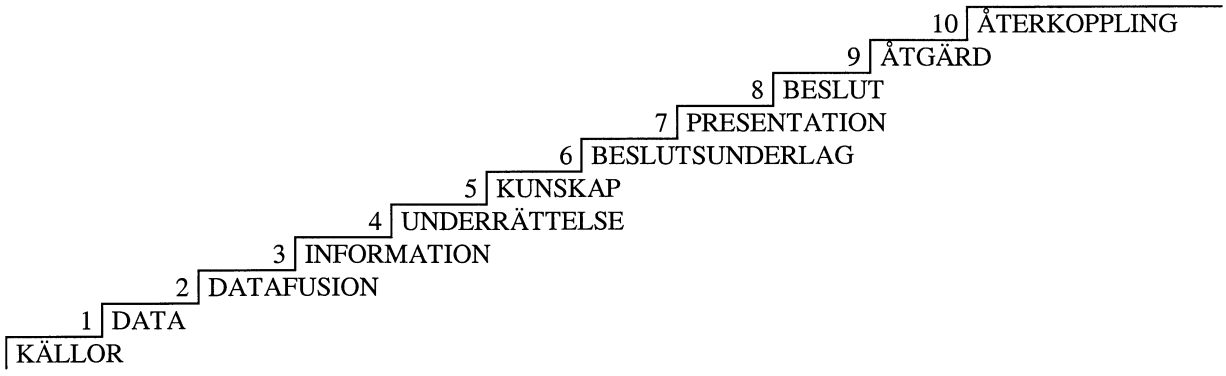

Fig. 7. Informationsförädling och beslutsprocess.

Informationsförädlingen består i att enskilda fakta i rå och okorrelerad form (data) ordnas, struktureras och tolkas till information, som i sin tur bearbetas och analyseras till underrättelser. Underrättelserna kan ha olika karaktär, de kan exempelvis vara beskrivande (nuläge) eller förutsägande (prognos). Allt efter som underrättelserna kvalificeras genom ökad förståelse och verifikation blir de till kunskap. Underrättelser och kunskap ligger till underlag för beslut. Det är givet att om denna process kan påverkas, kan även besluten påverkas.

Beslutsunderlag blir vilseledande om informationsförädlingen ovan avsikligt kan störas så att informationens kvalitet (relevans, sakriktighet, aktualitet, etc) försämras, degraderas. Detta kan ske genom påverkan i steg 1-10 enligt figur 7. Genom att olika åtgärder kombineras förstärks effekten i mottagaren.

Steg 1. Källorna kan bestå av sensorer, informationsbärare av ljud-bild-skrift, mänskliga observatörer eller rapportörer, etc. Om det är känt vilka typer av källor och kanaler motståndaren har kan vilseledningen sättas in redan här. Beroende av var sårbarheten är

störst kan man plantera ut förfalskad information, sprida falska rykten och vidta andra vilseledande åtgärder.

Steg 2-3. Eftersom motparten samlar in en mycket stor mängd data genom sina sensorer och på grund av att det råder tidsbrist (underrättelser är färskvara) måste en viss automatisk databehandling ske, s.k. datafusion. Beroende av sofistikeringsgrad kan data detekteras, klassificeras, ordnas, registreras och eventuellt identifieras av tekniska hjälpmedel. Man talar även om informationsfusion. Om man känner till kriterierna för fusionsprocessen kan vilseledning möjligen åstadkommas genom att processer för mönsterigenkänning och bekämpning missbrukas eller störs, exempelvis genom falksignalering. Eventuellt kan databehandlingen överstyras. Det finns även möjligheter att direkt skada eller förstöra information, men då är det inte fråga om vilseledning.

Steg 3-5. Underrättelser kommer till i en arbetsprocess som exempelvis kan beskrivas på följande sätt: inriktning (behov, planering, inriktning av källor) => insamling => bearbetning och analys => bedömande => delgivning => ny inriktning, etc., i en spiral. Om indata är samstämmiga över flera kanaler och vilseledande, kan det påverka hela processen. Med kännedom om denna process (vilka källor värderas högst, hur lång är bearbetningstiden, hur lång tid tar det att kontrollera en uppgift, etc.) kan en vilseledningsplan planeras. En inplanterad agent (mullvad) kan göra stor skada genom att ge deceptören återkoppling avseende hur underrättelsetjänsten reagerat på vilseledningen. Även andra "inre fiender" kan göra skada, exempelvis sådana administratörer som genom inkompetens inom sakområdet fattar beslut som försvårar verksamheten.

Steg 6-8. Att ge beslutsunderlaget en sista putsning, att presentera det på ett bra sätt är naturligtvis viktigt i all kommunikation. Finns det någon budbärare som kan påverkas? Finns det organisatoriska sediment som gör att vissa hypoteser får större genomslag, tas emot lättare, än andra? Har chefen förutfattade meningar som kan understödjas? Finns det kanske någon inflytandeagent att ta till? Eller går det att försena kloka beslut, förlänga beslutshanteringen genom att så split mellan befattningshavare och påskynda andra irrelevanta beslut, i vilseledande och nedbrytande syfte?

Steg 10. Motståndaren följer naturligtvis upp effekten av sina beslut. Går det att manipulera resultatet av utvärderingen? En befälhavare som får vilseledande information om resultatet av sina åtgärder riskerar att även fortsättningsvis fatta fel beslut.

Det förda resonemanget är endast exemplifierande. Det går att på motsvarande sätt strukturera andra processer (kommunikationssystem, ordersystem, underrättelsesystem i detalj, logistiksystem) och finna tänkbara angreppspunkter för vilseledande insatser.

[128] Tillvägagångssätt.
[129] First United States Army Group.

5.4 Risker vid vilseledning

Det är viktigt att inte hemfalla åt överdrifter, vare sig av vilseledningens möjligheter eller svagheter. Det finns nämligen ingen garanti för hur en vilseledd motståndare reagerar. Han kan göra något oväntat, även om vilseledningsfasen varit framgångsrik. Därför är det viktigt att inse att om vilseledningsoperationen har till syfte att motståndaren ska agera på ett visst sätt, så är det önskvärt att övervaka hur han reagerar (återkoppling, kontroll) och vara beredd att modifiera genomförandet därefter (flexibilitet).

Det kan också vara så att händelseförloppet i stort tar en annan väg än som planerats, vilket kan innebära att vilseledningsoperationen inte behövs eller blir föråldrad i ursprungligt skick. Därför behövs planeringsmässig adaptivitet och löpande underrättelser.

Genom överskattning av egen förmåga kan vilseledningsplanen göras alltför komplicerad. Det är då risk att man lurar sig själv i ett "speglarnas krig". Den enkla och naturliga planen är att föredra framför den eleganta och komplicerade!

Nya sensorer, automatiserad databehandling och datorstöd är inget försvar mot vilseledning. Maskinens förmåga att särskilja mönster, göra associationer och att tänka, är sämre än människans. Det är bara människan som förmår göra snabba hopp mellan tankebanor (intuition). Framför allt är det människan som fattar beslut, utom i några få tekniska sammanhang.

Vilseledningen riktar sig mot människan i egenskap av operatör, analytiker eller beslutsfattare.

Därvid tjänar tekniken som redskap att presentera den vilseledande informationen för människan.

Det gäller emellertid för planerare och beslutsfattare att ta ställning till om de förväntade fördelarna med att genomföra en vilseledningsoperation uppväger de förväntade nackdelarna.

Vilka är effekterna av vilseledning, effekterna i målet? Följande strukturering är en utgångspunkt för att tänka över felkällor och risker vid vilseledning.

- Objektet blir vilselett och vidtar önskad åtgärd.
- Objektet blir vilselett och vidtar någon annan åtgärd.
- Objektet blir vilselett men vidtar ingen åtgärd alls.
- Objektet vilseleder sig själv på gott eller ont.
- Objektet blir ej vilselett p.g.a. att betet eller idén förkastas.
- Objektet blir ej vilselett och avslöjar dessutom operationen.
- Objektet blir ej vilselett, men låtsas gå i fällan för att kontra.

Riskerna består således bl.a. i att

- inplanterad information negligeras eller förvrängs,
- situationen förändras så att hela operationen blir överspelad,
- egen personal reagerar mot att föras bakom ljuset,
- egna aktörer misstänks agera för motståndarens räkning,[130]
- det blir problem med samordningen i tid (timningen),
- larmklockefunktionen mankerar (ser ej skogen för bara träd, vargen kommer för ofta),
- förhandsuppfattningar, självöverskattning och beslutsvånda degenererar objektets beslutsprocess,
- vilseledningsobjektet kontrar.

[130] Mycket hög sekretess är en huvudförutsättning vid vilseledningsoperationer. Få personer är invigda i att det rör sig om en vilseledningsoperation. Därför förs nästan alltid en del av den egna personalen bakom ljuset och de egna aktörerna riskerar att misstänkas för att agera för motståndarens räkning (se t.ex. *Operation Neptun* i avsnitt 4.2).

6. Skydd mot strategisk vilseledning

Most academic historians have been slow to recognize the role of intelligence communities in the relations and political history of the twentieth century.
Vasilij Mitrochin och Christopher Andrew[131]

Inom området vilseledning finns en relativt utvecklad teoribildning.[132] Så är inte fallet när det gäller skydd mot vilseledning, även om försök till en sådan finns.[133] Föreliggande studie gör ett försök att strukturera problematiken kring skydd mot vilseledning med utgångspunkt från såväl teori som praktik.

När det gäller skydd mot vilseledning finns tre möjligheter att avslöja sådan. Den första är att vilseledningsobjektet (den avslöjande parten) har en mänsklig källa som kan berätta om verksamheten. Det kan vara en avhoppare eller en aktiv agent på plats i motståndarlägret. Den andra möjligheten är att man genom kritisk underrättelseanalys i kombination med studier av deceptörens övriga uppträdande möjligen kan sluta sig till att andra motiv och mål, än de som vilseledningen söker framhäva, ligger bakom deceptörens agerande och att man alltså är utsatt för en vilseledningsoperation, en förhandlings-bluff eller liknande. Den tredje möjligheten att avslöja en deceptör är oavsiktliga läckor vid genomförandet av vilseledningen.

Som framgår av exemplen i kapitel 4 och många av fallen som beskrivs i rapportens del 2 är mänskliga källor det vanligaste sättet på vilket vilseledning avslöjas. Vad beträffar läckor kan konstateras att ingen vilseledningsplan är vattentät och än mindre genomförandet. Som redan nämnts kännetecknas historiskt lyckade vilseledningsoperationer inte av total vilseledning/överraskning utan av att vilseledningsobjektet, trots att indikationer funnits, inte har dragit de riktiga slutsatserna.

Det svåraste sättet att avslöja vilseledning torde vara genom kritisk analys. Samtidigt är kritisk analys en metod som alltid står till buds, medan vilseledningsobjektet oftast inte kan styra uppkomsten av mänskliga källor och läckor. Och det är kritisk analys föreliggande rapport främst handlar om, även om mänskliga källor behandlas. När det gäller vilseledningsläckor kan dessa betraktas som insignaler till den kritiska analysen där svaga signaler utgör ett eget forskningsfält. Se avsnitt 6.3.5.

En inneboende svårighet vid avslöjandet av vilseledning är att inget av de ovan beskrivna sätten kan ge hundraprocentig säkerhet. Det klassiska problemet med mänskliga källor är huruvida man skall tro på en enda källa och på grundval av vad denne har att berätta, skall basera den egna statens agerande enbart på dennes vittnesmål. Med svaga

[131] Vasili Mitrokhin och Christopher Andrew *The Mitrokhin Archive*, s. 707.
[132] Se t.ex. Hans Furustig, *Militär vilseledning—Några grunder* och referenserna däri.
[133] Se t.ex. William R. Harris, *On Countering Strategic Deception*, draft R-1230-ARPA (RAND Corporation, Santa Monica, CA, 1973); Richards J. Heuer, "Cognitive Factors in Deception and Counterdeception", i D.C. Daniel och K.L. Herbig (red.) *Multidisciplinary Perspectives on Military Deception*, technical report 56-80-012, (Naval Post-graduate School, Monterey, CA, 1980); Theodore R. Sarbin, "Prolegomenon to a Theory of Counterdeception", i D.C. Daniel och K.L. Herbig (red.), *Strategic Military Deception*, (Pergamon Press, New York, 1982) och Michael Dewar, *The Art of Deception in Warfare*, Kap. 11 Countering deception.

signaler förhåller det sig så att människan har kognitiva begränsningar som gör att hon har mycket svårare att ta till sig svaga signaler, i synnerhet om de går stick i stäv med gängse bedömningar, och lättare att ta till sig konfirmerande information.

En kritisk analys med användande av s.k. *all-source*-material, dvs. alla typer av data från öppna såväl som hemliga källor, skapar en osäkerhet av något annorlunda karaktär där varje enskild källas trovärdighet har relativt mindre vikt eftersom de vägs samman till en aggregerad bedömning med vidhängande osäkerhet. Om t.ex. mänskliga källor saknas för den aggregerade bedömningen får den karaktären av indiciekedja. Hur beslutsfattare väljer att hantera osäkerheten skiftar från fall till fall och beror också på faktorer som ligger utanför analysen.

De mest gynnsamma förutsättningarna att med stor säkerhet kunna uttala sig om att vilseledning pågår torde föreligga då samtliga tre sätt kombineras, dvs. ett aktivt inriktande av särskilda inhämtningsmetoder, en kritisk analys samt ett uppmärksamt och öppet förhållningssätt till och tillvaratagande av svaga signaler.

Ag IW skriver att en grundsyn för arbetet med att ge nationen en tillräcklig förmåga att motstå informationskrigföring kan formuleras utifrån den generella säkerhetskedjan *skydda-upptäcka-reagera* (SUR-modellen).[134] Denna modell synes även kunna användas för skydd mot strategisk vilseledning, även om skydd mot vilseledning som regel ses som en tvåstegsprocess: upptäcka och sedan motverka /reagera.[135]

När det gäller vilseledning torde de viktigaste momenten vara att

- detektera att man är utsatt för vilseledning,
- klargöra syftet med vilseledningen,
- klargöra deceptörens identitet och
- motverka vilseledning.

I listan ovan är sannolikt deceptörens motiv den största stötestenen. Eftersom analysen som syftar till att avslöja vilseledning alltid kommer att vara behäftad med en viss osäkerhet (vilket berörts ovan) kan en analytiker som inte hittar ett trovärdigt motiv för deceptören få uppenbara svårigheter att övertyga sin organisation eller beslutsfattare om att vilseledning verkligen föreligger.

När det gäller modeller för motåtgärder mot vilseledande operationer bör Hans Furustigs *F-modell* nämnas här. Det är dock en modell för diskussion och analys, inte en förebild för planering och åtgärder. I korthet går den ut på att Förstå, Förebygga och Förutse. När man väl är utsatt för vilseledning kan man som motåtgärd Förtiga, Förmildra, Förhindra eller Frondera. Genom att studera deceptörens modus operandi (tillvägagångssätt) och lära sig av sina egna misstag (Feedback) kan ett Fungerande skydd erhållas.[136]

---

[134] *Ag IW*, Rapport nummer 2.
[135] I fallet vilseledning skulle man kunna formulera det som Skydd genom Upptäckt och Reaktion (SUR).
[136] Se vidare Hans Furustig, *Vilseledning mot företag*, FOA- R--95-00130-5.3-SE, maj 1995, s. 36-40.

Furustig framhåller också att det vid planering av motåtgärder finns anledning att varna för *ensidiga* ansatser. Sådana kan leda till *förutsägbarhet* och därmed, om de kommer till motpartens kännedom, till *sårbarhet*. Vilka motåtgärder som kan komma att vidtas och vilken beredskap som finns ska helst komma som en överraskning för deceptören. Att det dock finns en realistisk planering för skydd mot vilseledning bör däremot inte tystas ned. Kännedom om sådan planering/förmåga har rimligen en preventiv verkan.[137]

Vad görs internationellt när det gäller skydd mot vilseledning? För närvarande pågår även i många länder i omvärlden ett intensivt arbete rörande skydd mot informationskrigföring. Precis som i Sverige omfattar det hela spektrumet av åtgärder från nationell policy via organisationsstrukturer ner till metoder och tekniska verktyg för att implementera skyddet. I t.ex. USA föreslog *The President's Commission on Critical Infrastructure Protection* (PCCIP) 1997 bl.a. att såväl den offentliga sektorn som den privata, i sin skyddsverksamhet, bör kontrollera desinformation.[138] Detta är endast ett enstaka exempel på att problematiken med desinformation och vilseledning uppmärksammats i samband med skyddsverksamheten. Det har inte legat inom detta projekts ram göra en mer omfattande undersökning av vad som görs i omvärlden. Detta torde därför bli en viktig uppgift vid ett eventuellt fortsatt arbete (jfr kapitel 7).

Avslutningsvis kan det vara värt att kommentera relationen mellan tidig förvarning, s.k. *early warning*, och skydd mot vilseledning. Området tidig förvarning handlar i första hand om utvecklandet av metoder för att kunna förutse oväntad och elakartad omvärldsutveckling som hotar det egna landet. Även om begreppet är allomfattande och metoderna tillämpliga i olika sammanhang avses på nationell nivå oftast tidig förvarning om militära hot mot den egna staten eller dess intressen. Förvarningsmetoderna handlar om att hitta indikatorer som direkt eller indirekt vittnar om förestående hot, kapacitetsuppbyggnad e.dyl.[139]

Vilseledning däremot, handlar om vad som ibland beskrivs som indikatorhantering.[140] Med detta avses att en deceptör försöker kontrollera och samordna de indikatorer som har möjlighet att bidra till den bild deceptören avser att förmedla. Deceptören kan också skapa indikatorer för att understödja sin vilseledning. Relationen mellan förvarnings- och vilseledningsansträngningarna skulle alltså kunna beskrivas som en kamp mellan försök att identifiera och försök att dölja kritiska indikatorer. Problemet för deceptören består i att inte alla indikatorer som vittnar om en viss typ av verksamhet kan kontrolleras eller döljas. Förvarnarens problem är att han som regel har svårt att hantera svaga signaler.

Ett sätt att betrakta förvarningsproblematiken (den militära) skulle därför kunna vara att se den som en delmängd av skyddet mot vilseledning (som även omfattar vilseledning mot ekonomiska och andra mål). Detta torde dock inte vara det gängse betraktelsesättet inom det forskningsområde som har utvecklats kring tidig förvarning. Förvarningsproblematiken och dess relation till alternativa analytiska metoder behandlas i bilaga 2.

---

[137] Ibid., s. 36.
[138] *Ag IW*, Rapport nummer 2, s. 11.
[139] Vid FOI:s avdelning för Försvarsanalys pågår för närvarande arbete med problematiken kring tidig förvarning inom ramen för projektet Stöd för beslut.
[140] Se t.ex. det amerikanska reglementet för militär vilseledning, Joint Publication 3-58, *Joint Doctrine for Military Deception*, 6 June 1994.

Sett ur ett metod-effekt-perspektiv kan relationen mellan överraskning (det som förvarning försöker förhindra) och vilseledning beskrivas på följande sätt:

> *Strategic warning is the answer to strategic surprise, which may be accompanied by strategic deception. Alternatievly, the purpose of strategic surprise, which is likely to take place in conjunction with strategic deception, is to deprive an adversary of strategic warning.*[141]

6.1 Är det möjligt att upptäcka vilseledning? – En teoretisk utgångspunkt

> *(...) counter-deception, like deception, is in theory possible – always.*
> Barton Whaley[142]

I debatten kring vilseledning hörs ofta argumentet att den deceptör som känner sitt offer och som har tillräcklig träning i vilseledningskonsten alltid kommer att vara framgångsrik. Eftersom deceptören dessutom i sin arsenal förfogar över dubbelbluffen[143] och osäkerheten kommer samma trick att kunna användas framgångsrikt flera gånger. Därför skulle det inte finnas några större möjligheter att skydda sig mot vilseledning.[144] Det faktum att mycket få försök att skydda sig mot vilseledning finns beskrivna i den öppna litteraturen tycks delvis bekräfta detta argument.[145]

Ett annat argument som återkommer är att en ökad vaksamhet mot vilseledning kan leda till att man uppfattar sig vara utsatt för vilseledning när detta inte är fallet, dvs. ökad vaksamhet leder till improduktiva hjärnspöken och vargen-kommer-syndrom (se avsnitt 6.9).

Men ett närmare studium av vilseledning ger vid hand att möjligheter att skydda sig finns. Två av de stora auktoriteterna inom området vilseledning (*deception*), Barton Whaley och Michael Dewar, har också studerat möjligheterna att upptäcka vilseledning (*counter-deception*).[146] Se också CIA-analytikern Richards Heuers arbeten rörande *countering denial and deception* i avsnitt 6.5 nedan.

---

[141] Robert L. Pfaltzgraff, Jr., Uri Ráanan och Warren H. Milberg, *Intelligence Policy and National Security*, (Hamden, Connecticut, Archon Books, 1981), s. 303 citerat i Ladislav Bittman, *The KGB and Soviet Disinformation*, s. 130.

[142] Barton Whaley, "Toward a General Theory of Deception", *Journal of Strategic Studies*, 1982, s. 190.

[143] Dubbelbluff kan ha flera betydelser. En första tolkning är att deceptören använder samma bluff som förra gången. Offret tänker då vanligtvis att inte kan väl någon vara så dum att han använder samma bluff igen, med effekten att bluffen lyckas en gång till. En annan tolkning är att deceptören framhåller sanningen som bluff och en bluff som sanning varvid offrets osäkerhet ökar. En tredje tolkning, som dock har en helt annan innebörd, är att offret låtsas gå på bluffen och spelar med i syfte att kontra vilseledningen (se kap. 5.4).

[144] Michael Dewar, *The Art of Deception in Warfare*, kap. 11.

[145] En annan förklaring till varför mycket lite finns skrivet om skydd mot vilseledning skulle kunna vara att det omfattas av sekretess och därför inte omskrivs i öppna källor. En invändning mot detta är att även om underrättelsearbete och vilseledning är hemliga till sitt innehåll så beskrivs ändå teorierna/formerna för dessa verksamheter som regel i den öppna litteraturen.

[146] En av de svenska auktoriteterna på vilseledningsområdet är Hans Furustig, som därför naturligen har deltagit i detta projekt.

Kunskap om vilseledningens natur och struktur är en nödvändig utgångspunkt för att avslöja vilseledning. Varje vilseledningsakt är konstruerad. Enligt Barton Whaley omfattar varje vilseledningsakt simulerande och dissimulerande åtgärder. Med dissimulerande åtgärder avses att dölja det sanna. Med simulerande åtgärder menas framhävande av det falska (jfr avsnitten 3.3 och kapitel 5). Barton Whaley skriver i sin uppsats *Toward a General Theory of Deception* att det endast finns tre sätt att dölja det sanna och tre sätt att framhäva det falska, vilket framgick ovan i kapitel 5 (figur 6).[147] I ett särskilt avsnitt utvecklar Whaley möjligheterna att upptäcka vilseledning. Han skriver:

> *Counter-deception is the detection of deception. (---) its own theory flows smoothly from the general theory of deception.*
>
> *Several experts have argued that surprise is inevitable, particularly if deception is employed to gain it. While acknowledging the grave difficulties that the intelligence analyst (particularly the counter-deception analyst) faces, I would argue that counter-deception, like deception, is in theory possible – always.*
>
> *The possibility of detecting deception, any deception, is inherent in the effort to deceive. Every deception operation necessarily, inevitably, leaves clues. The analyst requires only the appropriate sensors and cognitive hypotheses to detect and understand the meaning of these clues. The problem is entirely one of technology and procedures and never one of theory.*
>
> *Because everything (whether objects or events) can to some extent be both simulated and dissimulated, deception is always possible. However, because this can never be done to the full extent, counter-deception is also always possible. In other words, incongruent characteristics (clues) inevitably are present in every deception operation. These incongrunent characteristics form alternative patterns (hypotheses) that themselves are incongruent (discrepant, anomalous, paradoxical) with reality. As there are no incongruencies in nature, to detect incongruency is to detect the false.*[148]

Barton Whaley har också funnit att de bästa vilseledningsanalytikerna (underrättelseanalytiker som sysslar med att försöka upptäcka vilseledning) är de som själva behärskar vilseledningens konst. Det huvudsakliga vapnet mot vilseledning är med andra ord att sätta sig i huvudet på deceptören.[149]

Whaleys resonemang ger oss ett övergripande förhållningssätt till hur man skall analysera vilseledning. Michael Dewar, som också är en av dem som försökt att beskriva hur vilseledning skall upptäckas, pekar i kapitlet *Countering deception* i sin bok *The Art of Deception in Warfare* på ett antal konkreta metoder, medel och aktiviteter som kan utnyttjas för att upptäcka vilseledning. Dessa kan betraktas som en nedbrytning och konkretisering av Whaleys mer allmänna utgångspunkt och återges nedan i punktform.

- Det är viktigt att vilseledningsobjektet undviker förutbestämda koncept och idéer och håller sinnet öppet. Historien visar att nästan all framgångsrik vilseledning bygger på att konfirmerande information bibringas vilseledningsobjektet (jfr figur 8 och kapitel 5).

[147] Barton Whaley, "Toward a General Theory of Deception", s. 178-92.
[148] Ibid., s. 190.
[149] Ibid., s. 190.

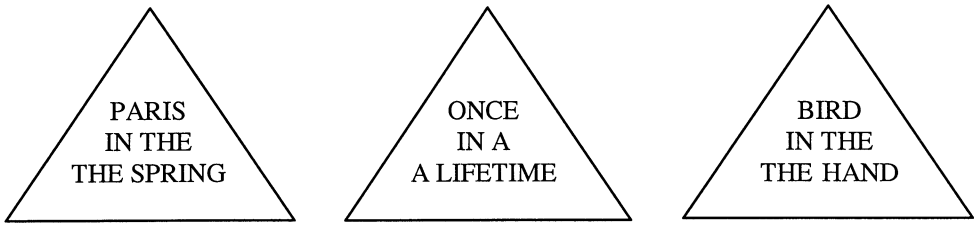

Fig. 8. Förväntningar inverkar på vår uppfattning av omvärlden. De flesta personer ser fraserna "Paris in the spring", "once in a lifetime" och bird in the hand" när de tittar på texten i trianglarna ovan och förbiser det faktum att den bestämda eller obestämda artiklen the och a uppträder två gånger i följd. (British Army)

- Att känna offret respektive deceptören väl. God kunskap om motståndaren är alltså en förutsättning både för framgångsrik vilseledning och skydd mot densamma.

- Att inte dra alltför snabba slutsatser och att försöka titta med deceptörens ögon, förstå hur han tänker och lista deceptörens möjliga handlingsalternativ. Denna process försvåras som regel av att analytikern ofta har tidskrav som han måste uppfylla varför dubbelkontroll av svaga signaler är det som först får stryka på foten (se avsnitt 6.3.5).

- Att kontinuerligt och över lång tid ifrågasätta den information som ens bedömningar ligger till grund för och särskilt att överse tidigare bedömningar i ljuset av ny information som framkommer. En svårighet för deceptören är bl.a. just att upprätthålla vilseledningen över en längre tid.

- Konkurrerande analys (*competitive analysis*) i syfte att möjliggöra perspektivbyte vid studiet av datamaterialet. En ensam analytiker har som regel svårt att göra av varandra helt oberoende analyser av datamaterialet ur olika perspektiv (vilket illustreras av bilden på rapportens omslag).

- Känna till vilseledningens fyra huvudsakliga verktyg: speglar, masker, lögner och sekretess (*mirrors, masks, lies and secrets*). Med spegel avses reflekterad information eller återkoppling. En deceptör kan pröva sin förmåga genom att sända vissa signaler och kontrollera hur vilseledningsobjektet reagerar. Genom denna återkoppling kan deceptören förbättra sitt genomförande. Den analytiker som vill avslöja vilseledning måste alltså tänka på att hans reaktioner övervakas och analyseras. En mask kan användas i defensivt/skyddande syfte för att förmedla en bild av att man är starkare, bättre utrustad, vet mer eller har vissa intentioner. En dylik mask är ett effektivt sätt att slå tillbaka mot deceptören, dvs. genom att skapa maximal osäkerhet i den återkoppling deceptören behöver för att kunna vara säker på vilseledningsobjektet har gått på bluffen eller genom att förmedla en bild av att deceptören själv är utsatt för vilseledning. Svårigheten för analytikern med en lögn är att han då måste ha tillgång till annan information som kan vederlägga lögnen. Sekretessen, slutli-

gen, kräver ett mödosamt arbete för att tränga igenom. Om en analytiker skall ha möjlighet att kunna avslöja operationer/strategier riktade mot honom måste han känna till dessa vilseledningens verktyg.

- Ett framgångsrikt avslöjande av vilseledning kräver att man först kan klarlägga vilka informationskanaler motståndaren har till sitt förfogande, ty det är där den vilseledande informationen förmedlas. Nästa steg är att öppna upp nya och för motståndaren okända kanaler. Alternativt kan man försöka öka detaljupplösningen i de existerande kanalerna till en nivå som inte omfattas av den vilseledande informationen. *Counter-deception* handlar med andra ord om att kunna kombinera mikro- och makroanalys för att kunna upptäcka den minsta inkonsistens och samtidigt kunna sätta in den i ett större sammanhang som beskriver motståndarens mål och medel, förutfattade meningar, vanor m.m.

- Vikten av kontinuitet i bevakningen av förmodad vilseledning. En välkänd princip inom vetenskapen är att ju längre man observerar ett undersökningsobjekt desto större blir noggrannheten.[150]

Dewar avslutar sin beskrivning av möjligheterna att avslöja vilseledning med att understryka att de första intrycken är svåra att ändra och att olika utgångspunkter kan leda till olika slutsatser. Därför bör konkurrerande analys genomföras så snart det är möjligt![151]

I de följande avsnitten diskuteras skydd mot vilseledning utgående från några av ovan beskrivna metoder och angreppssätt. Bland annat behandlas konkurrerande analys, alternativa analysmetoder, indikatorer för att upptäcka vilseledning, källkritik, kunskap om vilseledning, kontinuerlig bevakning inkl. utvärdering av tidigare underrättelseunderlag samt organisatoriska aspekter. Som komplement till ovanstående teoretiska utgångspunkt görs först en utblick i empirin.

[150] Samtidigt som noggrannheten ökar riskerar komplexiteten också att öka och försvåra analysen.
[151] Michael Dewar, *The Art of Deception in Warfare*, kap. 11.

6.2 Att i praktiken upptäcka och motverka vilseledning

Även om, som nämnts ovan, få heltäckande och teoretiska beskrivningar av skydd mot vilseledning finns beskrivna i den öppna litteraturen finns en mängd förslag och idéer till aktiviteter ägnade att förbättra förmågan att upptäcka och motverka vilseledning.

I detta avsnitt redovisas kortfattat de förslag till skydd och motåtgärder mot vilseledning som återfinns i den litteratur som redovisas i den kommenterade litteraturlistan i del 2 (kapitel 1). Av litteraturgenomgången framgår att ett helt spektrum av åtgärder torde stå till förfogande för den som vill skydda sig mot vilseledning. I ena änden av spektrumet finns upplysningsverksamhet, dvs. man vill medvetandegöra att vilseledning förekommer, dess mekanismer och potential samt redovisning av verkliga fall. Denna typ av verksamhet syftar helt enkelt till att öka den mentala beredskapen för att vilseledning kan förekomma och att detta medför en ökad osäkerhet i beslutsunderlaget. I andra änden av spektrumet återfinns egen aktiv vilseledning i syfte att mera aktivt påverka motståndaren. En sådan typ av motverkan kan fylla flera syften samtidigt; dölja egna svagheter, avleda allmänhetens uppmärksamhet, vända den mot den ursprungliga deceptören och skapa osäkerhet för densamme samt eventuellt avskräcka motståndaren.

Ur den kommenterade litteraturlistan har här dragits ut de aspekter av skydd mot informationskrigföring och vilseledning som kunnat hittas. Följande ledord beskriver innehållet i förslagen (som i en del fall kan vara överlappande):

- behov av nationell policy – (aktiv) motverkan bör administreras centralt,
- förstå hoten,
- publicera kända fall av vilseledning i syfte att medvetandegöra journalister och allmänhet, kunskap om deceptörens metoder, vapen och taktik (se t.ex. *Project Truth*[152])
- kunskap om motståndarens sätt att tänka,
- känna sin egen sårbarhet,
- organisationsform (en organisations sårbarhet är beroende av organisationsformen),
- nätverk för skydd, upptäckt och motverkan,
- konkurrerande analyscentra,
- A/B-team,
- djävulens advokat,
- god och snabb egen underrättelsetjänst,
- kritisk analys,
- många kanaler för inhämtning,
- bedriva icke förutsägbar inhämtning,
- korrigera felaktig information,
- kunna presentera eget trovärdigt hot (t.ex. vilseledning), dvs. avskräckning.

De empiriskt funna förslagen sammanfaller i flera fall med de metoder som beskrevs ur ett teoretiskt perspektiv.

[152] Se t.ex. Nordlund, R. & Tubin, E. (red. 1990). *Desinformation i öst och väst. Referat av forskning i Sovjetunionen och USA*, i kommenterade litteraturlistan i del 2.

6.2.1 Att motverka psykologisk krigföring – en analogi

När det gäller att motverka vilseledning gavs ovan några tänkbara metoder. I detta sammanhang kan det vara av vikt att studera hur man motverkar ett av de andra elementen i informationskrigföringen, nämligen psykologisk krigföring. Detta avsnitt baseras på FOA-rapporten *Lönande lögner* som beskriver ett antal scenarier där psykologisk krigföring förekommer och hur den bör motverkas.[153]

Definition: "Psykologisk krigföring utgör en aspekt av informationskrigföring där man medvetet utnyttjar den mänskliga psykologin för att påverka en utvald målgrupps uppfattning, attityder och beteende."[154]

Psykologisk krigföring brukar delas in i fyra delar:[155]

Propaganda *– icke-kommersiell information som sprids i syfte att påverka individers attityder och handlande. Informationen behöver inte vara lögnaktig, men är ofta ensidig och vinklad.*

Kortfattat är propaganda all form av icke-kommersiell information som har för avsikt att påverka individers attityder, perceptioner och beteende till avsändarens egen fördel. Propaganda baseras på i huvudsak sanna, men ofta utvalda och vinklade faktauppgifter. Propaganda kan även vara känsloladdad eller ideologisk till sitt innehåll.[156]

Desinformation *– falsk eller felaktig information som syftar till att vilseleda, förhindra, fördröja, påskynda eller dölja ett händelseförlopp. Genom att förvirra motståndaren kan man även uppnå överraskningseffekter.*[157]

Desinformation är en medveten förvanskning av verkligheten. Genom att systematiskt ljuga vill man påverka människors perceptioner, attityder, beslut och handlande. (---) Desinformation innebär att man antingen ljuger eller försöker dölja sanningen. Skillnaden är att man i ena läget vill få motståndaren att tro på en uppfunnen skenbild, medan den andra formen går ut på att hemlighålla faktiska förhållanden.[158]

Rykten *är påståenden där den ursprungliga källan inte går att säkerställa. Ett rykte kan formuleras och spridas avsiktligt eller bara vara en förstärkning av spontant uppkomna rykten.*

Rykten uppstår lätt när det finns ett otillfredsställt behov av information och gynnas av tillgång på informationskanaler.[159]

Påtryckningar *är övertalning genom hot eller löften.*

---

[153] Paula Stenström, *Lönande lögner*, FOA-R--97-00483-240—SE, 1997.
[154] Ibid., s. 11.
[155] Ibid., s. 12.
[156] Ibid., s. 24.
[157] Desinformationen kan även syfta till att försköna eller svartmåla.
[158] Paula Stenström, *Lönande lögner*, s. 33-34.
[159] Ibid., s. 43.

Motåtgärder mot propaganda

Att skydda sig mot yttre mental påverkan är förstås omöjligt om man inte isolerar sig totalt. Det enda egentliga skyddet är kunskap och medvetenhet om propaganda för att stärka ett kritiskt tänkande. Utan att bli paranoid gäller det att vara uppmärksam på sändarens sympatier, intressen och avsikter. Fientlig propaganda kan förhindras genom att korrekt information och "antipropaganda" sprids som väger upp eller överskuggar angriparens/avsändarens budskap.

(---) Vid upptäckt av propaganda kan alltså följande skyddsåtgärder sättas in: analys av propagandans innehåll för att identifiera avsändare och syfte, undersökning av propagandans inflytande genom exempelvis opinionsundersökningar, korrekt information och/eller motpropaganda, uppföljning och analys av effekter.[160]

Motåtgärder mot desinformation

Valet av motåtgärder vid desinformation beror självklart på situationen. Valet kan exempelvis stå mellan att förneka allt eller medge en del och förneka annat. I vissa lägen kan ett försök till förklaring av desinformation löna sig, men om motbevis saknas riskerar det att uppfattas som övertydlig motpropaganda. Största möjliga öppenhet är tillrådligt. Men hur man än beslutar sig för att bemöta desinformationen är främst den egna legitimiteten avgörande för hur man lyckas. Därför är någon form av propaganda för den egna tillförlitligheten (som skamfilats i den mån desinformationen lyckats) en tänkbar första motåtgärd.

Det psykologiska försvarets uppgift att "säkerställa en snabb och korrekt nyhetsförmedling, en fri opinionsbildning och en konkret och fullständig myndighetsinformation" – kan eventuellt hindras av att det med IT blivit svårare att kontrollera media och kommunikation. Med datakommunikationens alla trådar och länkar är det svårt att spåra ett felaktigt budskaps ursprung, källa och spridning. Detta försvårar även bemötandet av felaktig information: det är osäkert vilka som berörts av desinformationen, vilka man bör nå med korrigerande uppgifter, hur man skall nå dem, och vad som är lämpligast att säga. Å andra sidan står förstås desinformatören inför motsvarande svårigheter.[161]

Ett heltäckande skydd mot desinformation är lika orealistiskt som när det gäller propaganda. Motståndet kan endast utgöras av att utbud och tillgång på snabb och tillförlitlig information "överröstar" den felaktiga informationen.[162]

Motåtgärder mot rykten

För att stå emot falska rykten krävs det, trots svårigheterna, att man definierar ryktets innehåll och försöker sig på en lokalisering av ryktets källa. För att göra detta kan man se på vilka grupper som berörts av ryktet, dvs. källans tänkbara målgrupp, samt undersöka vilka kanaler ryktet introducerats med. En undersökning av ryktets effekter är bra

[160] Ibid., s. 29.
[161] För en genomgång av problematiken med Internet se *Källkritik för Internet* av Göran Leth och Torsten Thurén, SPF rapport 177, (Stockholm, 2000).
[162] Paula Stenström, *Lönande lögner*, s. 39.

för att avgöra om, och i så fall hur, man skall bemöta ryktet. Man kan dementera ryktet om man med säkerhet kan bevisa att det är falskt, annars kan man gå ut med relevant information, eller avleda uppmärksamheten från ryktet med ny information. Ignorans är förstås också ett sätt att bemöta ett rykte för att understryka absurditeten i påståendet. Ett annat alternativ är att bejaka ryktet med vissa (förmildrande) modifikationer.

Det bästa försvaret mot fientliga rykten är att soldater och befäl, men även befolkning, förses med kritiska glasögon som gör dem uppmärksamma på ryktet som psykologisk krigföringsmetod. Något fullständigt skydd lär vara svårt att uppnå eftersom få, om någon, är helt immuna mot rykten, särskilt inte om de kommer från en källa man har förtroende för.[163]

Motåtgärder mot påtryckningar

För att skydda sig mot potentiella hot i krig kan man försöka minimera angreppspunkterna genom att t.ex. sammanfoga stora områden (politiska med ekonomiska osv.) och se till att där det ena brister fyller det andra området i. Samarbete är ett sätt att stå stark mot hot. Det är förstås svårt att säga något om skydd mot hot i största allmänhet, men när det gäller psykologisk krigföring så är kunskap om metoder och hotande aktörer av stor betydelse. Underrättelser om politiska, sociala, ekonomiska, kulturella och militära förhållanden är inte minst viktigt för att kunna avgöra 1) vad som skall räknas som indirekta hot, 2) vilka eventuella hot som kan förekomma, 3) om ett hot är reellt, potentiellt, osannolikt eller över huvud taget inte är praktiskt möjligt, 4) hur man på bästa sätt undviker att hamna i trängda situationer, och 5) hur man på bästa sätt kan motverka hot.

Vad gäller löften som psykologiskt instrument är medvetenhet och en kritisk inställning, samt förkunskaper om beteende och pålitlighet bra för att avgöra om löftet syftar till något annat och om det över huvud taget finns grund för det. [164]

Sammanfattningsvis framträder en bild av de huvudsakliga metoder som bör användas i syfte att skydda sig mot psykologisk krigföring. Dessa är:

- Kunskap om aktörer, hot och metoder i syfte att stärka ett kritiskt tänkande.
- Vikten av att nå ut med sakriktig och relevant information som "överröstar" propagandan, desinformationen eller ryktena.
- Öppenhet i syfte att avslöja propagandister, desinformatörer eller ryktesspridare (kan ske genom press, TV, radio, böcker, Internet m.fl. medier).

Som har framgått av tidigare teoretiska och praktiska resonemang är detta metoder som även bör användas av dem som vill skydda sig mot vilseledning. Vilseledningsanalytikerna bör alltså kunna hämta en del kunskap från sina kolleger inom det psykologiska försvaret.

[163] Ibid., s. 47-48.
[164] Ibid., s. 53-54.

6.3 Skydd baserat på analytiska metoder

Svårigheten ligger i att kombinera ett öppet sinne med en kritisk och granskande attityd.

Hans Furustig

I avsnitt 6.1 talades om perspektivbyte som ett principiellt förhållningssätt för att förbättra möjligheterna att upptäcka vilseledning. Perspektivbyte åstadkoms genom att olika analytiska metoder/förhållningssätt utnyttjas. En av de viktigaste metoderna i arsenalen för att förbättra möjligheterna att upptäcka vilseledning är s.k. konkurrerande analys (*competitive analysis*). Detta beskrivs kortfattat i avsnitt 6.3.1. I avsnitt 6.3.2 beskriver vi kortfattat alternativa analytiska förhållningssätt på en metodologisk nivå. I avsnitt 6.3.3. diskuteras krav på indikatorer för att tidigt kunna upptäcka vilseledning. I avsnitt 6.3.4 berörs vikten av källkritik och i avsnitt 6.3.5 diskuteras något utförligare analys av svaga signaler och kopplingen till olika svarsstrategier. I rapportens del 2 appliceras teorin rörande svaga signaler på de fördjupade fallstudier som görs där.

6.3.1 Konkurrerande analys

Som framgått av de inledande teoretiska och praktiska genomgångarna är konkurrerande analys en av de mest centrala punkterna i ett effektivt skydd mot vilseledning. Med konkurrerande analys menas att två eller fler organisationer genomför analysen. Syftet med den konkurrerande analysen är att möjliggöra perspektivbyte vid studiet av datamaterialet. En ensam analytiker/organisation har som regel svårt att göra av varandra helt oberoende analyser av datamaterialet ur olika perspektiv (vilket illustreras av bilden på rapportens omslag). En annan aspekt är att de första intrycken är svåra att ändra och att olika utgångspunkter kan leda till olika slutsatser varför konkurrerande analys kan gynna möjligheterna att upptäcka inkonsistenser i verklighetsuppfattning.

Sett ur statens perspektiv handlar konkurrerande analys med andra ord om att skapa pluralism i underrättelsesystemet. Detta är synnerligen viktigt när Sverige tillämpar en anpassningsdoktrin som kräver tidig förvarning om hot och risker.

Den konkurrerande analysens fördelar synes vara väl kända hos Försvarsdepartementet varför ingen vidare genomgång av denna typ av verksamhet görs här. Ett exempel på konkurrerande analys från senare år rör just informationskrigföringsområdet där Försvarsdepartementet lagt ut uppdrag med liknande, om än ej helt identisk, ordalydelse på flera myndigheter.

Ett annat exempel är bedömningen av rysk militär förmåga. Såväl Försvarsmakten som FOA (numera FOI) har haft i uppdrag att inkomma med underlag till Försvarsberedningen inför de säkerhetspolitiska kontrollstationerna. Tanken var ursprungligen att FOA:s rysslandsforskare skulle ge en *second opinion* till Försvarsmaktens bedömningar. I dialog med Försvarsdepartementet beslöts att FOA endast skulle använda sig av öppna källor varför detta exempel inte är ett fullvärdigt exempel på konkurrerande analys. Å andra sidan kunde Försvarsdepartementet och Försvarsberedningen med denna ansats få en uppfattning om hur långt man kan komma med s.k. Open Source Intelligence (OSI) samt vilket mervärde hemliga källor tillför. Dessutom skulle FOA:s studier

resultera i en öppen rapport som skulle kunna användas som underlag i den svenska försvarsdebatten.

Det bör dock framhållas att konkurrerande analys inte är någon garanti mot att bli vilseledd, även om chanserna att upptäcka inkonsistenser i omvärldsanalysen torde öka.

6.3.2 Alternativa analytiska förhållningssätt

I föregående avsnitt diskuterades vikten av konkurrerande analys som ett sätt att byta perspektiv. I princip skulle det kunna vara organisationer med samma analytiska förhållningssätt (metod). I verkligheten är det sannolikt vanligare att analyskonkurrenterna arbetar utifrån olika analytiska förhållningssätt. I figur 9 listas några olika typer av analytiska förhållningssätt som står till buds.

Principiell ansats	Karakteristika
Akademisk verksamhet med höga krav på validitet och reliabilitet.	Ackumulering av kunskap. Generella lösningar. Hypotestestning. Logisk analys. Källkritik. Statistisk analys.
Utredningsverksamhet med höga krav på Användbarhet och relevans.	Systemspecifika lösningar. Operationsanalys. Systemanalys. Datorstödd simulering och kalkyl.
Underrättelseverksamhet med höga krav på användbarhet, aktualitet, relevans och sakriktighet.	Specifika situationsberoende lösningar. Underrättelsecykeln. Källkritik. Datorstödd inhämtning och bearbetning.
Bedömandeverksamhet med höga krav på att bereda och ta beslut i tid.	Inriktning Ad Hoc. Systemspecifikt. Nulägesorienterat. Erfarenhet och praxis.
Studieverksamhet med höga krav på strukturering av framtida hot och möjligheter.	Inriktning mot långsiktiga prognoser. Framtidsstudiemetodik. Spelmetodik. Simuleringsmetodik. S.k. lateralt tänkande.

Fig. 9. Exempel på några olika förhållningssätt till problemlösning.

Vilseledning syftar ytterst till att påverka motståndarens agerande genom att manipulera beslut och beslutsunderlag. Denna påverkan kanaliseras antingen direkt mot beslutscentrum och nyckelfunktioner eller indirekt mot inflytelserika opinioner alternativt ge-

nom ledtrådar, spår och olika kanaler för exponering av tillrättalagd information som ska "upptäckas" av motståndarens underrättelseverksamhet.

Metodmässigt är det skillnad mellan å ena sidan hantering av *fakta* – exempelvis att upptäcka, beskriva och förstå vad som faktiskt händer – och å andra sidan bedömning av *avsikter* – exempelvis att förutsäga alternativa samtida eller framtida händelseutvecklingar. Beslut och planer kan vara missvisande, kapacitet skenbar och handlingar diversionsmanövrer. Det innebär att beslutsfattare och analytiker behöver ta ställning till om, och i så fall hur, *osäkerheten* i en analyssituation eller beslutssituation ska hanteras.

Att lösa problem och att skapa beslutsunderlag i samband med hantering av vilseledning innebär att syftet är behovsstyrt och inriktningen är systemspecifik varför kunskap om de olika analytiska förhållningssätten i figur 9 är viktig. Vid identifiering och motverkan av vilseledning är det också viktigt att känna till tillvägagångssättet vid planering och genomförande av vilseledningsoperationer. Detta diskuteras i avsnitt 3.3, 3.5-3.6 och kapitel 5.

Underrättelseverksamheten förenar viktiga aspekter ur de olika förhållningssätten och dess metodarsenal är användbar vid analys av vilseledningsoperationer. Omvänt är underrättelseverksamheten målobjekt vid angrepp i samband med vilseledningsoperationer.

Diskussionen i detta avsnitt utvecklas i bilaga 2.

6.3.3 Krav på indikatorer för att upptäcka vilseledning

Finns det någon aktör eller part som skulle kunna tänkas initiera och driva en intressekonflikt till sin spets om syftet inte kan uppnås på annat sätt? I så fall uppstår frågan om denna aktör också har *förmåga* (kapacitet, resurser) att verkligen genomföra någon form av fientlig operation. Om det inte är fallet uppstår frågan om det kan finnas någon kombination av aktörer som i gemensamt intresse skulle kunna ha resurser och motiv att samordnat genomföra fientliga operationer. Om inte heller detta är sannolikt kvarstår frågan om det är tillräckligt att ha resurser men sakna kända motiv eller att ha motiv men sakna kända resurser för att genomföra en fientlig operation för att detta ska uppfattas som ett hot. Ett hot är som bekant ett möjligt scenario med negativa konsekvenser. Om hotbilden visar sig vara svag kanske det vore bättre att satsa resurser på egna positiva möjligheter att agera.

Om analys visar att någon aktör har kapacitet för eller motiv till att i fientligt syfte genomföra en vilseledningsoperation (informationsoperation, etc.) uppstår frågan hur en eventuell aktion ska kunna upptäckas på ett tidigt stadium. Det är givetvis önskvärt att om möjligt erhålla *förvarning* om att något kan komma att ske. Förvarningen baseras därvid på en eller flera indikatorer. För att det ska vara någon mening med förvarning måste den erhållas med sådan framförhållning att mottagaren har möjlighet att vidta erforderliga åtgärder i tid.

Om det exempelvis finns någon form av riktad misstanke avseende tillvägagångssätt, mot ett geografiskt område eller mot vissa aktörer kan det vara möjligt att identifiera en

lämplig *indikator*. En indikator används i syfte att påvisa något, i det här fallet en fientlig vilseledningsoperation. För att öka känsligheten och förvarningstiden kan olika indikatorer kombineras. Avvikelser från en normalbild, anomalier, kan vara ett tecken på att något håller på att hända. Allmänna krav som kan ställas på en indikator är exempelvis:

- relevans
- otvetydighet
- tillförlitlighet
- aktualitet
- tillgänglighet
- kommunicerbarhet

Om avsikten är att erhålla varningssignaler för att indikera vilseledning och inte bara fientliga operationer i största allmänhet, tillkommer några svårigheter. Information som kan avslöja vilseledning kan döljas i ökat bakgrundsbrus, undertryckande av avslöjande signaler och framhävande av falska signaler. Erfarenheten visar att organisatoriska låsningar och förutfattade meningar om motståndaren och vilken typ av åtgärder som förväntas från denne kan försvåra möjligheterna att upptäcka anomalier, samt försena analys och bedömning. Svårigheten ligger i att kombinera ett öppet sinne med en kritisk och granskande attityd.

Under normala säkerhetspolitiska faser och fredliga konkurrensförhållanden kan det vara svårt att särskilja vaga indikationer från bakgrundsbrus, "the fog of peace". Genom att laborera med kriterienivåerna för varning, exempelvis genom att öka känsligheten erhålls fler "träffar", men också fler "falsklarm". Genom att minska känsligheten erhålls färre "falsklarm", men också fler "missar".

Ett sätt att upptäcka vilseledning inom ett visst tillämpningsområde kan vara att studera hur *förändringar* normalt äger rum inom detta område. Det gäller inte bara förändringar i en normalbild, utan även förändringar i ett förändringsmönster! Enbart förändringar i sig är emellertid ett tveksamt urvalskriterium för vilseledning, särskilt inom områden som naturligt kännetecknas av snabb expansion (revolutionär utveckling). Indikatorer bör grunda sig på något, exempelvis relevant teoribildning eller beprövad erfarenhet.

6.3.4 Vikten av källkritik för att upptäcka vilseledning

En gemensam förutsättning för forskning och underrättelseverksamhet är kritisk attityd och kunskap om källkritik. Falsk eller tvivelaktig information låter ofta avslöja sig genom olika ledtrådar. Den kan uppvisa bristande konsistens i logiken, strida mot kända förhållanden eller enbart grunda sig på osäkra källor och sådant som inte kan undersökas närmare. Den som ska bedöma information måste bl.a. granska följande aspekter:

- frågeställningens krav
- källans tillförlitlighet (reliabilitet)
- innehållets sakriktighet (validitet)

- budskapets angelägenhetsgrad
- budskapets tillkomsthistoria

Dessa aspekter behöver förtydligas. Vi gör här endast några korta tillägg. Beträffande frågeställningens krav gäller att en förfalskning kan ha värde som dokumentation av en vilseledningsoperation, men samtidigt vara värdelös som ett historiskt dokument med pretentionen att avbilda ett verkligt skeende. En källas äkthet kan undersökas med olika tekniska och analytiska metoder. En källa och den kanal som överför budskapet kan bl.a. bedömas utifrån tidigare felfrekvens och propagandistisk tendens. Är sagesmannen kompetent inom sakområdet? Återges egna observationer eller finns mer primära källor? Närhet i tid till händelserna? Exceptionella uppgifter bör granskas särskilt, oavsett vilket rykte källan har. Varför blir innehållet tillgängligt just nu? Timing? Är budskapet viktigt och analysen i behov av särskild prioritering? Är innehållet i linje med kända förhållanden och är det logiskt konsistent? Är innehållet tendentiöst? Vad saknas? Är materialet relevant? Behöver materialet kompletteras?

6.3.5 Analys av svaga signaler och svarsstrategier

Att tidigt kunna upptäcka, identifiera och bedöma svaga signaler kan vara av avgörande betydelse för exempelvis individens hälsa, ekosystemets tillstånd, organisationens utveckling eller statens överlevnad. Svaga signaler kan utgöra ett hot, en möjlighet eller helt enkelt vara irrelevanta. De karakteriseras av att vara svåra att särskilja från omgivningens brus, störningar och andra konkurrerande signaler. Det är av ekonomiska respektive säkerhetspolitiska orsaker väsentligt att kunna hantera svaga signaler i olika sammanhang, inte minst för att erhålla tillräcklig förvarning och för att undvika överraskning. Därför behövs studier av och kunskapsuppbyggnad inom området *svaga signaler (*weak signal research), som är en vedertagen benämning. Det är lättare att skapa vilseledande intryck vid svaga signaler än vid starka, därför bör studiet av svaga signaler även beakta möjligheten av vilseledning.

Med signal menas i detta sammanhang en representation av en observerad eller uppmätt del av verkligheten. Denna representation kan vara sann, missvisande eller falsk i förhållande till det som den avbildar. Att signalen är falsk innebär att en aktör, i syfte att skapa osäkerhet eller för att försvåra, fördröja eller degradera en bedömning eller ett beslut, avsiktligt manipulerar verklighetsbilden genom vilseledande verksamhet. Det kan ske exempelvis genom att undertrycka sann information, genom att tillföra ett överskott av information som skapar osäkerhet eller genom att fördröja tillgången till relevant information för att försämra underlagets kvalitet. Att representationen är missvisande innebär att den oavsiktligt är mångtydig eller förledande. Det kan leda till felaktiga beslut och insatser.

En svag signal kan tolkas som information som är svår att upptäcka och identifiera på grund av förekomsten av andra signaler, störningar och brus i det berörda systemet. En signal kan vara svag, inte enbart därför att den har låg amplitud (styrka) i förhållande till andra signaler, utan även därför att den enbart inträffar vid sällsynta tillfällen (låg fre-

[165] Se bl.a. Internet http://www.mgtaylor.com (Weak Signal Research).

kvens, enstaka händelser), att den byggs upp extremt långsamt (tillvänjningseffekt) eller snabbt (språngvis) eller därför att den genom att manifesteras på ett speciellt och ovanligt sätt helt enkelt är fysiskt eller kognitivt svår att uppfatta av tillgängliga sensorer eller observatörer. Någon mer strikt definition på "svag signal" kommer inte att ges här.

Varför fokuserar vi mot *svaga* signaler och inte mot t.ex. *tidiga* signaler? Dessutom, om intresset fokuseras mot exempelvis avsiktlig vilseledning från en konkurrent eller motståndare, kanske *starka* signaler vore en mer adekvat inriktning? Den som avser att luras vill naturligtvis vara säker på att vilseförande signaler verkligen uppfattas, alltså måste de vara relativt sett starka. Emellertid genereras svaga signaler oavsiktligt genom läckor, i samband med att vilseledning planeras och genomförs, trots eventuella försök till sekretess och döljande åtgärder. Den som exempelvis vill kunna avslöja vilseledning försöker upptäcka motsvarande signaler så tidigt som möjligt, vilket motiverar intresset för *svaga* och *tidiga* relevanta signaler. Samtidigt föreligger här ett moment 22. En motståndare kan mycket väl producera svaga signaler i syfte att lura motparten att förbruka sina resurser på analys av svaga och i detta fall irrelevanta signaler. Dessutom är problembilden i samband med hot och möjligheter ofta diffus, dvs. även *sambanden* mellan de svaga signalerna är sannolikt vaga i sig.

Det väsentliga är inte att ge en snäv definition på svaga eller tidiga signaler, då det egentliga syftet med undersökningen därvid riskerar att definieras bort.

Det gäller helt enkelt att tidigt upptäcka och värdera *kritiska signaler* avseende relevans, autenticitet och aktualitet för att därmed skapa handlingsfrihet för beslut om åtgärd/motåtgärd.

Antag att någon sändare initialt avger svaga signaler och att dessa efter en tid växer i styrka, antal och frekvens, så att de för en observatör övergår från att vara diffusa och svaga till att bli starka. När signalerna fortfarande är svaga ger de sannolikt en möjlighet för en aktör att agera eller reagera på dem till en begränsad kostnad. När de växer i antal, frekvens och styrka kanske det är för sent, i varje fall om förloppet är irreversibelt eller språngvis och om åtgärder kräver en hög resursförbrukning. Här föreligger i så fall ett moment 22. Ju tidigare en signal behöver upptäckas, desto svagare kan den förväntas vara och därmed svårare att upptäcka.

Detekteringen av svaga signaler förutsätter att uppmärksamheten fokuseras mot relevant typ av objekt/fenomen (man kan inte uppmärksamma vad man inte beaktar) och att mottagaren därvid har lämpliga instrument eller sensorer för att indikera spår av objektet/fenomenet, som förutsätts sända ut någon typ av signaler eller ledtrådar (instrumentets/analysens känslighet måste vara tillräckligt stor). *Identifieringen* av signalerna, dvs. att hänföra fenomenet till en relevant kategori, är ett annat problem. Det räcker kanske inte att veta att ett flygplan befinner sig på väg att korsa ett territorium; det är också viktigt att veta vilken typ av flygplan det gäller, kanske även i vilket syfte detta sker. *Bedömningen*, att ta ställning till de identifierade svaga signalernas betydelse och konsekvens, är en annan svårighet. Bedömningen kan försvåras av att beslutsunderlaget är 1) osäkert eller otillräckligt (svaga men korrekta signaler), 2) missvisande eller direkt vilseledande, 3) eller att tiden för ett genomarbetat beslut är alltför knapp.

Av det korta resonemanget ovan framgår att det behövs *kriterier* på olika nivå. Det behövs exempelvis något kriterium för att bestämma om enskilda indata ska avfärdas som normala, föras vidare för analys eller ge upphov till någon form av åtgärd. Den inkommande informationen (den svaga signalen) kan därvid ha olika bearbetningsgrad.

Beslutsfattaren behöver sättas i fokus avseende beslutsfattandet och beslutsprocessen. Beslutsfattaren måste bestämma med vilken grad av säkerhet han vill kunna identifiera de svaga signalerna och till vilken kostnad och med vilken risk han är beredd att hantera dem. I svåra beslutssituationer kan det vara oklart vad som är tillförlitliga och relevanta kännetecken på de händelser som studeras och vilka av alla svaga signaler som ska detekteras och värderas. Därför kommer sambanden mellan iakttagna signaler och utfall i verkligheten inte vara deterministiska, utan ha sannolikhetskaraktär, vilket utgör ett problem i sig.

Beslutssituationen är i vissa tillämpningar mycket komplex. I maktpolitiska sammanhang stater emellan finns det skäl att skilja mellan signaler för avsikt och kapacitet. Vissa signaler, som erhålls genom politisk signalering, kan – men måste inte – vara ett mått på den politiska ledningens avsikter. De kan också vara vilseledande utspel eller "försöksballonger". Signaler som indikerar avsikt är svårtolkade och många gånger svåra att upptäcka. Om en stats eller organisations ledning inte vill avslöja sina planer för motståndare och konkurrenter, döljs eller manipuleras signalerna.

Signaler, som erhålls genom observation och mätning av fysiska förhållanden (antal flygplan, stridsvagnar etc) är ett mått på något faktiskt, den främmande statens faktiska kapacitet. Det kan därför samtidigt förekomma relativt relevanta och säkra signaler, exempelvis kapacitetsangivelser, samt potentiellt mycket relevanta men osäkra signaler (exempelvis indikationer på avsikt) och rent brus. De relevanta signalerna kan förstärka varandra (krigiska intentioner och stark militär kapacitet alternativt fredliga intentioner och svag militär kapacitet) eller motsäga varandra (fredliga intentioner och stark militär kapacitet alternativt krigiska intentioner och svag militär kapacitet). Det kan vara så att de mest relevanta signalerna är både svagast och mest svårtolkade, i synnerhet om de indikerar avsikt eller vilja eller om motståndaren försöker dölja dem. De starkaste signalerna, t.ex. antalet vapenplattformar, erbjuder visserligen ett entydigt mätbart kapacitetsmått, men den faktiska prestationsförmågan bestäms därutöver av många samverkande faktorer, exempelvis tekniska (utrustningens tillstånd och prestanda) och personella (operatörernas hälsa, träning och motivation) för att blott nämna några. Det innebär i så fall att även en analys av starka signaler leder fram till ett sekundärt behov av att identifiera och analysera därtill kopplade svagare signaler.

En studie av svaga signaler bör leda fram till strategier, både för signalernas upptäckt och för lämpliga reaktioner på dem. Vi ger här några exempel på tänkbara utgångspunkter för att utveckla strategier.

Det är viktigt att påminna om att svaga signaler kan förebåda både möjligheter och hot. Därför, när vi talar om att reagera på signaler, avser vi att parera (preventivt gardera eller i efterhand passivt bemöta ett hot) eller att agera (aktivt på förhand eller vid direkt indikation utnyttja en situations alla möjligheter), beroende av den faktiska situationen. Att parera och att agera är förhållningssätt som inte utesluter varandra. Att vara flexibel

och att vara adaptiv kan också kombineras. Ett förhållningssätt skulle således vara att kombinera dessa strategier.

Svag indikering på evolutionär utveckling —> Reagera inom ramen för befintlig mental modell genom flexibel strategi.

Svag förvarning på revolutionär utveckling —> Beredskap att omtolka befintliga mentala modeller för att kunna agera genom adaptiv strategi.

Det är emellertid orimligt kostsamt att ständigt upprätthålla en handlingsberedskap för alla eventualiteter. Därför behöver svaga signaler upptäckas, identifieras och bedömas på ett tidigt stadium. En invändning är att det är just detta som svårt: att tidigt särskilja om förändringar är revolutionära eller evolutionära, respektive om det föreligger negativa hot eller positiva möjligheter. Dessa invändningar behöver penetreras i anslutning till konkreta exempel. Svårigheterna har dels att göra med hur svaga signaler upptäcks och identifieras på ett tidigt förändringsstadium och dels hur man svarar på dem.

En förutsättning för att kunna indikera och följa en utveckling, och därmed för att kunna upptäcka svaga signaler, är att förstå och känna till sammanhanget och närmiljön. Detta kan tolkas som en uppmaning att "känna signalen". Känner man signalen kan den kanske förstärkas och förtydligas hos mottagaren. En kompletterande strategi är att "känna bruset". Känner man bruset kan det undertryckas och elimineras. I båda fallen förbättras signal-brus-förhållandet till fördel för mottagaren. Ansatserna kan kombineras och handlar egentligen om att eftersträva bättre kunskap och förståelse.

Ett annat förhållningssätt är att försöka förebygga att ett hot realiseras (försiktighetsprincipen) alternativt att förmildra konsekvenserna. Med försiktighetsprincipen menas att eliminera eller förstärka svaga punkter, som kan tjäna som utgångspunkt för angrepp alternativt att erbjuda någon väl förberedd angreppspunkt genom att simulera svaghet. Poängen med dessa förhållningssätt är att det inte är helt nödvändigt att kunna upptäcka alla svaga signaler av hotande karaktär, man motar i stället Olle i grind, utan att säkert veta om Olle är närvarande. Om det inte är möjligt att få förvarning om Olle närmar sig kan detta vara en adekvat ansats. Uttryckt på annat sätt är det fråga om att minska sårbarheten, att öka handlingsberedskapen och att förhärda sig mot vissa oönskade händelser.

Om man inte kan upptäcka eller identifiera en viss typ av svaga signaler kan det kanske vara möjligt att i stället förhindra att situationen alls uppstår. Sannolikt ligger emellertid orsaken per definition utanför det egna systemets inflytelsesfär, varför detta i så fall inte är någon allmänt framkomlig strategi.

Alternativt kan det vara möjligt att förneka och förtiga att en viss oönskad situation uppstått till följd av att svaga signaler utvecklats på ett oönskat sätt. Men, "icke-bemötandet" är inte en generell strategi. Tillvägagångssättet kan dessutom strida mot befintlig informationspolicy, exempelvis avseende strävan efter öppenhet.

Ur sändarens perspektiv kan ett kraftfullt utbud av svaga signaler förvirra, fördröja eller mätta motståndaren genom sin belastande mångfald och otydlighet. Starka signaler som

är missvisande och trovärdiga kan lura honom, under den rimliga förutsättningen att de uppmärksammas. Ur mottagarens perspektiv kan svaga signaler avslöja sändarens vilseledningsoperation – om de uppmärksammas och tolkas rätt.

I del 2 appliceras den teoretiska kunskap om svaga signaler, som presenterats i detta avsnitt och som utvecklas vidare i bilaga 3, på de vilseledningsfall som där beskrivs (se kapitel 3).

6.4 Implementering av olika skyddsaktiviteter

Avsnitt 6.3 behandlade olika analytiska skyddsmetoder. Som antyddes i avsnitt 6.1 behöver dessa metoder kompletteras med andra aktiviter för att ett maximalt skydd mot vilseledning skall erhållas. Viktiga komplement till ovan beskrivna analysmetoder är noggrann utvärdering av tidigare fall av vilseledning, eget konspiratoriskt tänkande, analys av egna sårbarheter samt bevakning av misstänkta fall av vilseledning. I avsnitt 6.4.5 antyds ett antal aspekter av vilseledning som vi inte har behandlat.

6.4.1 Utvärdering av tidigare fall av vilseledning

Vi har i kapitel 4 redovisat några historiska fall av strategisk vilseledning och fler fallstudier återfinns i rapportens del 2. Ett syfte med redovisningen av historiska fall är att skapa en medvetenhet hos den statliga säkerhetspolitiska bedömningsapparaten och i underrättelse- och säkerhetskretsar. Till synes mycket osannolika saker har faktiskt inträffat. Ett andra syfte är att ur ett praktiskt perspektiv visa hur vilseledning går till, dvs. som ett komplement till de teoretiska genomgångarna i föregående kapitel och avsnitt.

En utvärdering av tidigare fall bör koncentreras till fall som berört Sverige. Till exempel vore det intressant att försöka klarlägga vilken bedömning Sverige gjorde av de allierades hot att invadera Norge 1944 (se *Operation Graffham*). Gjorde den politiska och militära ledningen samma bedömning? Och vilken bedömning gjorde till exempel Säkerhetspolisen som indirekt genom källa *Onkel* hade insyn i de tyska planerna?[166]

Genom att hålla en sådan undersökning inom Försvarsdepartementet eller någon totalförsvarsmyndighet, t.ex. FOI, skulle även hemligstämplade dokument kunna granskas. Vid eventuella fördjupade arkivstudier avseende *Operation Graffham* är främst arkiven hos UD, Försvarsmakten och Säkerhetspolisen av intresse. Med hänsyn till norska värdepappers uppgång på den svenska börsen finns även en koppling till Börsen och kanske Riksbanken vars arkiv kanske kan lämna värdefulla upplysningar om hur dessa instanser såg på situationen.

Tre mycket intressanta fall som dock knappast är att betrakta som vilseledning är de polska tavelförsäljarna, TIR-långtradarna och ubåtsintrången i svenska skärgårdar. Studier av dessa historiska närtidsfall skulle sannolikt kunna ge kunskap om de organisatorisk-institutionella friktioner som förekom under 1970-, 80-och 90-talen. Dessa friktioner är sannolikt de som en deceptör skulle kunna utnyttja. Dessa tre fall är också intres-

[166] Se Erika Schwarze, *Kodnamn Onkel*, (Albert Bonniers förlag, Stockholm, 1993), s. 130-143.

santa eftersom de skapat något av ett trauma i den svenska säkerhetspolitiska debatten där mer eller mindre professionella inflytelseaktörer och desinformatörer uppträdde.

Intressant att notera i sammanhanget är dock att rykten om vilseledning förekom under bl.a. ubåtsintrången. Enligt dessa rykten skulle de (underförstått sovjetiska) ubåtsintrången syfta till att dra pengar till en kostsam återuppbyggnad av den svenska ubåtsjaktsförmågan från det likaledes kostsamma och i många kretsar kritiserade JAS-projektet. Syftet var alltså att skada det svenska flygvapnet och luftförsvarsförmågan. Eftersom en eventuell sovjetisk invasion i ett första skede sannolikt hade kommit genom luften var denna teori inte orimlig. Även andra omständigheter och tidsandan talade för att denna teori skulle kunna ha varit riktig.

Vi avser inte att fördjupa oss vidare i dessa fall här utan konstaterar endast att de är intressanta att studera inte bara ur ett vilseledningsperspektiv, utan även ur ett ledningsperspektiv när det gäller underrättelse- och säkerhetstjänst.

Utvärderingar av tidigare fall kan också tjäna som utbildningsmaterial av skarp karaktär (se vidare avsnitt 6.5).

6.4.2 Skyddsforskning utifrån ett eget konspiratoriskt tänkande

Ett karaktäristiskt drag för nästan alla typer av skyddsforskning är att de kräver en god kunskap om offensiva förmågor. Till exempel kräver kunskap om pansarskydd kunskap om pansarpenetrationsförmåga och utveckling av vacciner kräver tillgång till offensiva agens om än i små mängder. Vår utgångspunkt för denna studie har varit just detta faktum.

Av såväl de teoretiska som praktiska genomgångarna ovan framgår också att kunskap om vilseledning krävs för att framgångsrikt kunna skydda sig. Enligt en uppgift visar bland annat engelska erfarenheter under andra världskriget att de analytiker som var bäst skickade att avslöja vilseledning var de egna deceptörerna (jfr avsnitt 6.1).

Slutsatsen blir alltså att man för att öka sin skicklighet i att avslöja och motverka vilseledning även bör ha en offensiv forskning/utveckling. I det idealistiskt dominerade paradigm vi nu lever, med EU och andra typer av förtroendeskapande byggen, är dock ett sådant konspiratoriskt tänkande en anomali och av diplomatiska skäl känsligt. Men man bör dock erinra sig att även om den multipolära världen är mer godartad än den tidigare bipolära så finns det nu samtidigt fler potentiella motståndare. Inte minst gäller detta den ekonomiska arenan.

En andra del av det egna konspiratoriska tänkandet är att undersöka vilka potentiella aktörer som finns i omvärlden och huruvida vilseledning kanske redan bedrivs mot oss. Hur är det t.ex. med vårt ekonomiska bidrag till ickespridningsansträngningar och nedrustning i omvärlden? Vem driver Echelon-debatten och i vilket syfte? Och hur är det med larmrapporterna om riskerna med utarmat uran i pansarbrytande ammunition?[167]

[167] Av t.ex. en nyligen publicerad FOA-rapport framgår att det på vetenskapliga grunder är osannolikt att utarmat uran kan ha orsakat de cancerfall som rapporterats hos soldater som tjänstgjort i Kosovo. Halter-

Vem var egentligen Henrik Westanders källa som till slut fällde Kockums ubåtsaffär i Thailand? osv...

En tredje del av det egna konspiratoriska tänkande är att studera vilka svenska svagheter en deceptör skulla kunna utnyttja. Detta görs i nästa avsnitt.

6.4.3 Sårbarhetsanalys – Analysera egna förutfattade koncept

Som nästan alla i denna rapport redovisade fall av vilseledning visar beror säkerhetspolitiska eller underrättelsemässiga felbedömningar på ett begränsat antal mekanismer som dock tycks kunna utnyttjas gång på gång av olika deceptörer och mot olika vilseledningsobjekt.

Ur skyddssynpunkt är det därför av vikt att studera de egna sårbarheterna. Eftersom lyckade vilseledningsoperationer oftast bygger på att deceptören förmedlar desinformation som underbygger vilseledningsobjektets tidigare uppfattningar är det synnerligen angeläget att studera vilka uppfattningar eller förutfattade meningar vi har inom den säkerhetspolitiska sfären samt underrättelse- och säkerhetssfären.

Egna sårbarheter är ingenting som kan diskuteras i ett öppet dokument som detta varför detta avsnitt endast ger två korta exempel.

Ett belysande exempel är Israel som i början av 1970-talet fastnade i den bestämda uppfattningen att arabländerna inte skulle kunna anfalla förrän 1975. Bedömningen grundade sig på en kombination av operationsanalys och underrättelsebedömningar. Anfallet genomfördes dock redan 1973 och så sent som vid anfallets början fick fältoperatörerna som varnade för att anfallet nu skulle börja veta att de skulle hålla sig till insamling av underrättelser och inte lägga sig i analysarbetet vid militärhögkvarteret.[168]

En svensk motsvarighet till denna situation är den allmänt utbredda uppfattning att det inte finns några militära hot mot Sverige inom den närmaste tioårsperioden. Ett noggrannare studium av det underlag som tillhandahållits regeringen och Försvarsdepartementet visar att bedömningarna i själva verket talar om att inget invasionshot finns mot Sverige inom de närmaste tio åren. Däremot finns militära resurser i omvärlden som kan verka mot Sverige. Denna förskjutning av omvärldsuppfattningen bör noteras.

---

na av uran i urinen hos svenska soldater som varit i Kosovo uppgår bara till ca 25% av uranhalterna i den svenska jämförelsegruppen. Björn Sandström och Ulrika Nygren, *Urannivåerna i urinen hos svensk personal som arbetat eller avser att arbeta i den svenska KFOR-styrkan*, FOI-R—0165—SE, augusti 2001. När det gäller de leukemifall som först rapporterades från Italien 1999 är det sannolikare att bensen som använts vid vapenrengöring har orsakat leukemin.

[168] Wilhelm Agrell, *Konsten att gissa rätt – Underrättelsevetenskapens grunder*, s. 140-146. Det faktum att egyptierna utövade strategisk vilseledning saknas dock i Agrells framställning. Denna vilseledning var nyckeln till de initiala egyptiska framgångarna vid övergången av Suezkanalen. De egyptiska förbanden förövade övergången av Suezkanalen 22 ggr (!). Vid urdragningen (!) från den 23:e övningen slogs det skarpa anfallet ut. Förutom att den egyptiska vilseledning byggde på israeliska fördomar om arabernas förmåga att kriga i allmänhet ställde de upprepade övningarna Israel inför en moment-22-situation. Ingen israelisk politiker eller militär hade kunnat beordra (partiell) mobilisering 22 ggr med bibehållet förtroende. För en initierad beskrivning av *Operation Badr* hänvisas till Lars Ulfving, *Brännpunkt Sinai: Ett kompilat av opublicerat material om Oktoberkriget 1973*.

6.4.4 Kontinuerlig bevakning av misstänkta händelser

En metod, eller aktivitet om man så vill, för att mer aktivt skydda sig mot vilseledning skulle kunna vara att löpande bevaka händelser av misstänkt karaktär. När det gäller löpande bevakning kan vi konstatera att det redan förekommer vid ett antal totalförsvarsmyndigheter.

- Informationskrigföringsfrågor bevakas av Informationskrigföringskansliet vid FHS,
- politiska frågor bevakas av UD,
- polisiära av KUT, SÄPO, NSD och TV,
- militära frågor bevakas av HKV MUST, HKV INFO samt FRA,
- mediefrågor bevakas av SPF och
- civila beredskapsfrågor av ÖCB.

Emellertid bevakas inte respektive område från en analytikers metodperspektiv eller ur ett vilseledningsperspektiv från den svenska statsmaktens intressehorisont.

Intressant ur skyddssynpunkt är huruvida det finns kärnor till tolkningskonflikter mellan myndigheter? Om detta är fallet, skulle det kunna vara lättare för en fristående arbetsgrupp än för en myndighetsorganisation att bedriva en dylik bevakningsverksamhet på försök under något år. Denna metod eller aktivitet behöver enligt vår uppfattning inte behöva bli särskilt ekonomiskt betungande. För det fall att bevakningen avses skötas av ordinarie myndigheter bör den kunna ske inom ramen för bevakarens ordinarie verksamhet. För den händelse att alternativet med en fristående arbetsgrupp väljs torde årskostnaden knappast behöva uppgå till mer än några hundra tusen kr.

Vi föreslår därför att en pilotstudie med löpande bevakning av misstänkta fall av vilseledning genomförs med följande avgränsningar:

- Nivå: strategisk.
- Primärt perspektiv: nationellt svenskt säkerhetspolitiskt intresse.
- Sekundärt perspektiv: studium av modus operandi och indikatorer.
- Tertiärt perspektiv: EU-gemensamt säkerhetspolitiskt intresse.
- Försöksperiod: två år.
- Urvalskriterier och prioriteringar: enligt referensgrupp.
- Fördjupningsstudier: två studieobjekt utväljs per verksamhetsår.
- Avrapportering: Avtappning i form av ett PM per månad. Muntlig kvartalsvis redovisning inför referensgrupp. Årsredovisning i form av rapport.
- Precisering av arbetsgrupp, referensgrupp och uppdragsgivare.

Inom ramen för föreliggande projektet har en minipilotstudie av ovan nämnda slag genomförts där misstänkta fall av vilseledning eller händelser som kan ha med vilseledningsoperationer att göra förts upp på en bevakningslista som sedan kontinuerligt följts. I rapportens del 2 (kap. 5) återfinns denna bevakningslista över händelser under år 2000.

Ett antal fall redovisas kortfattat. Där återfinns också ett fall av misstänkt vilseledning som utretts mer grundligt (*Rhenfallet*).

Ett historiskt fall av framgångsrik bevakning av desinformation är AIDS-kampanjen under mitten av 1980-talet. Fallet nämns här eftersom det är mycket instruktivt. Denna sovjetiska desinformationskampanj hävdade att AIDS-viruset var tillverkat vid Fort Detrick i USA, centrum för den amerikanska B-skyddsforskningen. Den första artikeln som uppmärksammade detta var en artikel 1983 i den indiska tidningen Patriot, knuten till det prosovjetiska indiska kommunistpartiet. Med hänvisning till den "välrespekterade" tidningen Patriot tog sedan sovjetiska media upp tråden 1985 och desinformationen fick en explosionsartad spridning i tredje världen och i delar av västvärlden. Sedan 1962 då Patriot startades har den varit ett instrument för spridning av sovjetisk desinformation. Flera motiv till kampanjen har förts fram. Genom att rikta misstankar mot USA och eventuell hemlig forskning kring biologiska vapen ville man avleda uppmärksamheten från västvärldens tilltagande misstankar om att Sovjetunionen i brott mot B-vapenkonventionen bedrev en offensiv biologisk forskning. Ett annat motiv som förts fram är att Sovjetunionen genom AIDS-kampanjen ville avleda uppmärksamheten från anklagelserna om sovjetiska brott mot de mänskliga rättigheterna. Ett tredje motiv är att kampanjen skulle lägga grunden för andra desinformationskampanjer, t.ex. sovjetiska anklagelser att USA forskade kring s.k. etniska bomber, biologiska vapen kapabla att selektivt slå mot vissa raser. Ett fjärde motiv var att genom att utmåla amerikanska militärbaser på allierades territorium som AIDS-smitthärdar skapa spänning mellan USA och dess alierade och i bästa fall stängning av amerikanska baser utomlands. I AIDS-kampanjens spår följde även debatten om rika amerikaners handel med barn från tredje världen i syfte att använda dem som organdonatorer, vilket också ledde till ett fördömande i Europaparlamentet 1988.[169]

En av dem som bevakade AIDS-kampanjen och framgångsrikt motpublicerade i Sverige var Joakim von Braun. Senare avslöjande genom bl.a. avhoppare har visat att han i stort sett hade gjort en korrekt bedömning.[170]

[169] James P. O'Donnell, "AIDS and Bum Dope: A Case Study in Disinformation", *Program for the Study of Disinformation Series 2*, 1988, Boston University, College of Communication; Joakim von Braun, "Sovjetisk desinformation", *Svensk Tidskrift*, nr 1, 1987, s. 64-66; Oleg Gordievskij och Christopher Andrew, *KGB inifrån – 2 Spionskandalernas tid*, (Bonniers, 1990), s. 250 och Vasili Mitrokhin och Christopher Andrew, *The Mitrokhin Archive*, s. 318-319.

[170] Rapportförfattarna är skyldiga Joakim von Braun ett stort tack för att han så generöst ställt hela sitt arkivmaterial rörande AIDS-kampanjen till vårt förfogande.

6.4.5 Ej behandlade aspekter av vilseledning

Föreliggande rapport har inte behandlat en del viktiga frågor. En första fråga är huruvida vissa kulturer är mer benägna att utöva vilseledning. Det antyds i litteraturen att den österländska kulturen skulle vara mer gynnsam för vilseledning, medan den västerländska kultursfären med medeltidens riddarideal snarast tar avstånd från lögnen som umgängesmedel.

En annan intressant fråga är om man kan urskilja nationella särdrag som skulle kunna göra det möjligt att förutsäga hur vissa aktörer kommer att utnyttja vilseledning. Det finns en del arbete gjort inom detta område. Exempelvis har sovjetisk vilseledning ofta använt skräcken för krig som ett sätt att övertyga sina motståndare,[171] dess förkärlek för desinformation och ansträngningarna att hos motståndaren inducera en överskattning av den sovjetiska militära förmågan.[172] Den kinesiska vilseledningen föredrar djupt liggande lögner, multipla strategier och förutsägande av motståndarens intentioner med hjälp av skarpsinnighet. Kunskap om dylika mönster i vilseledningsstilar skulle kunna vara ett verktyg för att tidigt varna vilseledningsanalytiker.[173]

Andra studier antyder att det politiska system som en aktör verkar inom kan påverka villigheten att bedriva vilseledning. I länder med starka politiska ledare med en framträdande roll inom det militära beslutsfattandet tenderar vilseledning att vara vanligare. Diktaturer och auktoritära regimer tenderar generellt att vara mer beredvilliga att utöva vilseledningens ädla konst.[174]

En näraliggande aspekt är att organisationer som är tränade att göra något också strävar efter att göra detta (t.ex. utöva vilseledning). Dessutom tenderar personer att tänka i termer av vad de redan kan eller vad som är bekant. Dessa fenomen antyder att förekomsten av vilseledning är mer troligt om en nation har en apparat för att planera och genomföra vilseledning.

Slutligen finns frågan huruvida vissa personlighetstyper skulle vara mer inklinerade att hemfalla åt vilseledning än andra. Inga sådana bevis tycks föreligga, men personlighetsfaktorer i kombination med miljö och organisation tycks ändå få dem som en gång framgångsrikt vilselett att praktisera igen.

Kunskap om ovan beskrivna fenomen skulle kunna underlätta för vilseledningsanalytikern att söka efter deceptörer och genomskåda deras modus operandi.

---

[171] Se t.ex. Polenkrisen i avsnitt 4.7.

[172] Se The Bomber Gap och The Missile Gap i del 2, avsnitt. 3.4.

[173] Scott A. Boorman, "Deception in Chinese Strategy", i William W. Winston (red.), *The Military and Political Power in China*, (Praeger publishers, New York, 1972, s. 315-316 citerat i Douglas H. Dearth och R. Thomas Goodden, *Strategic Intelligence: Theory and Application*, s. 269.

[174] Herbert G. Goldhamer, "Reality and Belief in Military Affairs: A Fisrt Draft", (R-2448-NA, juni 1977, ed. by Joan Goldhamer (RAND Corporation, Santa Monica, 1979), s. 107-108 citerat i Douglas H. Dearth och R. Thomas Goodden, *Strategic Intelligence: Theory and Application*, s. 269.

6.5 Utbildning

The possibility of deception should not be rejected until it is disproved or, at least, until a systematic search for evidence has been made and none has been found.
Richards Heuer[175]

Som tidigare nämnts är kunskap om vilseledning vital för att framgångsrikt kunna avslöja och skydda sig mot vilseledning. Av denna anledning är utbildningsinsatser av stor vikt. Utbildningen bör syfta till att medvetandegöra berörda parter att framgångsrik vilseledning har förekommit och förekommer samt att förmedla kunskaper om dess mekanismer och funktionssätt.

Tre målgrupper kan urskiljas för utbildningsinsatser. Den första är allmänheten och media. Genom böcker, artiklar i pressen, radio- och TV-program m.m. kan allmänheten "utbildas" eller upplysas om vad som verkligen pågår i omvärlden. Även historiska fall bör redovisas. Av stor vikt i sammanhanget är att det organ som redogör för vilseledningen, desinformationen m.m. har hög trovärdighet. Detta innebär bl.a. begränsningar vad gäller att själv vara en aktiv aktör inom informationskrigföringsområdet eller att ha politiska, ekonomiska eller andra särintressen som kan skada förtroendet och objektiviteten. Två exempel belyser detta.

När det gäller t.ex. skyddet mot psykologisk krigföring ligger sedan länge ansvaret på en särskild myndighet, SPF. Ett annat exempel är förlaget Timbro som under åren försökt att föra fram information om t.ex. underrättelseverksamhet och industrispionage riktat mot Sverige. Mot bakgrund av Timbros politisk-ekonomiska stöd har förlaget sannolikt inte haft lika högt förtroende hos allmänheten som SPF. Icke desto mindre bör tre böcker utgivna av Timbro nämnas här. *Industrispionage* (1984) och *Krig i fredstid* (1988), båda av Charlie Nordblom (med ett stort bakomliggande arbete av Joakim von Braun) samt *Sovjet och fredsrörelsen* (1985) av Peppe Engberg.

Även enskilda aktörer (journalister/analytiker) har genom åren arbetat med upplysningsarbete avseende främmande makts underrättelseverksamhet i Sverige, men inte heller dessa "frilansare" har åtnjutit samma förtroende som t.ex. en myndighet eller en akademisk organisation.

En lösning som används i t.ex. USA och England är att det finns någon form av akademiskt baserad studie- eller forskningsorganisation med knytning till underrättelse- och säkerhetsväsendet. Inom CIA finns t.ex. en underrättelsehistorisk avdelning, *Center for the Study of Intelligence*, som publicerar och kommenterar avhemligade dokument. Material därifrån har använts som underlag i föreliggande studie.[176] I England finns *The British Intelligence Study Group*, vars ordförande är professor Christopher Andrew.

---

[175] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis*, (Center for the Study of Intelligence, CIA, 1999), http://www.odci.gov/csi/books/19104/index.html, hämtad 9 augusti 2001, s. 9.
[176] I del 2 (fallstudierna rörande sovjetisk vilseledning avseende kärnvapnen) beskrivs hur USA faktiskt blev vilselett och i sina National Intelligence Estimates under slutet av 1950- och början av 1960-talet gjorde grova felbedömningar av antalet sovjetiska bombflygplan och missiler (the bomber gap and the missile gap).

Professor Andrew är professor i modern historia vid universitetet i Cambridge. Han har, för att bara nämna två exempel, tillsammans med avhopparna Oleg Gordijevskij och Vasilij Mitrochin skrivit böckerna *KGB: The Inside Story of its Foreign Operations from Lenin to Gorbachev* (1990) resp. *The Mitrokhin Archive: The KGB in Europe and the West* (1999). I framför allt den senare boken som till mycket stora delar är baserade på dokument från KGB:s arkiv beskrivs en mängd desinformations- och vilseledningsoperationer (varav en redovisades i avsnitt. 4.7). Ytterligare ett exempel på akademiskt förankrade studier är den ovan nämnda avhoppade deceptören Ladislav Bittman som är verksam som professor vid Bostons universitet i USA, dels i journalistik och dels som chef för studier av desinformation.

Kanske skulle en institution liknande de ovan beskrivna amerikanska eller brittiska kunna inrättas i Sverige. En annan typ av verksamhet som syftar till att både upplysa den egna allmänheten samtidigt som den slår mot en eventuell deceptör är motpublicering. 1981 startade president Reagan *Project Truth* som skulle avslöja och svara på sovjetisk desinformation. En metod var att systematiskt offentliggöra sådana operationer. Efterhand har olika universitet i USA startat kurser bl.a. propagandans och desinformationens mål och medel.[177] Eftersom opinioner kan påverkas – och i värsta fall luras – genom media, var tanken bakom projektet att både medias och allmänhetens kunskap och kritiska attityd skulle förbättras genom publiceringarna.[178] En mängd anglosaxiska nyhetsbrev av motpubliceringskaraktär gavs ut under det kalla kriget.[179] En viktig aktör i sammanhanget var naturligtvis också *US Information Agency* (USIA) som hade en Soviet Active Measures Coordinator för att bedriva upplysningsverksamhet kring sovjetisk desinformation.

En andra målgrupp för utbildningsinsatser är befattningshavare inom totalförsvaret. Dessa kan naturligtvis ta del av all offentlig publicering som eventuellt förekommer. Därutöver skulle mer kvalificerade kurser kunna ges på respektive myndighet eller inom ramen för kurserna på Försvarshögskolan (vi avser här i första hand kurserna för högre befattningshavare inom totalförsvaret och inte den tidigare militärhögskoledelen).

Den tredje målgruppen är personal inom underrättelse- och säkerhetstjänsten samt eventuellt annan personal som har i uppgift att försöka avslöja vilseledning. Denna målgrupp har behov av den mest kvalificerade utbildningen. Det ligger inte inom ramen för denna studie att peka på all litteratur rörande underrättelseanalys. Sådan litteratur utgör och bör utgöra utbildningsunderlag för personer som arbetar med sådan analys. Vi skall här bara referera till en intressant publikation *Psychology of Intelligence Analysis*.[180]

Amerikanska CIA har genom åren gjort ansträngningar att förbättra kvaliteten på agenturens analyser. I ovan nämnda bok nämns fyra personer som gjort särskilt viktiga bi-

[177] Ett exempel under 1980-talet var *Program for the Study of Disinformation*, vid Boston University, College of Communication (där Ladislav Bittman arbetar).
[178] Se Nordlund, R. & Tubin, E., *Desinformation i öst och väst,* i kommenterade litteraturlistan i del 2.
[179] Se t.ex. *Disinformation – Soviet Active Measures and Disinformation Forecast* och *Counterpoint – A monthly report on Soviet Active Measures: the worldwide psychological warfare offensive.*
[180] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis*, (Center for the Study of Intelligence, CIA, 1999), http://www.odci.gov/csi/books/19104/index.html, hämtad 9 augusti 2001.

drag till kvalitetsutvecklingen rörande CIA:s underrättelseanalys: Sherman Kent,[181] Robert Gates,[182] Douglas MacEachin[183] och Richards Heuer.[184] Heuer har framför allt skrivit om inneboende svagheter och avvikelser i den mänskliga tankeprocessen. Enligt Heuer står underrättelseanalytikern inför tre fundamentala utmaningar:

- *The mind is poorly "wired" to deal effectively with both inherent uncertainty (the natural fog surrounding complex, indeterminate intelligence issues) and induced uncertainty (the man-made fog fabricated by denial and deception operations).*

- *Even increased awareness of cognitive and other "unmotivated" biases, such as the tendency to see information confirming an already-held judgment more vividly than one sees "discomforting" information, does little by itself to help analysts deal effectively with uncertainty.*

- *Tools and techniques that gear the analyst's mind to apply higher levels of critical thinking can substantially improve analysis on complex issues on which information is incomplete, ambiguous, and often deliberately distorted. Key examples of such intellectual devices include techniques for structuring information, challenging assumptions, and exploring alternative interpretations.*[185]

Ett område där Heuers insatser varit speciellt viktiga för CIA:s analysmetodologi är hypotesprövning.[186] Detta behandlades i bilaga 2. Hypotesprövning har en viktig funktion som struktureringsverktyg.

Ett annat område där Heuer gjort banbrytande insatser är hur man skall avslöja vilseledning (*countering denial and deception*). Heuer noterar bl.a.

> *...that analysts often reject the possibility of deception because they see no evidence of it. [---] rejection is not justified under these circumstances. If deception is well planned and properly executed, one should not expect to see evidence of it readily at hand. Rejecting a plausible but unproven hypothesis too early tends to bias the subsequent analysis, because one does not then look for the evidence that might support it. The possibility of deception should not be rejected until it is disproved or, at least, until a systematic search for evidence has been made and none has been found.*[187]

Heuers verk används regelbundet i undervisningen av alla CIA:s nyanställda analytiker samt vid kurser i *warning analysis* och *countering denial and deception.*

---

[181] Tjänstgjorde vid CIA:s föregångare Office of Strategic Services (OSS) och blev sedermera professor vid Yale.
[182] Slutade sin karriär som chef för CIA.
[183] Tidigare Deputy Director for Intelligence (DDI), dvs. chef för CIA:s analysavdelning.
[184] Heuer skiljer sig från de övriga genom att han har haft en mycket lång karriär vid CIA:s Directorate of Operations innan han efter 24 år flyttade över till analysavdelning Directorate of Intelligence. De övriga var analytiker från början till slut.
[185] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis*, s. 8.
[186] Analysis of Competing Hypotheses (ACH) enligt Heuers terminologi.
[187] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis*, s. 9.

Syftet med att i denna rapport nämna Richards Heuer och hans bok *Psychology of Intelligence Analysis* har varit att visa på att det finns organisationer som på ett kvalificerat sätt sysslar med problematiken att avslöja vilseledning. Boken samt referenserna i denna förtjänar ett noggrannt studium.[188]

I bokens inledande kapitel föreslås, baserat på Heuers råd, ett antal rekommendationer. CIA:s ledning bör vidta åtgärder för att:

- *Establish an organizational environment that promotes and rewards the kind of critical thinking he [Heuer] advocates – or example, analysis on difficult issues that considers in depth a series of plausible hypotheses rather than allowing the first credible hypothesis to suffice.*

- *Expand funding for research on the role such mental processes play in shaping analytical judgments. An Agency that relies on sharp cognitive performance by its analysts must stay abreast of studies on how the mind works – i.e., on how analysts reach judgments.*

- *Foster development of tools to assist analysts in assessing information. On tough issues, they need help in improving their mental models and in deriving incisive findings from information they already have; they need such help at least as much as they need more information.*

- *Commit to a uniform set of tradecraft standards based on the insights in this book. Leaders need to know if analysts have done their cognitive homework before taking corporate responsibily for their judgments. Although every analytical issue can be seen as one of a kind, I suspect that nearly all such topics fit into policy sensitivity. Corporate standards need to be established for each such category. And the burden should be put on the managers to explain why a given analytical assignment requires deviation from the standards. I am convinced that if tradecraft standards are made uniform and transparent, the time saved by curtailing personalistic review of quick-turnaround analysis (e.g., "It reads better to me this way") could be "reinvested" in doing battle more effectively against cognitive pitfalls. ("Regarding point 3, let's talk about your assumptions")*

- *Pay more honor to "doubt". Intelligence leaders and policymakers should, in recognition of the cognitive impediments to sound analysis, establish ground rules that enable analysts, after doing their best to clarify an issue, to express doubts more openly. They should be encouraged to list gaps in information and other obstacles to confident judgment. Such conclusions as "We do not know" or "There are several potentially valid ways to assess this issue" should be regraded as badges of sound analysis, not as dereliction of analytic duty.*[189]

[188] Material av liknande typ används regelbundet i FOI Försvarsanalys undervisning av nyanställda operationsanalytiker. Även om operationsanalytikerna inte sysslar med underrättelseanalys så syftar undervisningen till att få bukt med de inneboende svagheter och avvikelser som den mänskliga tankeprocessen har.

[189] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis*, s. 10.

6.6 Särskild inhämtning

> *Risken för desinformation och vilseledande är också påtaglig och måste så vitt möjligt kunna avslöjas och identifieras. Bl.a. av den anledningen behövs det under alla förhållanden en underrättelsefunktion, som arbetar med vad som betraktas som traditionella underrättelsemetoder.*[190]

Som framgår av flera av de exempel som presenteras i denna rapport (se kapitel 4 och del 2) är det svårt att avslöja vilseledning endast med hjälp av kritisk analys och analys av svaga signaler (i synnerhet läckor vid genomförandet av vilseledningsplanen). Nästan alla större, initialt framgångsrika vilseledningsoperationer som i något stadium har blivit avslöjade har avslöjats av mänskliga källor.

Även andra särskilda inhämtningsmetoder så som signalspaning och satellitspaning kan potentiellt ge viktiga bidrag till en kritisk analys med syftet att upptäcka vilseledning. Samtidigt är det högst sannolikt att en deceptör lägger stor vikt vid att manipulera just sådana indikatorer som kan upptäckas med dessa insamlingsmetoder.

När man undersöker misstänkta fall av vilseledning kommer man att stöta på en stor mängd informationsbitar av vilka de flesta är sanna. För att, med ökad sannolikhet, genom analys kunna visa att vilseledning föreligger måste man kunna påvisa att åtminstone någon eller några informationsbitar är osanna. Det kan t.ex. ske då man genom satellit- eller flygspaning kan konstatera att det som skulle föreställa markrobotar i själva verket utgörs av attrapper. Men de flesta vilseledningsåtgärder är som regel mer sofistikerade och kan inte avslöjas med tekniska hjälpmedel. Det krävs personbaserad information. Vid inriktning av inhämtningsresuserna bör man därför i första hand sikta på mänskliga källor. Dessa bör helst finnas nära beslutsfattare eller eventuella deceptörer. Vikten av mänskliga källor som en del i arsenalen för att upptäcka vilseledning kan inte nog understrykas!

Förmåga till sådan inriktning av underrättelseinsamling samt över huvud taget vikten av en centraliserad policy för nationellt skydd mot vilseledning ställer vissa krav på den organisatoriska lösningen för detta skydd. Detta diskuteras i nästa avsnitt.

Även om skydd mot vilseledning i de flesta fall torde vara en rent nationell angelägenhet, i synnerhet i kris och krig, kan internationell samverkan i syfte att upptäcka och identifiera deceptörer bli aktuell. Sådan samverkan bör styras från samma instans som inriktar insamlingsresurserna.

[190] SOU, *Underrättelsetjänsten—en översyn*, s. 251.

6.7 Vikten av att aktiva och passiva skyddsåtgärder kombineras

Ett vanligt förekommande sätt är att betrakta vilseledning som en del av en samordnad plan i syfte att få vilseledningsobjektet att göra något som det annars inte skulle göra. Vår utgångspunkt är därför att ett skydd mot vilseledning på motsvarande sätt skall utgöra en **samordnad verksamhet** bestående **av olika metoder för att upptäcka vilseledning samt skyddande åtgärder och aktiviteter** som kompletterar och delvis överlappar varandra. Överlappningen är viktig eftersom den ger en möjlighet att kontrollera uppfattningar mot flera analyser/källor.

Den som vill skydda sig mot avsiktlig vilseledning gör klokt i att kombinera både passiva skyddsåtgärder och aktiva motåtgärder (se figur 10).

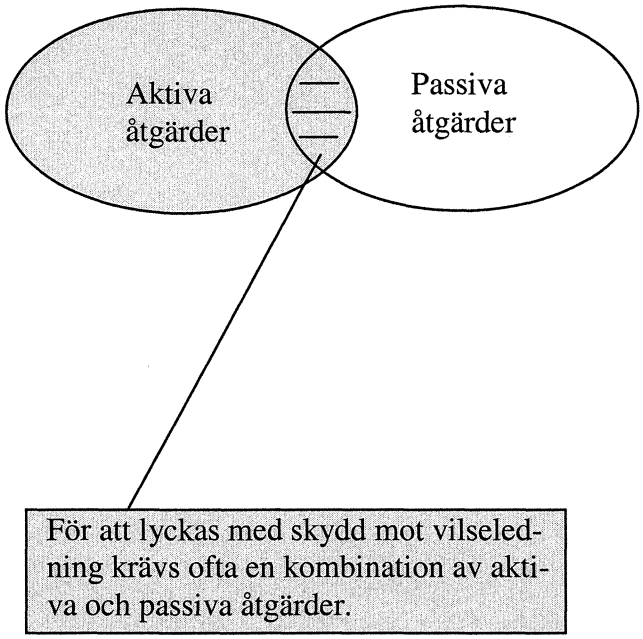

Fig. 10. Grundprinciper för skydd mot vilseledning (jfr fig. 4).

Skyddsåtgärderna bör omfatta bl.a. följande:

- inkorporerande av skydd mot vilseledning i en nationell policy för skydd mot informationskrigföring,
- olika analytiska förhållningssätt inkl. konkurrerande analys,
- löpande bevakning av misstänkta fall av vilseledning,
- förstå vilseledningens mekanismer och tillvägagångssätt (modus operandi),
- möjliggöra tidig indikation (upptäckt) av pågående vilseledningsoperationer,
- förebygga, förhindra och försvåra att vilseledningen alls kommer till stånd,
- gardera förväntad vilseledning genom förutseende (sårbarhet),

- mildra och dölja den trots allt genomförda vilseledningens effekter,
- återförsäkra att kritiska systemfunktioner ej helt slås ut trots genomförd vilseledning,
- vända motståndarens åtgärder mot honom själv,
- frondera motståndaren och förvirra honom genom egna aktiva och vilseledande åtgärder och
- följa upp och utvärdera effekten av olika utspel och motåtgärder.

Generellt (oavsett konfliktnivå och situation) är det en god idé att till alla informationskonsumenter förmedla en grundläggande kritisk attityd i källkritiska sammanhang. För analytiker och beslutsfattare i allmänhet är en grundläggande kunskap i underrättelsemetod (underrättelsecykeln) värdefull. De som dessutom bedöms utgöra målgrupp för vilseledningsoperationer behöver kunskap om vilseledningens teori och praktik, dess modus operandi. Syftet med dessa riktade åtgärder är att öka kunskapen om vilseledning och därmed kanske förebygga att den kommer till stånd. Övriga principiella åtgärder/motåtgärder i förteckningen ovan har olika karaktär och syften och behöver systematiskt utvecklas för den specifika miljö och situation som är aktuell. Det är emellertid en separat studieuppgift.

6.8 Organisatoriska aspekter

Hur skyddet mot vilseledning skall arrangeras organisatoriskt är en komplicerad fråga. Det har inte varit möjligt att inom ramen för detta projekt studera organisationsaspekten mer djupgående. Detta avsnitt har därför karaktären av reflexioner kring problemet utifrån den litteratur som studerats. Efter några inledande funderingar reflekterar vi kring möjligheten att ansluta oss till den organisationsstruktur som *Ag IW* har föreslagit för skyddet mot informationskrigföring.

Eftersom vilseledning kan vara av militär, politisk, ekonomisk, teknisk-vetenskaplig eller annan art, antingen var för sig eller integrerat, bör ett antal myndigheter engageras i skyddet. Hur detta skydd bör organiseras, vilka arbetsformer som bör utnyttjas samt vilka myndigheter som bör delta diskuteras övergripande i nedan. Vilka arbetsuppgifter skulle kunna tänkas ingå för dem som ingår i skyddet mot vilseledning (avgränsningar och klargörande av ansvarsfördelning)? En preliminär utgångspunkt är att nätverk för samverkan mellan berörda myndigheter synes vara en tilltalande modell med hänsyn till indikatorernas diversifierade art.

Inledningsvis diskuteras nedan några principiella punkter som rör organisationsformer för ett skydd mot vilseledning. Bland annat motiveras varför nätverk synes vara en av de mest effektiva lösningarna.

Litteraturen talar om nätverk i olika sammanhang för att skydda sig. Det finns flera anledningar till att nätverk är att fördra framför en vilseledningskyddsmyndighet à la SPF (Styrelsen för psykologiskt försvar). För det första, om man hade en organisationsenhet som svarade för nationellt skydd mot vilseledning skulle den omedelbart bli ett förstahandsmål för en eventuell deceptör. Endast om en sådan organisation kunde vara så hemlig att ingen kände till den skulle den kunna räkna med att få verka ostört. Men ef-

tersom många av de åtgärder för att skydda sig som beskrivs i denna rapport kräver öppenhet för allmänheten hamnar man i en slags moment-22-situation.

I analogi med studier från andra områden där olika distribuerade försvarsstrukturer utsätts för attacker finns det anledning att tro att ett nätverk är svårare att störa än en centraliserad och hierarkisk försvarsstruktur.

För det andra är det förmodligen också lättare att organisera ett nätverk bestående av befattningshavare på olika myndigheter, organisationer och företag. Detta kan då sannolikt ske inom ramen för redan existerande organisationsenheter.

För det tredje är det sannolikt enklare att hålla åtminstone delar av nätverket hemligt. Att nätverket existerar behöver inte vara hemligt, men däremot bör identiteten hos de individer som ingår var okänt för dem som inte är direkt involverade i verksamheten.

För det fjärde innebär ett nätverk en distribuerad hjärnkraft, dvs. fler personer med en samlad och bred kompetens samt fler par ögon och öron som kritiskt granskar omvärlden i syfte att upptäcka indikatorer på pågående vilseledning. Som tidigare beskrivits handlar vilseledning om indikatorhantering. De indikatorer som kan förväntas uppträda kommer förmodligen vara av mycket varierande art varför en organisation ensamt svårligen kan tänkas ha kompetens att bevaka samtliga indikatorer.

För det femte innebär ett nätverk en effektiv form att främja ett incidentrapporteringssystem, dvs. de i nätverket ingående organisationerna eller personerna rapporterar in till ett nav som bär huvudansvaret för den kritiska analysen och förslagen till motverkan.

Samtidigt är det viktigt att understryka att även nätverkslösningar har nackdelar. Två uppenbara sådana är svårigheten att hantera sekretessen i ett alltför vitt förgrenat nätverk samt att olika organisationskulturer ingående i nätverket riskerar att leda till friktioner och därmed minskad effektivitet.

Ett dylikt nätverk skulle kunna organiseras på olika sätt. Nedan diskuteras några förslag till nätverksformer.

En möjlighet är att organisationsenhet inom Regeringskansliet (Försvarsdepartementet) utgör huvudman i nätverket. Myndigheter, organisationer och företag rapporterar från sina respektive kompetensområden trender som en deceptör skulle kunna tänkas utnyttja, anomalier i den ordinarie verksamheten som skulle kunna tyda på pågående vilseledning osv. Med myndigheter avses i första hand UD, Försvarsdepartementet, SÄPO, MUST, FRA, FOI, FMV, ÖCB, SPF och FHS (Informationskrigföringskansliet, IKK). Med hänsyn till eventuella ekonomiska aspekter av vilseledning bör nätverket möjligen även omfatta t.ex. Riksbanken, Börsen, Kommerskollegium, Riksgäldskontoret m.fl. centrala myndigheter. I synnerhet när det rör försvarsindustrin finns anledning att även inkludera privata företag (jfr vidare exemplen i del 2).

En annan möjlighet är att utse t.ex. MUST till huvudman i ett nätverk. Detta kan vara lämpligt med tanke på att MUST av Underrättelseutredningen pekats ut som den svenska "all-source-underrättelsefunktionen". Frågor som då uppstår är t.ex. hur skyddsverksamheten skall organiseras på MUST? Skall det spridas ut på olika befattningshavare

som tillika-uppgift över hela organisationen för att täcka in så många aspekter av undsäk-komplexet som möjligt? Eller skall en speciell grupp hantera dessa frågor?

Båda dess typer av nätverk skulle kunna organiseras på samma sätt som de referensgrupper som redan existerar inom till exempel ickespridningsområdet, där en stor respektive liten referensgrupp deltar och där Säkerhetspolisen har det samordnande huvudansvaret för verksamheten.

För att få extra bredd och kompetens skulle ett sådant nätverk utöver myndigheter, organisationer och företag kunna knyta pensionerad personal från statsförvaltningen till sig. Exempel på lämpliga kategorier är erfarna diplomater, underrättelse- och säkerhetspersonal samt säkerhetspolitiska forskare – alla med kunskap om vilseledning.

Diskussionen ovan, rörande skyddets organisatoriska form, har hittills varit relativt principiell till sin karaktär. Vi övergår nu till att diskutera ett mer konkret förslag. I syfte att åstadkomma enhetlighet i ett eventuellt skydd mot informationskrigföring, som omfattar även skydd mot vilseledning, tar vi därför vår utgångspunkt i *Ag IW*:s förslag i stort till ansvarsstruktur.

Författarna är väl medvetna om att en del av *Ag IW*:s förslag är föråldrade eller kan komma att ges en något annorlunda utformning med tanke på senare utredningar, i första hand *Sårbarhetsutredningen* (SOU 2001:41 *Sårbarhet i en ny tid*). Som ett resultat av denna kan nya organisationsenheter/myndigheter komma att uppstå och nuvarande organisationer/myndigheter att upphöra/förändras. Det förtjänar därför att understrykas att diskussionen nedan i första hand är principiell och rör funktioner och inte konkreta organisationsenheter, även om sådana nämns vid namn. Dessutom kan en del terminologi i diskussionen nedan skilja sig från ordbruket i *Sårbarhetsutredningen.*

Mot bakgrund av de sammanvägda förslagen från *ASTA-studien* och *Ag IW:s* första rapport (se avsnitt 2.1) skisserar *Ag IW* i sin andra rapport en ny ansvarsstruktur för ett nationellt skydd mot informationskrigföring. Där beskrivs de organisatoriska behoven för det nationella samordningsansvaret enligt nedanstående. Inom parentes anges föreslagen lokaliseringen av respektive enhet/funktion.

- Inrättande av en **interdepartemental samordningsgrupp** inom Regeringskansliet för att lösa IW-relaterade problem av förvaltningsmässig karaktär. Gruppen bör även kunna utgöra en krishanteringsresurs. (Regeringskansliet)
- Behov av ett nytt **nationellt funktionsansvar på central nivå**. Denna bör vara ett funktionsövergripande inriktningsorgan, men kan också ha av Regeringen delegerade operativa befogenheter för vissa situationer. Enheten bör innehålla delar för hotbearbetning, skydd, incidentanalys samt övergripande samordning och inriktning. (ÖCB)
- Behov av en s.k. **statistikenhet** för att få en uppfattning om omfattning och karaktär av IT-incidenter inom såväl privat som offentlig sektor. Statistikenheten kan även fungera som taktisk varningsfunktion. (Näringslivets säkerhetsdelagation, NSD)
- Behov av en **aktiv IT-kontrollfunktion** av Red Team-modell för statsförvaltningen. (FM/MUST)

- En **StatsCERT**[191] som hanterar IT-incidenter mot statsförvaltningen i realtid. (PTS med stöd av RPS).
- Inrättandet av en särskild analysgrupp för **operativ mediebevakning** av främst Internet. (SPF)[192]

På motsvarande sätt anser vi att ett **organ i Regeringskansliet** behövs. Detta organ bör ha flera uppgifter. För det första att formalisera en nationell policy för skydd mot vilseledning. För det andra att övervaka implementeringen av densamma. För det tredje att initiera utbildning rörande vilseledning hos de deltagande myndigheterna, organisationerna och företagen. För det fjärde bör detta organ ha en begränsad bearbetningsförmåga avseende vilseledningshot. Även om huvudansvaret för hotbearbetning m.m. föreslås vara huvuduppgift för ett nationellt funktionsansvar på central nivå (se nedan) har ett organ i Regeringskansliet delvis en annan utblick i säkerhetspolitiska frågor genom sin centrala placering. Och som redovisats ovan är centralisering såväl vid genomförande av vilseledning som skydd mot vilseledning av stor vikt. För det femte bör organet i Regeringskansliet ansvara för egna aktiva motåtgärder för det fall att vilseledning upptäcks. Detta organ skulle i fallet vilseledning företrädesvis kunna vara Samordningssekretariatet för säkerhetspolitiska underrättelsefrågor (Fö/SUND). Motivet till detta är givetvis den nära koppling som finns mellan underrättelseverksamhet och vilseledning. Dessutom bör organet ansvara för inriktning av insamlingsresurserna (jfr avsnitt 6.6), en uppgift som redan i dag åligger SUND.[193]

I likhet med *Ag IW:s* struktur bör ett **nationellt funktionsansvar på central nivå** finnas. Det bör innehålla delar för hotbearbetning, skydd, incidentanalys samt övergripande samordning och inriktning. Den bör också ha det operativa ansvaret för eventuella aktiva motåtgärder. Det centrala nationella funktionsansvaret bör enligt vår mening ligga på HKV MUST. Motivet till detta är i första hand att MUST är rikets *all source*-underrättelsefunktion. Med tanke på den vikt som bör läggas vid mänskliga källor i skyddet mot vilseledning blir samverkan med Säkerhetspolisen av särskild vikt.[194]

Även i fallet med skydd mot vilseledning synes ett behov föreligga av en väl fungerande **gränsyta mellan myndighetssfären och den privata sektorn**. Till skillnad mot de IW-relaterade hoten och statistikenheten för att få en uppfattning om omfattning och karaktär av IT-incidenter inom såväl privat som offentlig sektor, skulle detta organ utgöra rapporteringscentral dit misstänkta fall av vilseledning eller misstänkta trender skulle kunna rapporteras. Med hänsyn till ärendenas karaktär vid vilseledning mot försvarsekonomiska intressen synes en nära samverkan mellan organet i gränsytan och Säkerhetspolisen också vara behövlig. Liksom i fallet med IW skulle Näringslivets säkerhetsdelegation (NSD) kunna utgöra gränsytan mellan myndighetssfären och den privata sektorn.

---

[191] Ett statligt s.k. Computer Emergency Response Team.
[192] *Ag IW*, Rapport nummer 2, s. 21-33.
[193] I *Ag IW Rapport 2* (s. 32) skrivs att "Ett effektivt skydd mot informationskrigföring kräver att de funktions- och samordningsansvariga myndigheterna tillförs så bra underrättelsematerial avseende IW-området som är möjligt att få fram. Det kräver också att våra underrättelsemyndigheter inriktas mot att ta fram och leverera material med högre prioritering än vad som sker i dag. Vår underrättelse-/informationsinhämtning etc måste bedrivas på samma sätt som i omvärlden."
[194] Att samverkan mellan MUST och SÄPO är av central betydelse framgår av de tre "historiska" fallen med polska tavelförsäljare, TIR-långtradare och ubåtsjaktverksamheten.

När det gäller en **aktiv kontrollfunktion** av Red Team-modell kan konstateras att ett behov av sådan aktiv kontroll synes föreligga även i fallet vilseledning. Men, de praktiska svårigheterna vid genomförandet av sådan aktiv kontroll (där den kontrollerade parten är omedveten om kontrollen) bedöms vara avsevärda eller t.o.m. oöverstigliga av olika skäl. Samtidigt finns det all anledning att i stället peka på möjligheterna att inom ramen för olika övningar vid såväl Regeringskansliet som totalförsvarsmyndigheterna belysa vilseledning och skydd däremot.

En funktion som motsvarar ett nationellt Computer Emergency Response Team synes knappast föreligga i fallet med vilseledning med hänsyn till den ovan nämnda annorlunda tidsskalan.

En funktion som däremot blir minst lika viktig i fallet vilseledning är den **operativa mediebevakningen** (jfr avsnitt 6.4.4). Den bör omfatta alla medier, inte enbart Internet. Var denna mediebevakning skall placeras kan diskuteras. Ett alternativ är att MUST Sök får ansvaret för denna operativa bevakning. Fördelarna med detta torde vara uppenbara om MUST har det nationella funktionsansvaret.

FRA med sin stora inhämtnings- och analyskapacitet är en annan möjlig placering. På samma sätt som MUST Sök är närheten till underrättelsematerial en stor fördel.

SPF är möjligen mindre lämpligt eftersom denna myndighet har ett mycket tydligt mandat rörande just skydd mot psykologisk påverkan på nationen. Konspiratoriskt tänkande och letande efter vilseledning skulle möjligen riskera att kompromettera SPF:s trovärdighet. Å andra sidan har SPF stor vana av att granska medieflödet.

Ytterligare en annan möjlighet är FOI:s säkerhetspolitiska institution där inte bara långsiktig forskning bedrivs, utan även mer operativ och policyinriktad utredning till stöd för i huvudsak Försvarsdepartementet. Bland annat finns där verksamhet inom området tidig varning (*early warning*).

När det gäller operativ mediebevakning skulle svenska ambassader utomlands kunna bevaka misstänkta fall av vilseledning i respektive målland och regelbundet leverera underlag till det organ som har ansvaret för mediebevakningen.

Oavsett var den operativa mediebevakningen placeras är det viktigt att denna enhet kan samverka med övriga delar av skyddsorganisationen. Mediesignalerna behöver ju jämföras med andra inkommande signaler från UD, MUST, FRA, SÄPO, försvarsindustrin m.fl. aktörer.[195]

[195] Ytterligare en möjlighet som möjligen är värd att beakta är att mediebevakning av enstaka fall (dvs. ej mediebevakning på bredden) sköts av oberoende forskare/utredare med kunskaper om såväl vilseledning som underrättelse- och säkerhetsverksamhet. Med hänsyn till myndigheternas resursmässigt ansträngda arbetssituation kunde detta vara ett kostnadseffektivt alternativ. Dessutom finns redan i dag sådan personal att tillgå. I många fall rör det sig om pensionerade personer som av eget intresse och mot en inte alltför hög ersättning skulle kunna arbeta som fristående konsulter. Ett problem i sammanhanget blir i så fall formerna för dessa personers samverkan med övriga delar av skyddsorganisationen. Värt att notera är dock deras intressanta ställning med hänsyn till egna offensiva åtgärder.

Avslutningsvis är det angeläget att understryka vikten av att en fördjupad analys av ansvarsstrukturen för en eventuell skyddsorganisation görs. Som redan påpekats är ovanstående resonemang att betrakta som högst preliminära reflexioner kring organisationsfrågan. Än mindre har det varit möjligt att inom ramen för denna studie utvärdera olika organisatoriska lösningars skyddseffekt i förhållande till kostnaderna.[196]

6.9 Problem vid skydd mot vilseledning

> *Paradoxically alertness to possible deception increases susceptibility to it.*
>
> Richards J. Heuer[197]

Precis som i fallet med *early warning* finns det inneboende svårigheter förbundna med metoderna för att skydda sig mot vilseledning. I första hand beror detta på den osäkerhet som omgärdar överraskning och vilseledning. På samma sätt som vi varnade för övertro på vilseledningens möjligheter (avsnitt 5.4) finns det anledning att varna för skyddsmetodernas fallgropar. En del av problemen berörsvidare i bilaga 2.

En av de faror som ofta framförs sammanfattas på ett bra sätt av följande citat:

> *Any state's attempt to harness more mundane intelligence assets to the counter-deception problem must be done delicately, for it is probable that attempts to sen-isitize intelligence analysts to the prospects of deception will incline them to find "deception" when it isn't there.*[198]

Som regel räcker det inte för en underrättelseorganisation att ha vaga misstankar om att vilseledning föreligger. Vilseledningsobjektet måste kunna skilja på det som är sant och det som är falskt. Historien uppvisar också fall där vilseledningen har accepterats som sanning samtidigt som sanningen har bedömts vara vilseledning.[199]

Om ett underrättelsesystem görs känsligare för möjligheterna att vilseledning kan förekomma kan också frekvensen falsklarm komma att öka med ett vargen-kommer-syndrom som följd där verklig vilseledning riskerar att avfärdas.

Det kan också leda till en situation där analytikerna p.g.a. att de inte vet vad de kan betrakta som sant sätter upp så rigorösa beviskriterier att det undertrycker intuitionens spelrum (vilket är en viktig del i underrättelseanalysen) eller flödet av underrättelser till beslutsfattarna.[200]

---

[196] En metod att värdera olika skyddsstrukturers effektivitet skulle kunna vara genom spel. Försvarets krigsspelscentrum har tidigare givit ut en rapport om spel och vilseledning (*Vilseledning, desinformation och spel*, Spel för ökad kunskap, FKSC, 1995:06.). (Se vidare kapitel 7 Förslag till fortsatt arbete).
[197] Richards J. Heuer, Jr., "Strategic Deception: A Psychological Perspective", paper presented at the Twenty-first Convention of the International Studies Association, St. Louis, Missouri, mars 1980 citerat i Richard K. Betts, *Surprise Attack*, s. 109.
[198] Katherine L. Herbig och Donald C. Daniel, "Strategic Military Deception" in *Strategic Intelligence: Theory and Application*, (red.) Douglas H. Dearth och R. Thomas Goodden, United States Army War College och Defense Intelligence Agency, andra upplagan, 1995, s. 280.
[199] Ibid., s. 280.
[200] Ibid. s. 280.

Som framgick av kapitel 5 är det människans kognitiva förmågas karaktäristika som möjliggör vilseledning.

För det första verkar tvivlet/osäkerheten alltid till deceptörens fördel. Förutsatt att den vilseledande informationen inte på goda grunder kan avfärdas helt måste den granskas av offret.

För det andra formar de initiala intrycken uppfattningen om efterföljande händelser. Hjärnan arbetar sedan i små och gradvisa (s.k. inkrementella) steg varvid efterkommande intryck jämförs med föregående. Ett utmärkande drag för den mänskliga perceptionsprocessen är sedan motståndet mot att omformulera den initiala bedömningen trots att enskilda efterkommande intryck uppvisar inkonsistenser.

För det tredje förekommer som regel oupplösliga osäkerheter i alla typer av mer komplexa bedömningar utan att desinformation förekommer. Eventuella läckor vid genomförandet av en vilseledningsoperation eller andra felsteg betraktas ofta av offret med samma misstänksamhet som alla andra fakta. Vad som alltså ur deceptörens perspektiv ses som en fatalt misstag betraktas av offret antingen som avsiktlig desinformation (det är för bra för att vara sant) eller som vanlig information behäftad med de sedvanliga osäkerheterna.

Och för det fjärde har deceptören en fördel i det faktum vilseledningen nästan alltid medför kostnader för offret medan kostnaden för deceptören ofta är mycket ringa även om planen misslyckas. Deceptören, som känner sina egna intentioner, kan skilja mellan sanning och lögn vilket offret inte kan göra med säkerhet. Bördan av att reda ut de extra osäkerheter som vilseledningen medför faller därför på offret oavsett om vilseledning sedan accepteras som sanning eller lögn (om inte offret är mycket riskbenäget eller berett att bära vissa kostnader).[201]

Av det ovanstående framgår att vilseledningsobjektet, i sina ansträngningar att skydda sig, står inför en rad svårigheter av organisatorisk, kommunikativ och kognitiv art. Emellertid torde det genom goda kunskaper om dessa svårigheter vara möjligt att eliminera en del av dem samt göra det möjligt att kringgå andra.

För fullständighetens skull bör det samtidigt påpekas att vilseledning är ett riskfyllt företag med inneboende osäkerheter även för deceptören. En vilseledningsoperation kan lätt omintetgöras av olika omständigheter. För det första måste vilseledningsobjektet nås av de vilseledande signalerna. För det andra måste objektet tolka signalerna på det sätt deceptören avser. För det tredje måste objektet agera på ett sätt som verkligen är till fördel för deceptören. I synnerhet den psykologiska perceptionsprocessen och organisatoriska processer hos objektet (objektet utgörs t.ex. av en underrättelsetjänst) gör det svårt att förutse hur objektet kommer att reagera. Andra svårigheter för deceptören sammanhänger t.ex. med sekretess, tidssamordning och integration med andra aktiviteter (jfr avsnitt 3.3 och 5.4).

[201] Ibid. s. 273-274.

7. Förslag till fortsatt arbete

För det fall att Försvarsdepartementet eller någon totalförsvarsmyndighet avser att fortsätta den här beskrivna studieverksamheten lämnar vi nedan ett antal förslag till fortsatt forskningsarbete. Nedan listar vi alltså inte förslag av policytyp då vi anser att förslagen i t.ex. avsnitt 6.8 är tillräckligt tydliga för att Försvarsdepartementet skall kunna gå vidare direkt därifrån.

- Undersöka vad som för närvarande pågår i olika länder när det gäller aspekten skydd mot vilseledning inom ramen för olika program för skydd mot IO.

- Genomföra en kostnads-effekt-analys av organisatoriska aspekter av skyddet mot vilseledning som en del i IW/IO-försvaret.

- Genomföra en pilotstudie under två år med löpande bevakning av misstänkta fall av vilseledning som skisseras i avsnitt 6.4.4.

- Fortsatta studier rörande möjligheter till att avslöja vilseledning utgående ifrån de psykologiska mekanismer som är i funktion vid vilseledning.

- Det vore önskvärt att genomföra en fördjupad analys av de i denna rapport (del 1 och 2) beskrivna fallen av vilseledning utgående från de principer och mekanismer för vilseledning som redovisats i avsnitt 3.3 och kapitel 5.

- Fortsatta studier rörande de aspekter av vilseledning som nämndes i avsnitt 6.4.5.

- Genomgång av svenska arkiv (även sådana som ännu inte är tillgängliga för akademiska forskare) i syfte att, mot ökad kunskap om historiska fall av vilseledning, utvärdera egna tidigare säkerhetspolitiska och andra bedömningar. Ett första fall att fördjupa sig i bör utgöras av *Operation Graffham*.

- Pröva de föreslagna skyddsmetoderna mot verkliga fall av vilseledning. Genom omfattande arkivstudier skulle man möjligen kunna återskapa stora delar av det beslutsunderlag som förelåg under t.ex. *Operation Graffham*.

- Fortsatta studier av hur man kan komma runt eller lindra problemen när det gäller inneboende svårigheter av typen vargen-kommer-syndromet som skydd mot vilseledning (och early warning) tenderar att framkalla. Se avsnitt 6.9.

- Utveckla Furustigs F-modell, som är en modell för diskussion och analys, när det gäller motåtgärder mot vilseledande operationer.

- Påbörja utveckling av egen förmåga till planering och genomförande av vilseledningsoperationer, dvs. som en av flera aktiva motåtgärder inom informationskrigföringsområdet.

- Spel är ett kraftfullt verktyg för såväl analys som utbildning. Genom spelverksamhet skulle olika scenarier kunna utarbetas som exemplifierar tänkbara vilseledningsoperationer mot Sverige (enskilt eller som en del av Västvärlden) eller mot något land i närområdet vilket indirekt får återverkningar på Sverige. Dessa scenarier skulle i ett senare skede kunna utnyttjas för att medvetandegöra och utbilda andra myndigheter och organisationer som kan tänkas delta i det nationella skyddet mot strategisk vilseledning.

  I detta sammanhang kan därför nämnas det arbete som tidigare genomförts av Försvarets krigsspelscentrum (FKSC) avseende spel och vilseledning på nationell nivå. Se "Vilseledning, desinformation och spel", *Spel för Ökad Kunskap*, nr 6 1995.

  En viktig komponent vid spel är scenarier. Vid FOI:s Institutionen för säkerhetspolitik och strategi togs 1999 ett antal scenarier fram för värdering av försvarsmaktsstrukturer.[202] Även om alltså dessa scenarier tagits fram i ett annat syfte skulle de möjligen kunna utnyttjas i samband med vilseledning och nationella spel.

- Undersöka möjligheterna att använda olika typer av datoriserade hjälpmedel för underättelseanalys. Tekniker, för hantering av stora text- och datamängder, som kan analysera informationen både avseende innehåll och relationer till annan information (innehållsanalys resp. nätverksanalys) borde kunna utnyttjas för sökande av avvikelser i makroanalysen eller svaga signaler i samband med skyddet mot vilseledning. Flera sådana datoriserade verktyg används eller studeras för närvarande vid FOI.[203] Ett exempel på ett sådant datoriserat hjälpmedel är SemioMap.[204]

- Rapportens del 1 skulle kunna översättas till engelska. Rapporten skulle på detta sätt kunna utgöra underlag för ett internationellt seminarium till vilket välrenommerade personer inom vilseledningsområdet bjuds in.

- Genomföra ett internationellt seminarium med brett deltagande. Ett antal av de i denna rapport nämnda personerna/referenserna med erfarenhet från det kalla kriget är fortfarande kontaktbara. Till seminariet skulle även den nationella kompetensen avseende vilseledning bjudas in.

---

[202] Bengt Andersson, Niklas Granholm och Johannes Malminen, *Scenarier för värdering av försvarsmaktsstrukturer* (1 bilaga), FOA, HPM från projektet Europeisk säkerhet, 1999-06-04.
[203] En mängd dylika verktyg behandlas i Göran Neiders rapport *Kunskapshantering, konceptstrukturer, textbrytning*, FOA-D-99-00478-111—SE, 1999.
[204] Semio Corporation, Internet http://www.semio.com.

Bilaga 1 Några definitioner av begreppet vilseledning

Genomgången nedan kompletterar texten i avsnitt 3.2.

I *Nomenklatur för Försvarsmakten 1997* (Nomen F 97) definieras vilseledning på följande sätt:

> *Operativ princip som främst innebär åtgärder i syfte att undandra eller vilseleda motståndaren om t ex operativ avsikt, kraftsamling, anfallsriktning eller anfallstidpunkt.*

Därutöver finns i *Nomen F 97* en definition av vilseledning inom ledningskrigföring:

> *Militärt planerade åtgärder som syftar till att ge motståndarens ledare en falsk bild av vår militära förmåga och/eller våra avsikter i syfte att få fienden att agera på ett för oss gynnsamt sätt.*

Arméledningsstudie 6 Vilseledning 1995-97 (även kallad *Arméns vilseledningsstudie*) antog följande definition:

> *Med vilseledning avses medvetna åtgärder som syftar till att ge motståndaren ett felaktigt beslutsunderlag för att få honom att disponera sina resurser på ett sätt som gynnar vår strid.*[205]

Hans Furustig redovisar i FOA-rapporten *Militär vilseledning – Några grunder*[206] ett antal utländska definitioner. NATO definierade 1985 vilseledning som

> *Åtgärder som vidtagits för att missleda fienden genom manipulering, förvrängning eller förfalskning av fakta för att förmå honom att agera på ett sätt som är till men för hans intressen.*

Det amerikanska fältreglementet *FM 90-2 Battlefield Deception* från 1988 menar att

> *Vilseledning på stridsfältet består av operationer under ledning av echelongnivå och lägre, för att avsiktligt vilseleda fiendens beslutsfattare genom att förvränga, dölja eller förfalska indikatorer på egna eller allierades avsikter, kapacitet eller dispositioner.*

Med sovjetisk maskirovka (maskering, döljande, vilseledning) menas

> *Döljande av egna och allierades styrkor och militära installationer från fienden. Maskering används för att vilseleda fienden om styrkornas läge, verksamhet och avsikt. Maskering är en stridsmässig säkerhetsåtgärd under strid eller operation och dessutom en åtgärd för det lokala luftförsvaret.*

Enligt den sovjetiska militärencyklopedin (1964) är maskirovka

---

[205] Denna definition är också den som används av Hans Furustig i *Militär vilseeldning—Några grunder*, bilaga 1. Denna definition antogs sedermera av Försvarsmaktens *Huvudstudie Ledningskrigföring* med vissa smärre modifieringar och föreslogs gälla för det fortsatta arbetet inom området.
[206] Hans Furustig, *Militär vilseledning*, bilaga 1.

Konsten att säkerställa framgång i strid, bestående av ett komplex av åtgärder för att vilseleda avseende läge och stridsvärde hos förband och objekt och stridsplaner...[207]

I den sovjetiska militärencyklopedin *Vojennyj Entsiklopeditjeskij Slovar* från 1984 definieras maskirovka på följande sätt:[208]

Ett komplex av åtgärder för att vilseleda motståndaren vad gäller förekomst och gruppering av egna stridskrafter, militära objekt (mål), deras tillstånd, stridsberedskap och verksamhet samt även vad gäller ledningens planer. Maskirovka ingår i handlingsmönstret för att säkerställa operativ och taktisk förmåga. Maskirovka bidrar till att uppnå överraskning, bevarar stridskrafternas beredskap och ökar deras uthållighet. Efter tillämpningarnas omfattning och uppgifternas karaktär skiljer man mellan strategisk, operativ och taktisk maskirovka. Beroende av mot vilka underrättelsemedel som den riktas mot talar man om hydroakustisk, ljud- eller akustisk, magnetisk, optoelektronisk, radioaktiv strålnings-, radar-, radionavigerings- och målsöknings-/-styrnings etc maskirovka. Den största effekten uppnås vid samtidigt utnyttjande av maskirovka mot fiendens alla underrättelsemedel. Maskirovka genomförs oavbrutet vid alla slags verksamhet hos stridskrafterna. Huvuddelar av maskirovka är döljande och demonstrativ verksamhet, simulering, desinformation.

Strategisk maskirovka i sin tur definieras enligt samma källa på följande sätt:

Strategisk maskirovka genomförs efter beslut av högsta ledningen och omfattar ett komplex av åtgärder för att hemlighålla förberedelser för strategiska operationer och fälttåg samt även för vilseledning av motståndaren vad gäller stridskrafternas gruppering, tillstånd och planer. Strategisk maskirovka planeras och organiseras av generalstaben.

Operativ maskirovka genomförs som demonstrativ verksamhet, simulering av truppkoncentrationer, av grupperingar av förband och andra militära objekt, desinformation beträffande egna stridskrafters tillstånd och karaktären av deras förestående verksamhet. Operativ maskirovka sker vid förberedelse för och genomförande av operationer. Operativ maskirovka planeras och organiseras av frontstab (militärområde, flotta) på grundval av beslut om operation.

Taktisk maskirovka syftar till att dölja grupperingsplatser och förflyttningar av egna förband, raket- och artilleriförbandens eldpositioner, ledningscentraler och andra viktiga objekt med utnyttjande av omgivningens maskeringsmöjligheter, sikt- och synbarhetsvillkor, maskeringshjälpmedel av olika slag samt även genom utnyttjande av falska positioner och grupperingsområden. Taktisk maskirovka verkställs, enligt beslut av taktisk chef (divisions-, regements-, bataljonschef), av all personal utan någon som helst anvisning.

Som maskeringshjälpmedel används maskeringskläder, täckta skydd (maski), atrapper för militär materiel, radarreflektorer, radarabsorberande yttäckning, medel för mörkläggning, värmeskärmar, elektronisk störning, rök, färgmedel etc.

---

[207] Lars Ulfving, *Den stora maskeraden—Sovjetrysk militär vilseledning*, s. 63.
[208] Översättningen är tagen från Per-Olov Nilsson, *Teknisk utveckling i Öst och Väst*, FOA-rapport C10299-1.1, november 1987, bilaga 2.

> *Döljande verksamhet (skrytije) innebär undanröjande eller försvagande av för stridskrafternas och även för enskilda objekts gruppering och verksamhet avslöjande kännetecken. Det uppnås genom iakttagande av "maskirovka-disciplin" och krav på icke röjande ledningsverksamhet, vaksamhet hos personalen, utspridd gruppering av förband och tross, växling av grupperingsplatser, klokt utnyttjande av terrängen, maskeringshjälpmedel m.m.*
>
> *Demonstrativ verksamhet (demonstrativnyje dejstvija) innebär militär och annan verksamhet hos stridskrafterna med mål att vilseleda motståndaren rörande karaktären av förestående stridsverksamhet, anfallets huvudriktning (koncentreringsområdet för den militära insatsen) och avleda hans stridskrafter mot en för egen sida fördelaktig riktning. Verksamheten ingår i planering på operativ (strategisk) nivå och genomförs tillsammans med döljande åtgärder, simulering och desinformation.*
>
> *Simulering (imitatsija) genomförs med olika simuleringshjälpmedel t.ex. skenanläggningar, atrapper för militär materiel, lösa skott, pyroteknik, ljus- och ljudimitationer, rök m.m. Simulering sker i kombination med övriga slag av maskirovka.*
>
> *Desinformation (dezinformatsija) ingår i operativ (strategisk) maskirovka och består i avsiktlig spridning av falsk information om egna stridskrafter, deras gruppering, sammansättning, beväpning, stridsförmåga, planer för stridsverksamhet osv. med mål att missleda motståndaren. För desinformation utnyttjas sambandsmedel, tryckta alster, radiosändning, TV m.m. Desinformation kombineras med demonstrativ verksamhet, simulering och döljande verksamhet.*

Enligt en senare sovjetisk encyklopedisk militär uppslagsbok är maskirovka

> *Ett komplex av åtgärder för att vilseföra motståndaren avseende förekomst och gruppering av styrkor, militära installationer, deras tillstånd, stridsberedskap och verksamhet, samt ledningens planer/avsikter.*[209]

Där definieras även vad som avses med strategisk, operativ respektive taktisk maskirovka.

Furustig definierar också vilseledning (allmänt, till skillnad från militär dito) som

> *Avsiktligt spridande av falsk eller missvisande information för att förvränga mottagarens verklighetsbild i avsikt att uppnå egen fördel eller för att skada motpartens intresse.*

Oavsett att ovan anförda definitioner ofta hänför sig till det militära området framträder tydligt bilden av hur vilseledning och maskirovka genomförs, nämligen som en kombination av framhävande och döljande åtgärder i syfte att vilseleda en eller flera aktörer avseende den egna förmågan och den egna avsikten. Resonemanget kan överföras till andra områden såsom t.ex. det politiska eller ekonomiska.

[209] *Vojennyj entsiklopeditjeskij slovar*, Moskva, 1986, andra upplagan, s. 429.

Bilaga 2 Alternativa analytiska förhållningssätt

Följande framställning är en bearbetning ur ett vilseledningsperspektiv grundad på Hans Furustigs rapporter om vilseledning samt kapitel 2 i Hans Furustigs och Gunnar Sjöstedts lärobok *Strategisk omvärldsanalys*.[210]

Strukturering av problemet

Vilseledning syftar ytterst till att påverka motståndarens agerande genom att manipulera beslut och beslutsunderlag. Denna påverkan kanaliseras antingen direkt mot beslutscentrum och nyckelfunktioner eller indirekt mot inflytelserika opinioner alternativt genom ledtrådar, spår och olika kanaler för exponering av tillrättalagd information som ska "upptäckas" av motståndarens underrättelseverksamhet.

Metodmässigt är det skillnad mellan å ena sidan hantering av *fakta* – exempelvis att upptäcka, beskriva och förstå vad som faktiskt händer – och å andra sidan bedömning av *avsikter* – exempelvis att förutsäga alternativa samtida eller framtida händelseutvecklingar. Fakta kan bestå av dokumenterade officiella beslut och planer, mätning av kapacitet och prestanda, samt observation eller registrering av genomförda handlingar. Med avsikter menas här återspeglingar av motståndarnas strategiska och operativa planer, oftast fördolda eller flertydiga, eller av attityder som på olika sätt, medvetet eller omedvetet, *signalerats* till omgivningen. Det är en analytisk svårighet redan att på ett korrekt sätt beskriva, förstå och förutsäga faktiska händelseförlopp och sannolika utvecklingar. Till denna uppgift överlagras möjligheten att motståndaren aktivt och med vilseledande operationer försöker förändra utvecklingen till sin fördel. Beslut och planer kan vara missvisande, kapacitet skenbar och handlingar diversionsmanövrer. Det innebär att beslutsfattare och analytiker behöver ta ställning till om, och i så fall hur, *osäkerheten* i en analyssituation eller beslutssituation ska hanteras.

De "system" och aktörer som analytikern undersöker och bedömer kallas här nedan för "undersökningsobjektet". För diskussionen antas att analytikern har tre förhållningssätt att välja mellan, beroende av undersökningsobjektets karakteristika (passivt, reaktivt eller aktivt).

(1). Undersökningsobjektet är i huvudsak *passivt*, dvs. det svarar på olika utspel och handlingar, men tar få "egna" initiativ. Ett exempel där denna tolkning kan vara relevant är ekologiska system som i ett visst ögonblick kan betraktas vara i balans, men där människans ingrepp och olika naturkatastrofer förorsakar avvikelser från ett normalmönster (anomalier) och därmed ger upphov till svarsreaktioner från det ekologiska systemet. (Spel mot naturen).

Analytikerns förhållningsätt bestäms av att undersökningsobjektet i stort sätt kan beskrivas med hjälp av observerbara och mätbara faktiska förhållanden. Osäkerheten kommer in i bilden genom kunskapsbrister avseende sakförhållanden och genom den osäkra efterlevanden av mänskliga avtal och lagar.

De motåtgärder som kan vidtas är satsning på kunskapsuppbyggnad, effektivare regelverk och kontrollmekanismer, samt preventiva skyddsåtgärder mot undersökningsobjektets agerande.

(2). Undersökningsobjektet är *reaktivt*, i betydelsen att däri finns aktörer som löpande tar egna initiativ inom ramen för ett relativt snävt handlingsutrymme. Exempel på en sådan situation är en förhandling mellan olika parter eller en normal konkurrenssituation mellan företag. Det är i denna situation möjligt att bli överraskad av motparten genom dennes skickliga agerande, eller

[210] Hans Furustig och Gunnar Sjöstedt, *Strategisk omvärldsanalys* (Studentlitteratur, 2000).

genom förutfattade meningar och underskattning av motparten. Det är således möjligt att bli överraskad av andra orsaker än renodlad vilseledning! Vilseledning uppfattas i denna kontext som ett osannolikt agerande på grund av de negativa konsekvenserna av ett avslöjande i form av badwill och eventuell formell bestraffning. Manipulering av beslutsunderlag inom ramen för en legal gråzon kan dock inte uteslutas om den förväntade belöningen är tillräckligt hög.

Analytikerns förhållningssätt påverkas av att undersökningsobjektets aktörer har *egenintressen*, de initierar egna speldrag. Osäkerheten består principiellt i att motpartens avsikter inte är kända, även om dennes totala resurser kan vara kartlagda, liksom spelreglerna som är allmänt vedertagna. Även den pågående systemförändringen innebär en osäkerhet till sin grundläggande karaktär. Leder den till revolutionära förändringar, exempelvis överraskande teknologiska språng, eller kommer den att förlöpa evolutionärt, dvs. inom ramen för trendframskrivningar och överraskningsfria prognoser?

Överraskning i detta sammanhang får ekonomiska konsekvenser varför ett strategisk förhållningssätt med syfte att minska sannolikheten för negativa utfall är att genomföra löpande hotbildsanalyser, riskvärderingar och säkerhetsrevisioner. Åtgärder vidtas sedan för att skydda värdefull information och egen verksamhet. (Spel mot konkurrenter. Observera att det inte behöver vara ett "nollsummespel").

(3). Undersökningsobjektet uppfattas som *aktivt* i en situation som kännetecknas av hård konkurrens, kris och krig. Dess aktörer planerar och genomför egna initativ och motåtgärder, varvid konventioner, lagar och regler kan komma att åsidosättas beroende av situationen. Konkurrenters och angripares metoder förknippas med informationsoperationer, informationskrigföring och ledningskrigföring. Det innebär att motparten med avsikt vilseleder eller agerar på andra sätt för att uppnå sina syften, även om det innebär att avvika från vad som normalt betraktas som "spelets regler". Det ovanstående kan innebära att analytikern inte säkert kan lita på erhållna underrättelser. (Spel mot motståndare. Observera att inte heller detta behöver vara ett "nollsummespel").

Förutom att motståndarens aktiva agerande är en väsentlig osäkerhetsfaktor tillkommer det förhållandet att en konflikt eller kris kan utvecklas och kontrolleras inom ett begränsat område, exempelvis handel eller industriell konkurrens, medan utvecklingen inom andra områden kan uppvisa helt annorlunda mönster, exempelvis inom internationell säkerhetspolitik. Det är möjligt för säkerhetspolitiskt goda allierade att hamna i hård teknisk-vetenskaplig konkurrens och kontrollerad handelsekonomisk konflikt, utan att krisen med naturnödvändighet måste sprida sig till andra områden. Det är således inte uppenbart på vilken spelplan och med vilken konstellation av pjäser som en kris eller konflikt kan komma att utspela sig. Av t.ex. Säkerhetspolisens årsberättelse 1999 framgår att

> *När det gäller ekonomisk inhämtning och industrispionage – kategorier som skulle kunna kallas underrättelsevärldens "svarta får" – är det dock tydligt att det inte existerar några vänner eller allierade.*[211]

Ett handlingssätt vore att förtränga att motparten kan vilseleda eller på andra sätt avvika från "spelreglerna" och i linje därmed avstå från kanske kostsamma motåtgärder i olika konstellationer (förebyggande eller efterhjälpande). Konsekvensen av att bli överraskad på grund av motståndarens vilseledning eller annan manipulation kan emellertid vara förödande och utgör ett argument för att genomföra ett lämpligt kombinat av passiva och aktiva metoder för att reducera eller motverka detta hot.

[211] *SÄPO Verksamhetsåret 1999*, (Säkerhetspolisen, mars 2000), s. 17.

Frågeställningar

De grundläggande frågeställningar som väcks av detta resonemang är i vilka situationer som avsiktlig vilseledning kan förväntas och vilka åtgärder som därvid kan vidtas. En principiell delfråga är huruvida enskilda analytiker och beslutsfattare bör förhålla sig på något särskilt sätt när vilseledning kan förväntas, eller om de kan förhålla sig och agera på samma sätt som om vilseledning inte förekommer, därför att de förlitar sig på att särskilda aktörer återför situationen till normala premisser?

Detta korta resonemang leder till några frågeställningar, som kortfattat diskuteras nedan och som bör utvecklas närmare för att det ska vara möjligt att ta ställning till och hantera vilseledning på ett rationellt och systematiskt sätt.

- Är det möjligt att förutse vilseledningsoperationer?
- Är det möjligt att upptäcka vilseledningsoperationer?
- Är det någon skillnad på förhållningssätt och metoder för att analysera omvärldsutveckling utan vilseledning till skillnad från omvärldsutveckling med vilseledning?
- Finns det konkreta exempel på metoder för att motverka vilseledning?

Att förutse

Finns det någon aktör eller part som skulle kunna tänkas initiera och driva en intressekonflikt till sin spets om syftet inte kan uppnås på annat sätt? I så fall uppstår frågan om denna aktör också har *förmåga* (kapacitet, resurser) att verkligen genomföra någon form av fientlig operation. Om det inte är fallet uppstår frågan om det kan finnas någon kombination av aktörer (extremister, internationell organiserad brottslighet, storföretag, stater) som i gemensamt intresse skulle kunna ha resurser och motiv att samordnat genomföra fientliga operationer. Om inte heller detta är sannolikt kvarstår frågan om det är tillräckligt att ha resurser men sakna kända motiv eller att ha motiv men sakna kända resurser för att genomföra en fientlig operation för att detta ska uppfattas som ett hot. Ett hot är som bekant ett möjligt scenario med negativa konsekvenser. Om hotbilden visar sig vara svag kanske det vore bättre att satsa resurser på egna positiva möjligheter att agera.

Ett sätt att försöka förutse en konkurrents eller motparts intentioner är att ikläda sig motståndarens glasögon och se situationen från dennes perspektiv. Har motparten något strategiskt intresse av att driva en intressekonflikt i dagsläget eller i en överblickbar framtid? I så fall, vilka är den egna sidans svagheter? Kan motparten utnyttja dessa? Vad är sannolikheten för motpartens framgång och vilka blir i så fall konsekvenserna för egen sida? Kan denna risk accepteras? Bedömningen kan genomföras med olika metoder, exempelvis i form av spel mellan olika lag (A/B-team).

Som komplement kan en form av riskvärdering genomföras. Relevanta faktorer av nedanstående typ kan kombineras i en flerdimensionell matris (figur 11) i vilken varje cell bedöms avseende sannolikhet och konsekvens. Endast vissa celler torde representera intressanta utfall.

Det är naturligtvis skillnad mellan att göra bedömningar i realtid (nulägesanalys) för att skapa handlingsunderlag här och nu och att göra förhandsbedömningar av framtida utveckling (hotbildsanalys) för att möjliggöra handlingsberedskap och framförhållning.
Huvudmotståndarens eller konkurrentens officiella avsikt kan utläsas från val av medarbetare, genom analys av tal, dokument och handlingar av olika slag. Denna typ av signaler behöver emellertid inte vara rättvisande, det är inte ovanligt att mentala potemkinkulisser förevisas för omgivningen. Det är den *dolda agendan* som är avgörande. För att tränga djupare in i motpar-

tens agenda behövs personkännedom, exempelvis genom psykologiska profiler, och i synnerhet genom välplacerade rapportörer.

Motpart	Situation	Spelplan	Metoder
Passiv	Fredlig	Teknologi	Juridiska
Reaktiv	Hård konkurrens	Ekonomi	Ekonomiska
Aktiv	Krisartad	Handel	Psykologiska
	Lågintensiv konflikt	Diplomati	Vilseledande
	Begränsat krig	Internet	Fysiska
	Fullskaligt krig	Andra slagfält...	Etc...

Fig. 11. Idémässigt underlag för en inledande riskvärdering.

Ett principiellt annorlunda sätt att få vetskap om motståndarens avsikter är att kontrollera dennes agerande, genom att påverka och styra. Motståndaren lockas (belönas, tvingas) att vidta åtgärder eller att fatta beslut.

Ytterligare ett sätt är att försätta motparten i testsituationer, dvs. att på prov göra olika utspel som motparten måste svara på. Dessa utspel kan i sig vara oskyldiga, men det sammanvägda ställningstagandet till dem kan avslöja motpartens djupare agenda. Detta innebär principiellt att analys och agerande blandas samman.

Upptäcka

Om analys visar att någon aktör har kapacitet för eller motiv till att i fientligt syfte genomföra en vilseledningsoperation (informationsoperation, etc.) uppstår frågan hur en eventuell aktion ska kunna upptäckas på ett tidigt stadium. Det är givetvis önskvärt att om möjligt erhålla *förvarning* om att något kan komma att ske. Förvarningen baseras därvid på en eller flera indikatorer. För att det ska vara någon mening med förvarning måste den erhållas med sådan framförhållning att mottagaren har möjlighet att vidta erforderliga åtgärder i tid.

Om det exempelvis finns någon form av riktad misstanke avseende modus operandi, mot ett geografiskt område eller mot vissa aktörer kan det vara möjligt att identifiera en lämplig *indikator*. En indikator används i syfte att påvisa något, i det här fallet en fientlig vilseledningsoperation. För att öka känsligheten och förvarningstiden kan olika indikatorer kombineras. Avvikelser från en normalbild, anomalier, kan vara ett tecken på att något håller på att hända. Allmänna krav som kan ställas på en indikator är exempelvis:

- relevans
- otvetydighet
- tillförlitlighet
- aktualitet
- tillgänglighet
- kommunicerbarhet

Om avsikten är att erhålla varningssignaler för att indikera vilseledning och inte bara fientliga operationer i största allmänhet, tillkommer några svårigheter. Information som kan avslöja vilseledning kan döljas i ökat bakgrundsbrus, undertryckande av avslöjande signaler och framhä-

vande av falska signaler. Erfarenheten visar att organisatoriska låsningar och förutfattade meningar om motståndaren och vilken typ av åtgärder som förväntas från denne kan försvåra möjligheterna att upptäcka anomalier, samt försena analys och bedömning. Svårigheten ligger i att kombinera ett öppet sinne med en kritisk och granskande attityd.

Under normala säkerhetspolitiska faser och fredliga konkurrensförhållanden kan det vara svårt att särskilja vaga indikationer från bakgrundsbrus, "the fog of peace". Genom att laborera med kriterienivåerna för varning, exempelvis genom att öka känsligheten erhålls fler "träffar", men också fler "falsklarm". Genom att minska känsligheten erhålls färre "falsklarm", men också fler "missar".

Ett sätt att upptäcka vilseledning inom ett visst tillämpningsområde kan vara att studera hur *förändringar* normalt äger rum inom detta område. Det gäller inte bara förändringar i en normalbild, utan även förändringar i ett förändringsmönster! Enbart förändringar i sig är emellertid ett tveksamt urvalskriterium för vilseledning, särskilt inom områden som naturligt kännetecknas av snabb expansion (revolutionär utveckling). Indikatorer bör grunda sig på något, exempelvis relevant teoribildning eller beprövad erfarenhet.

Metodmässigt förhållningssätt

Att lösa problem och att skapa beslutsunderlag i samband med hantering av vilseledning innebär att syftet är behovsstyrt och inriktningen är systemspecifik. En jämförelse mellan olika förhållningssätt görs nedan.

Visserligen skiljer sig de olika ansatserna i figur 12 från varandra både i syfte och metodarsenal, men underrättelseverksamheten förenar viktiga aspekter ur de olika förhållningssätten. Antingen testas formella hypoteser eller så besvaras preciserade frågeställningar. Datorstöd och källkritik är viktiga element i arbetsmetoden. Analysverksamheten leder fram till ett beslutsunderlag, ett s.k. bedömande. Tidsperspektivet kan vara både nulägesorienterat och framtidsinriktat. Vid identifiering och motverkan av vilseledning är det viktigt att känna till tillvägagångssättet vid planering och genomförande av en vilseledningsoperation. Detta diskuterades i avsnitt 3.3, 3.5-3.6 och kapitel 5.

Underrättelseverksamhetens metodarsenal är användbar vid behandling av vilseledningsoperationer och omvänt är underrättelseverksamheten målobjekt vid angrepp i samband med vilseledningsoperationer.

En gemensam förutsättning för forskning och underrättelseverksamhet är kritisk attityd och kunskap om källkritik. Falsk eller tvivelaktig information låter ofta avslöja sig genom olika ledtrådar. Den kan uppvisa bristande konsistens i logiken, strida mot kända förhållanden eller enbart grunda sig på osäkra källor och sådant som inte kan undersökas närmare. Den som ska bedöma information måste bl.a. granska följande aspekter:

- frågeställningens krav
- källans tillförlitlighet (reliabilitet)
- innehållets sakriktighet (validitet)
- budskapets angelägenhetsgrad
- budskapets tillkomsthistoria

Principiell ansats	Karakteristika
Akademisk verksamhet med höga krav på validitet och reliabilitet.	Ackumulering av kunskap. Generella lösningar. Hypotestestning. Logisk analys. Källkritik. Statistisk analys.
Utredningsverksamhet med höga krav på Användbarhet och relevans.	Systemspecifika lösningar. Operationsanalys. Systemanalys. Datorstödd simulering och kalkyl.
Underrättelseverksamhet med höga krav på användbarhet, aktualitet, relevans och sakriktighet.	Specifika situationsberoende lösningar. Underrättelsecykeln. Källkritik. Datorstödd inhämtning och bearbetning.
Bedömandeverksamhet med höga krav på att bereda och ta beslut i tid.	Inriktning Ad Hoc. Systemspecifikt. Nulägesorienterat. Erfarenhet och praxis.
Studieverksamhet med höga krav på strukturering av framtida hot och möjligheter.	Inriktning mot långsiktiga prognoser. Framtidsstudiemetodik. Spelmetodik. Simuleringsmetodik. S.k. lateralt tänkande.

Fig. 12. Exempel på några olika förhållningssätt till problemlösning.

Dessa aspekter behöver förtydligas. Det är här endast möjligt att göra några korta tillägg. Beträffande frågeställningens krav gäller att en förfalskning kan ha värde som dokumentation av en vilseledningsoperation, men samtidigt vara värdelös som ett historiskt dokument med pretentionen att avbilda ett verkligt skeende. En källas äkthet kan undersökas med olika tekniska och analytiska metoder. En källa och den kanal som överför budskapet kan bl.a. bedömas utifrån tidigare felfrekvens och propagandistisk tendens. Är sagesmannen kompetent inom sakområdet? Återges egna observationer eller finns mer primära källor? Närhet i tid till händelserna? Exceptionella uppgifter bör granskas särskilt, oavsett vilket rykte källan har. Varför blir innehållet tillgängligt just nu? Timing? Är budskapet viktigt och analysen i behov av särskild prioritering? Är innehållet i linje med kända förhållanden och är det logiskt konsistent? Är innehållet tendentiöst? Vad saknas? Är materialet relevant? Behöver materialet kompletteras?

Bilaga 3 Analys av svaga signaler

Att tidigt kunna upptäcka (detektera), identifiera och bedöma svaga signaler kan vara av avgörande betydelse för exempelvis individens hälsa, ekosystemets tillstånd, organisationens utveckling eller statens överlevnad. Svaga signaler kan utgöra ett hot, en möjlighet eller helt enkelt vara irrelevanta. De karakteriseras av att vara svåra att särskilja från omgivningens brus, störningar och andra konkurrerande signaler. Det är av ekonomiska respektive säkerhetspolitiska orsaker väsentligt att kunna hantera svaga signaler i olika sammanhang, inte minst för att erhålla tillräcklig förvarning och för att undvika överraskning. Därför behövs studier av och kunskapsuppbyggnad inom området "svaga signaler".

Med signal menas i detta sammanhang en representation av en observerad eller uppmätt del av verkligheten. Denna representation kan vara sann, missvisande eller falsk i förhållande till det som den avbildar. Att signalen är falsk innebär att en aktör, i syfte att skapa osäkerhet eller för att försvåra, fördröja eller degradera en bedömning eller ett beslut, avsiktligt manipulerar verklighetsbilden genom vilseledande verksamhet. Det kan ske exempelvis genom att undertrycka sann information, genom att tillföra ett överskott av information som skapar osäkerhet eller genom att fördröja tillgången till relevant information för att försämra underlagets kvalitet. Att representationen är missvisande innebär att den oavsiktligt är mångtydig eller förledande. Det kan leda till felaktiga beslut och insatser. En pilot som flyger i moln kan bli osäker på sin orientering. Om omvärldsrepresentationen är oklar eller i strid med hans intuition eller normala praxis kan han helt oavsiktligt förledas att agera felaktigt, exempelvis genom att ta fel på riktningen upp eller ned. Den missvisande representationen kan vara korrekt men svag, vilket innebär att mottagaren riskerar att inte uppmärksamma den i tid, eller inte förmå tolka den korrekt.

Att vi fokuserar mot *svaga* signaler kräver en liten utredning. Varför just svaga? Det skulle väl kunna tänkas att *tidiga* signaler vore lika intressanta. Dessutom, om intresset fokuseras mot exempelvis avsiktlig vilseledning från en konkurrent eller motståndare, kanske *starka* signaler vore en mer adekvat inriktning? Den som avser att luras vill naturligtvis vara säker på att vilseförande signaler verkligen uppfattas, alltså måste de vara relativt sett starka. Emellertid genereras svaga signaler oavsiktligt genom läckor, i samband med att vilseledning planeras och genomförs, trots eventuella försök till sekretess och döljande åtgärder. Den som exempelvis vill kunna avslöja vilseledning försöker upptäcka motsvarande signaler så tidigt som möjligt, vilket motiverar intresset för *svaga* och *tidiga* relevanta signaler. Samtidigt föreligger här ett moment 22. En motståndare kan mycket väl producera svaga signaler i syfte att lura motparten att förbruka sina resurser på analys av svaga och i detta fall irrelevanta signaler. Dessutom är problembilden i samband med hot och möjligheter ofta diffus, dvs. även *sambanden* mellan de svaga signalerna är sannolikt vaga i sig. Sammantaget leder detta resonemang till att vi väljer den förkortade benämningen svaga signaler, "weak signal research", som är en vedertagen benämning.

Emellertid bör denna diskussion inte hårddras. Betrakta exempelvis Hitlers "Mein Kampf". Bokens innehåll ger en ganska god bild av vad Hitler eftersträvade. Den utgjorde med tanke på sina avsiktsdeklarationer en stark signal (i varje fall för nutida läsare). Trots detta tolkades den inte, som vi har uppfattat det, på ett korrekt sätt av den tidens bedömare, kanske beroende på att den förvirrande ekonomiska och politiska turbulens som då rådde försvagade signalens dåtida relativa styrka (normalbilden var oklar). Det var också en tidig signal i förhållande till Hitlers politiska utspel. Hitler var vid publiceringen visserligen inte en etablerad politiker, men boken fanns tillgänglig för dåtidens analytiker och beslutsfattare, när han under 1930-talet blivit ledare för det nationalsocialistiska partiet.

Det väsentliga är inte att ge en snäv definition på svaga eller tidiga signaler, då det egentliga syftet med undersökningen därvid riskerar att definieras bort.

Det gäller helt enkelt att tidigt upptäcka och värdera *kritiska signaler* avseende relevans, autenticitet och aktualitet för att därmed skapa handlingsfrihet för beslut om åtgärd/motåtgärd.

Framställningen här är idémässig, konceptuell och tvärvetenskaplig. Den utgör en utgångspunkt för fortsatt studieverksamhet. Tekniska aspekter (signaltransmission, dekryptering och kryptering), biologisk systemteori och ansatser som härstammar från fysiken (informationsteori) behandlas inte närmare. Följande praktiska frågeställningar behöver fortsatt konkret behandling:

- Hur upptäcka svaga signaler?
- Hur identifiera svaga signaler?
- Hur bedöma svaga signaler?
- Hur hantera möjligheten av vilseledning vid hantering av svaga signaler?

Exempel på svaga signaler

Diffusa miljöförändringar kan förebåda omstörtande tekniska och sociala förändringar. Företaget Facit, som var en framgångsrik tillverkare av mekaniska kontorsmaskiner, överraskades av de elektromagnetiska (räknare, skrivmaskiner) och elektroniska (ordbehandlare, räknedosor) hjälpmedlens intrång på maknaden, liksom företaget Keuffler & Esser, som tidigare med framgång tillverkat manuella räknestickor. Utvecklingen av idéer till tekniska innovationer, nya produkter och förändrade behov representerar ett nätverk av ledtrådar i form av svaga signaler som efterhand växer till irreversibla faktiska förhållanden. I början förelåg rimligen en potentiell möjlighet för Facit och Keuffler & Esser att uppmärksamma och agera på utvecklingen. Efter en tid var denna möjlighet tydligen överspelad och det uppstod i stället ett påtagligt och övermäktigt ekonomiskt hot från nya framgångsrika konkurrenter. Signalerna blev överstarka och irreversibla. De här nämnda företagen är i gott sällskap, vilket beror på att problemet att tidigt identifiera, tolka och svara på svaga signaler är mycket svårt, i synnerhet om konkurrenterna gör sitt bästa för att förvirra varandra. Exemplet visar att de ekonomiska insatserna kan vara mycket höga: ett företags fortlevnad kan till och med stå på spel. Motsvarande resonemang gäller även för en stat i spelet mellan handelsblock och konkurrerande stater om begränsade resurser.

Ett annat exempel kan hämtas från kategorin militära anfallsförberedelser. Angriparen försöker i det längsta att dölja indikationer på sina avsikter, t.ex. upprustning, inkallelser, kraftkoncentration och uppmarsch genom maskering och skenverksamhet. När det inte längre går att dölja verksamheten gäller det att bjuda offret någon form av bete, som medger (bort)förklaringar och som skapar beslutsångest. Det gäller därför för ett tilltänkt offer att tidigt uppmärksamma vaga avvikelser från ett politiskt, ekonomiskt och militärt normalmönster. Efterhand som tiden går minskar nämligen handlingsfriheten och kostnaden ökar. Angriparen tillgriper avsiktlig vilseledning mot offret, vilket försvårar både identifiering och tolkning av svaga signaler och efterföljande bedömning. Även i detta exempel är insatserna höga; en stats strategiska intressen och oberoende kan i extremfall stå på spel om de svaga signalerna inte hanteras adekvat.

Antag att en patient söker läkare för diffusa symptom. Läkaren har då att göra en anamnes, varvid olika svaga signaler måste uppmärksammas och tolkas. Ett svårt fall inträffar då signalerna är nya och okända eller då olika sjukdomstillstånd har samma indikationer och således kan feltolkas. Motsvarande resonemang är tillämpligt på diagnosticering av problemföretag och för den delen även tekniska system. Ur teoretisk synpunkt är uppgiften att söka och svara på svaga signaler, typ felindikationer.

Andra exempel på indikering och analys av svaga signaler är de pågående klimatstudierna, strävan efter att finna relevanta signaler för att förutsäga naturkatastrofer typ jordbävningar (ett avskräckande exempel är domedagssekternas undergångscenarier grundade på irrelevanta signaler), behovet att tidigt identifiera tecken på kommande katastrofer i syfte att förbereda internationella hjälpinsatser eller tecken på utökning av den organiserade brottslighetens verksamhet. Uppgifterna underlättas inte av att det kan råda oklarhet om vad som konstituerar goda kriterier och indikatorer, oavsett om signalerna är svaga eller ej. Det är stora värden som står på spel.

Med facit i hand borde det vara möjligt att bedriva forskning rörande förekomst av och förståelse för (svaga) signaler. Vilka lärdomar kan hämtas för framtiden när det gäller exempelvis klimatstudierna, Sovjetunionens sammanbrott, utbrottet av "galna kosjukan", den japanska AUM-sektens ökade användning av terrorliknande metoder, inkl. (N)BC-användning eller al-Qaidas utveckling till ett säkerhetspolitiskt hot mot den civiliserade världen? Förelåg det några "svaga signaler" som hade kunnat ge omgivningen någon förvarning?

Problemanalys

En svag signal kan tills vidare tolkas som information som är svår att upptäcka och identifiera på grund av förekomsten av andra signaler, störningar och brus i det berörda systemet. En signal kan vara svag, inte enbart därför att den har låg amplitud (styrka) i förhållande till andra signaler, utan även därför att den enbart inträffar vid sällsynta tillfällen (låg frekvens, enstaka händelser), att den byggs upp extremt långsamt (tillvänjningseffekt) eller snabbt (språngvis) eller därför att den genom att manifesteras på ett speciellt och ovanligt sätt helt enkelt är fysiskt eller kognitivt svår att uppfatta av tillgängliga sensorer eller observatörer. Någon mer strikt definition på "svag signal" kommer inte att ges här.

Antag att någon sändare initialt avger svaga signaler och att dessa efter en tid växer i styrka, antal och frekvens, så att de för en observatör övergår från att vara diffusa och svaga till att bli starka. När signalerna fortfarande är svaga ger de sannolikt en möjlighet för en aktör att agera eller reagera på dem till en begränsad kostnad. När de växer i antal, frekvens och styrka kanske det är för sent, i varje fall om förloppet är irreversibelt eller språngvis och om åtgärder kräver en hög resursförbrukning. Här föreligger i så fall ett moment 22. Ju tidigare en signal behöver upptäckas, desto svagare kan den förväntas vara och därmed svårare att upptäcka.

Detekteringen av svaga signaler förutsätter att uppmärksamheten fokuseras mot relevant typ av objekt/fenomen och att mottagaren därvid har lämpliga instrument eller sensorer för att indikera spår av objektet/fenomenet, som förutsätts sända ut någon typ av signaler eller ledtrådar. Ett konkret sätt att upptäcka främmande objekt såsom flygfarkoster och fartyg oavsett väderlek är exempelvis genom radarspaning och presentation av radarekon på någon form av indikator. Radarbilden visar exempelvis objektets position, hastighet och riktning. Självfallet måste ett instrument inriktas åt rätt håll respektive ha ett relevant mätområde för att kunna upptäcka om något händer. Motsvarande gäller den mänskliga observatören. Man kan inte uppmärksamma vad man inte beaktar. Inte heller dessa krav är tillräckliga för att garantera detektering. Om objektet är ett smygflygplan kanske signalerna är alltför svaga i förhållande till omgivningsbruset. Eller det kanske omvänt förekommer så mycket verksamhet inom området att operatör eller tekniska hjälpmedel blir överstyrda. Alternativt kan falska ekon och störningar produceras på elektronisk väg.

Identifieringen av signalerna, dvs. att hänföra fenomenet till en relevant kategori, är ett annat problem. Det räcker kanske inte att veta att ett flygplan befinner sig på väg att korsa ett territorium; det är också viktigt att veta vilken typ av flygplan det gäller, kanske även i vilket syfte detta sker. Genom kommunikation, exempelvis genom radiosamband eller någon form av igenkänningssignal (IK), kan identifieringen ske. När den amerikanska robotkryssaren USS Vincennes

1988 sköt ned ett iranskt passagerarplan i Persiska Viken hade fartyget tidigare gjort flera försök att få kontakt med flygplanet. En orsak till nedskjutningen kan ha varit misslyckade eller felaktiga försök till identifiering.

Hanteringen av svaga signaler underlättas naturligtvis av om information inhämtas från flera olika källor. Därvid kan vaga signaler vägas mot varandra och eventuellt forma ett mönster. Denna sammanvägning och jämförelse kallas fusion. Den kan i och för sig vara datorstödd. Fusion kan även ske av information av högre förädlingsgrad.

Bedömningen, att ta ställning till de identifierade svaga signalernas betydelse och konsekvens, är en annan svårighet. I fallet med nedskjutningen av det iranska passagerarplanet påstås att identifieringen var felaktig, vilket ledde till att objektet betraktades som ett fientligt flygplan och inte som ett passagerarflygplan. Bedömningen kan således försvåras av att beslutsunderlaget är 1) osäkert eller otillräckligt (svaga men korrekta signaler), 2) missvisande eller direkt vilseledande, 3) eller att tiden för ett genomarbetat beslut är alltför knapp. För att agera, exempelvis avskjuta en robot från fartyget mot flygplanet, krävs att tillräckligt många, aktuella och relevanta indikationer föreligger för att ett fullgott beslut ska kunna tas i tid.

Av det korta resonemanget ovan framgår att det behövs *kriterier* på olika nivå. Det behövs exempelvis något kriterium för att bestämma om enskilda indata ska avfärdas som normala, föras vidare för analys eller ge upphov till någon form av åtgärd. Den inkommande informationen (den svaga signalen) kan därvid ha olika bearbetningsgrad.

Beslutsfattaren behöver sättas i fokus avseende beslutsfattandet och beslutsprocessen. Beslutsfattaren måste bestämma med vilken grad av säkerhet han vill kunna identifiera de svaga signalerna och till vilken kostnad och med vilken risk han är beredd att hantera dem. Många tillämpningar förutsätter datorstödd fusion av signaler med efterföljande automatiskt datorstött beslutsfattande, därför att mängden information är så stor och tiden så knapp att automatisk databehandling framtvingas. Sådan behandling kan emellertid bara ske när relevanta och tillräckliga data levereras av tillförlitliga sensorer och när det existerar klara beslutskriterier. När detta inte är fallet är det klokt att hänföra beslutssituationen till en mänsklig beslutsfattare. Den diskussion som kommer att föras här och de exempel som anförs utgår från att bedömningen görs av en mänsklig beslutsfattare.

I svåra beslutssituationer kan det vara oklart vad som är tillförlitliga och relevanta kännetecken på de händelser som studeras och vilka av alla svaga signaler som ska detekteras och värderas. Därför kommer sambanden mellan iakttagna signaler och utfall i verkligheten inte vara deterministiska, utan ha sannolikhetskaraktär, vilket utgör ett problem i sig. För det fortsatta resonemanget kommer vi att söka en begreppslig ram med vars hjälp problematiken med svaga signaler och vilseledande signaler lättare kan diskuteras.

Teori – Allmänt

Framställningen här grundar sig på ett allmänt systemteoretiskt synsätt därför att det underlättar kommunikation på olika tillämpningsnivåer. Det är därvid på intet sätt nödvändigt att ta ställning till exempelvis generell biologisk systemteori. Vårt syfte är helt pragmatiskt: Hur svaga signaler definieras och hur mängden av olika signaler klassificeras har betydelse för hur de uppfattas och hanteras. Vad som ytterst är ett fruktbart angreppssätt beror på syftet med undersökningen och på det undersökta systemets egenskaper. Därför är det för tidigt att redan nu göra definitiva prioriteringar avseende terminologi och den därmed sammanhängande teorin.

De allmänna exempel och korta resonemang som förs här tror vi kan ha en grundläggande tillämpning i samband med fortsatt metodutveckling för omvärldsanalys. Det är emellertid troligt

att ett fortsatt fördjupad resonemang bör föras relaterat till ett konkret system eller konkreta fallstudier och inte i anslutning till generella hypotetiska principer. Det följer senare (se del 2 kapitel 3).

Signaler, inklusive svaga signaler, kan exempelvis indelas efter sin grundläggande effekt på det mottagande systemet. Vi föreställer oss att en sådan effekt kan prognosticeras på förhand eller uppmätas i efterhand och betraktar denna fråga som oproblematisk tills vidare. Utgångspunkten för följande generella resonemang är att miljön (omgivningsmiljön, närmiljön eller den inre miljön) förändras och i samband därmed sänder ut svaga signaler till ett mottagande system (organism, organisation, stat).

Antag att den yttre miljön förändras kontinuerligt och relativt långsamt (evolutionärt). Det är då sannolikt att de utsända signalerna får motsvarande egenskaper och att systemets nödvändiga och tillräckliga svar på signalerna är "flexibilitet", anpassning till en förutsägbar föränderlig miljö. En evolutionär förändring kan leda till att systemet reagerar med "mer och bättre av det gamla vanliga". Systemets adekvata svar på förändringen, dess strategi, är strävan efter att bevara status quo, exempelvis genom någon form av homeostatisk mekanism.

Antag att miljön i stället förändras språngvis (revolutionärt). Den betyder att förändringen är fundamental och snabb men inte nödvändigtvis att den är principiellt oförutsägbar. Förändringen kan innebära både potentiella möjligheter och hot. Systemets svar på en sådan förändring beror av om den kunnat förutsägas i tid genom svaga signaler, om systemet haft en särskilt beredskap och organisation för plötsliga förändringar eller om den enbart kunnat iakttas genom signaler i efterhand, i så fall sannolikt starka signaler. Systemets goda strategi i detta fall torde vara en adaptiv beredskap till omformning efter en ny miljös krav.

Problemet är uppenbart. Det föreligger en allvarlig risk för att förväxla och misstolka de svaga signalerna så att systemets svar blir inadekvat. Det räcker inte att kontinuerligt fila på och förbättra en mekanisk eller elektromekanisk räknare typ "snurra" (evolutionär förändring), om framtiden ligger i små, snabba och billiga elektroniska räknare (revolutionär förändring). Poängen med denna diskussion har varit att peka på ett möjligt samband mellan förändringstyp och svarsstrategi.

Signaldetektionsteori (SDT)

Eftersom det ytterst är fråga om att hantera signaler i vid bemärkelse är det naturligt att luta sig mot signaldetektionsteorin (signal detection theory, SDT), i varje fall dess tankegång. Den möjliggör nämligen beskrivning av sambanden mellan utfall, beslutskriterium, signaler och brus med hjälp av sannolikhetsfördelningar. Vi går dock inte in på den statistiska analysen.Vi inleder diskussionen av SDT med att hänvisa till matrisen (figur 13) nedan, som avser en observatörs upptäckt av ett fientligt eller allierat flygplan, samt eventuell avskjutning av robot.

Antag att en serie experiment genomförs med försökspersoner, olika signaler och brusnivåer. Genom att ansätta olika kriterier för huruvida det föreligger en signal respektive när det enbart föreligger brus och upprepa dessa experiment erhålles två separata frekvensfördelningar, en signalfördelning och en signal-brus-fördelning, varvid det blir möjligt att experimentellt och teoretiskt studera effekten av olika beslutskriterier. En praktisk tillämpning skulle kunna vara att fastställa kriteriet för när en observatör kan identifiera ett flygplan på en radardisplay, dvs. att särskilja en svag signal från omgivningsbruset. (Ett helt annat sätt att tackla problemet vore att undertrycka allt brus på elektronisk väg och att förstärka presentationen av flygplansymbolen).

OBSERVATÖRENS BESLUT	MÄTNING, OBSERVATION, DATA = BRUS = i verkligheten störningar eller falska signaler, ej fi fpl	MÄTNING, OBSERVATION, DATA = SIGNAL+BRUS = i verkligheten både fpl och bakgrundsstörningar
LARM => skjut rb	Falsklarm Felaktigt accepterande av signal Avskjutning av rb mot allierad	Träff Korrekt accepterande Avskjutning av rb mot fi fpl
EJ LARM => fredlig passage	Korrekt förkastande Fri passage för allierat fpl	Miss Felaktigt förkastande Fri passage för fi fpl

Fig. 13. De korrekta utfallen, träffar och korrekta förkastanden, samt de felaktiga oönskade utfallen, missar och falsklarm. Flygplan = fpl. Robot = rb. Fientligt = fi.

I anslutning till figur 14 kan vi föreställa oss en domstolsförhandling. Det föreligger ett mål och en bevisning. Signalerna är i detta fall bevisningens styrka. Bevisningen är som vanligt inte fullständig, den åtalade kan vara oskyldig. Om beviskravet ansätts mycket högt (snävt kriterium) kommer den åtalade att frikännas. Om det ansätts betydligt lägre kommer han att dömas. Generellt betyder snäva kriterier det negativa att skyldiga kommer att frikännas (missar) och det positiva att antalet oskyldiga som döms (falsklarm) kommer att minska. Omvänt kommer vida kriterier innebära det positiva att alla skyldiga döms (många träffar, få missar) och det negativa att många oskyldiga också döms (många falsklarm, färre korrekta förkastanden).

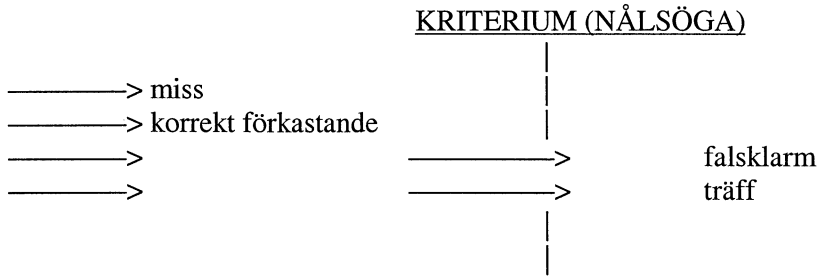

Fig. 14. Utformningen av kriteriet ("nålsögat) bestämmer andelen träffar, missar respektive falska larm och korrekta förkastanden. Fler träffar betyder också fler falska larm. Om man kräver att alla falsklarm ska elimineras kommer också antalet träffar att minska och missar att öka.

Beslutssituationen är i vissa tillämpningar mer komplex. I maktpolitiska sammanhang stater emellan finns det skäl att skilja mellan signaler för avsikt och kapacitet. Vissa signaler, som erhålls genom politisk signalering, kan – men måste inte – vara ett mått på den politiska ledningens avsikter. De kan också vara vilseledande utspel eller "försöksballonger". Signaler som indikerar avsikt är svårtolkade och många gånger svåra att upptäcka. Om en stats eller organisations ledning inte vill avslöja sina planer för motståndare och konkurrenter, döljs eller manipuleras signalerna.

Signaler, som erhålls genom observation och mätning av fysiska förhållanden (antal flygplan, stridsvagnar etc) är ett mått på något faktiskt, den främmande statens faktiska kapacitet. Det kan därför samtidigt förekomma relativt relevanta och säkra signaler, exempelvis kapacitetsangivelser, samt potentiellt mycket relevanta men osäkra signaler (exempelvis indikationer på avsikt) och rent brus. De relevanta signalerna kan förstärka varandra (krigiska intentioner och stark militär kapacitet alternativt fredliga intentioner och svag militär kapacitet) eller motsäga varandra (fredliga intentioner och stark militär kapacitet alternativt krigiska intentioner och svag militär kapacitet). Det kan vara så att de mest relevanta signalerna är både svagast och mest svårtolkade, i synnerhet om de indikerar avsikt eller vilja eller om motståndaren försöker dölja dem. De starkaste signalerna, t.ex. antalet vapenplattformar, erbjuder visserligen ett entydigt mätbart kapacitetsmått, men den faktiska prestationsförmågan bestäms därutöver av många samverkande faktorer, exempelvis tekniska (utrustningens tillstånd och prestanda) och personella (operatörernas hälsa, träning och motivation) för att blott nämna några. Det innebär i så fall att även en analys av starka signaler leder fram till ett sekundärt behov av att identifiera och analysera därtill kopplade svagare signaler.

Det är lättare att skapa vilseledande intryck vid svaga signaler än vid starka, därför bör studiet av svaga signaler även beakta möjligheten av vilseledning.

Strategi

Avsikten med detta avsnitt är att påvisa att det är möjligt att diskutera olika strategier i allmänhet och nödvändigt att diskutera sådana vid konkreta tillämpningar (fall) i synnerhet. Med strategi menas val av handlingslinje för att uppnå ett systems övergripande mål med dess samlade resurser. En studie av svaga signaler bör leda fram till strategier, både för signalernas upptäckt och för lämpliga reaktioner på dem. Vi ger här några exempel på tänkbara utgångspunkter för att utveckla strategier.

Det är viktigt att påminna om att svaga signaler kan förebåda både möjligheter och hot. Därför, när vi talar om att reagera på signaler, avser vi att parera (preventivt gardera eller i efterhand passivt bemöta ett hot) eller att agera (aktivt på förhand eller vid direkt indikation utnyttja en situations alla möjligheter), beroende av den faktiska situationen. Att parera och att agera är förhållningssätt som inte utesluter varandra. Att vara flexibel och att vara adaptiv kan också kombineras. Ett förhållningssätt skulle således vara att kombinera dessa strategier.

Svag indikering på evolutionär utveckling —> Reagera inom ramen för befintlig mental modell genom flexibel strategi.

Svag förvarning på revolutionär utveckling —> Beredskap att omtolka befintliga mentala modeller för att kunna agera genom adaptiv strategi.

Det är emellertid orimligt kostsamt att ständigt upprätthålla en handlingsberedskap för alla eventualiteter. Därför behöver svaga signaler upptäckas, identfieras och bedömas på ett tidigt stadium. En invändning är att det är just detta som svårt: att tidigt särskilja om förändringar är revolutionära eller evolutionära, respektive om det föreligger negativa hot eller positiva möjligheter. Dessa invändningar behöver penetreras i anslutning till konkreta exempel. Svårigheterna har dels att göra med hur svaga signaler upptäcks och identifieras på ett tidigt förändringsstadium och dels hur man svarar på dem.
En förutsättning för att kunna indikera och följa en utveckling, och därmed för att kunna upptäcka svaga signaler, är att förstå och känna till sammanhanget och närmiljön. Detta kan tolkas som en uppmaning att ”känna signalen”. Känner man signalen kan den kanske förstärkas och förtydligas hos mottagaren. En kompletterande strategi är, enligt företaget Taylor, att ”känna

bruset".[212] Känner man bruset kan det undertryckas och elimineras. I båda fallen förbättras signal-brus-förhållandet till fördel för mottagaren. Ansatserna kan kombineras och handlar egentligen om att eftersträva bättre kunskap och förståelse.

Ett annat förhållningssätt är att försöka förebygga att ett hot realiseras (försiktighetsprincipen) alternativt att förmildra konsekvenserna. Med försiktighetsprincipen menas att eliminera eller förstärka svaga punkter, som kan tjäna som utgångspunkt för angrepp alternativt att erbjuda någon väl förberedd angreppspunkt genom att simulera svaghet. Poängen med dessa förhållningssätt är att det inte är helt nödvändigt att kunna upptäcka alla svaga signaler av hotande karaktär, man motar i stället Olle i grind, utan att säkert veta om Olle är närvarande. Om det inte är möjligt att få förvarning om Olle närmar sig kan detta vara en adekvat ansats. Uttryckt på annat sätt är det fråga om att minska sårbarheten, att öka handlingsberedskapen och att förhärda sig mot vissa oönskade händelser.

I utökad handlingsberedskap ingår förmåga och kapacitet att upprätthålla sådana systemfunktioner som är hotade. Idealet vore naturligtvis att om möjligt eliminera alla svaga länkar i systemet, sådana förhållanden eller egenskaper som skulle kunna utgöra angreppspunkter. Det kan emellertid helt uppenbart ställa sig kostsamt, varför ett handlingsalternativ skulle kunna vara att avsiktligt (odla) skapa svagheter och därmed diskret bjuda motståndaren väl förberedda angreppspunkter.

Om man inte kan upptäcka eller identifiera en viss typ av svaga signaler kan det kanske vara möjligt att i stället förhindra att situationen alls uppstår. Sannolikt ligger emellertid orsaken per definition utanför det egna systemets inflytelsesfär, varför detta i så fall inte är någon allmänt framkomlig strategi.

Alternativt kan det vara möjligt att förneka och förtiga att en viss oönskad situation uppstått till följd av att svaga signaler utvecklats på ett oönskat sätt. I undantagsfall och tillfälligt kan en sådan taktik vara acceptabel. Det går emellertid att finna situationer där "icke-bemötandet" lett till att företag slagits ut från marknaden eller att en angripare fått förhand och övertag. Det går också att finna situationer där en möjlig skandal genom undertryckande av information inte växt till något värre. I varje fall är "icke-bemötandet" inte en generell strategi. Tillvägagångssättet kan dessutom strida mot befintlig informationspolicy, exempelvis avseende strävan efter öppenhet.

Ur sändarens perspektiv kan ett kraftfullt utbud av svaga signaler förvirra, fördröja eller mätta motståndaren genom sin belastande mångfald och otydlighet. Starka signaler som är missvisande och trovärdiga kan lura honom, under den rimliga förutsättningen att de uppmärksammas. Ur mottagarens perspektiv kan svaga signaler avslöja sändarens vilseledningsoperation – om de uppmärksammas och tolkas rätt.

I del 2 appliceras den teoretiska kunskap om svaga signaler, som presenterats i detta avsnitt, på de vilseledningsfall som där beskrivs (se kapitel 3).

[212] Se bl.a. Internet http://www.mgtaylor.com (Weak Signal Research).

Bibliografi

Nedan listas all litteratur som använts under projekets gång. Här återfinns även referenser som inte direkt citeras i texten. I rapportens del 2 kommenteras valda referenser.

Statens offentliga utredningar och departementsskrivelser

- Försvarsberedningen, *Förändrad omvärld – omdanat försvar*, Regeringskansliet, Ds 1999:2, Internet, http://forsvar.regeringen.se/propositionermm/ds/pdf/ds99_2sve.pdf, hämtad 27 februari 2001.
- Försvarsberedningen, *Gränsöverskridande sårbarhet – Gemensam säkerhet*, Regeringskansliet, Ds 2001:14, Internet, http://forsvar.regeringen.se/propositionermm/ds/pdf/ds2001_14.pdf, hämtad 9 mars 2001.
- Statens offentliga utredningar, *Säkerhet i en ny tid*, SOU 2001:41, Internet, http://forsvar.regeringen.se/propositionermm/sou/pdf/sou2001_41a.pdf, hämtad 29 juni 2001.
- Statens offentliga utredningar, *Underrättelsetjänsten – en översyn*, SOU 1999:37, Internet, http://forsvar.regeringen.se/propositionermm/sou/pdf/sou99_37.pdf, hämtad 27 februari 2001.

Rapporter och utredningar

- *Ag IW*, Rapport nummer 2 om åtgärder och skydd mot informationskrigföring från arbetsgruppen för informationskrigföring, 1998-09-01, dnr FO 98 1828/MIL.
- ASTA 2, FHS/SPF, *ASTA-studien*, 23385:60763.
- Aust, Michael, *Strategisk överraskning, varning och beslut*, C-uppsats ht-96 vid Uppsala universitet.
- Clevström, Jenny, Norlander, Lena och Unge, Wilhelm, *Rysk toxin- och bioregulatorkompetens*, FOA-R–00-01703-170–SE, december 2000.
- Conflict Studies Research Center, CSRC, Sandhurst, England (f.d. Soviet Studies Research Center, SSRC) (diverse rapporter och meddelanden).
- Grabo, Cynthia M., *Soviet Deception in the Czechoslovak Crisis*, CIA Center for the Study of Intelligence, Studies in Intelligence (kursmateial hösten 2000), Internet, http://www.odci.gov./csi/studies/fall00/ch5_Soviet_Deception.pdf, hämtad 9 augusti 2001.
- Gustafsson, Magnus, Furustig, Hans, Lindahl, Nils-Emil och Sjöstedt, Gunnar, *Vilseledning, desinformation och spel*, Spel för ökad kunskap, Försvarets Krigsspelscentrum, 1995:06.
- Foreign Military Studies Office, FMSO (f.d. Soviet Army Studies Office, SASO), Fort Leavenworth, USA (diverse rapporter).
- Furustig, Hans, *Debatt och försvarsdebatt. Några problemområden*, FOA rapport C 56036-H2, december 1982.
- Furustig, Hans, *Etik och teknik i informationens värld*, FOA rapport D 56003-H9, januari 1981.
- Furustig, Hans, *Marin vilseledning*, FOA-R–98-00757-706–SE, april 1998.
- Furustig, Hans, *Militär vilseledning – Några grunder*, FOA-R–96-00365-5.2–SE, november 1996.
- Furustig, Hans, *Vilseledning mot företag,* FOA- R--95-00130-5.3-SE, maj 1995.

- Furustig, Hans, *Vilseledning och påverkan genom reflexive control*, FOA-R–94-00036-5.3–SE, november 1994.
- Furustig, Hans och Lindahl, Nils-Emil, *Omvärldsanalys*, FOA-R–95-00129-5.3–SE, maj 1995.
- Furustig, Hans och Lindahl, Nils-Emil, *Psykologiska operationer vid internationella insatser*, FOA-D–95-00176-5.3–SE, september 1995.
- Furustig, Hans och Sjöstedt, Gunnar, *Operationer mot nationella säkerhetspolitiska militära intressen – Förstudie*, FOA-A–50022-5.3–SE, april 1994.
- Försvarshögskolan, *ASTA-studien – Ett regeringsuppdrag om aktiva åtgärder rörande Informationskrigföring*, H01710:6014, 1997-06-30.
- Försvarsmakten, *Försvarsmaktens gemensamma nomenklatur – Nomen F 97.*
- Försvarsmakten *Huvudstudie Ledningskrigföring – slutrapport*, HKV 21 120:60831, 1999-01-27.
- Försvarsmakten, *Ledningskrigföring, definition av ny struktur och begrepp*, HKV 21 120:79934, 1995-09-22.
- Försvarsmakten, *PM Vilseledning*, 21 120:73579, 1997-12-15.
- Herman, Michael, *Modern Intelligence Services: Have They a Place in Ethical Foreign Polices*?, (Conflict Studies Research Centre, RMA-Sandhurst), rapport M18, september 1999.
- *Intentions and Capabilities: Estimates on Soviet Strategic Forces, 1950-1983*, Donald P. Steury (red.), History Staff, Center for the Study of Intelligence, CIA, Washington D.C., 1996.
- Joint Publication 3-58, *Joint Doctrine for Military Deception*, 6 June 1994.
- Leth, Göran och Thurén, Torsten, *Källkritik för Internet*, SPF rapport 177, (Stockholm, 2000).
- Ljunggren, Boris, *Militärt relaterade tidiga indikatorer på en utveckling i Ryssland som kan bli ett hot i närområdet och mot Sverige*, outgiven rapport FOA, hösten 1997.
- Nilsson, Per-Olov, *Teknisk utveckling i Öst och Väst*, FOA-rapport C10299-1.1, november 1987, bilaga 2.
- Nordlund, R. och Tubin, E. (red.), *Desinformation i öst och väst. Referat av forskning i Sovjetunionen och USA*, SPF, Meddelande nr 120, feb 1990.
- O'Donnell, James P., "AIDS and Bum Dope: A Case Srudy in Disinformation", *Program for the Study of Disinformation Series 2*, 1988, Boston University, College of Communication.
- Saar, Stütz och Tubin, *Ett ryktes anatomi*, SPF, Meddelande nr 132, aug 1991.
- Sjöstedt, Gunnar, *Som en saga. Lögnen som maktmedel. Sårbarhetsproblem och motåtgärder*, SPF, Rapport nr 159, maj 1992.
- Stenström, Paula, *Lönande lögner – Psykologisk krigföring som hot i fred, kris och krig*, FOA-R–97-00483-240–SE, oktober 1997.
- *SÄPO Verksamhetsåret 1999*, (Säkerhetspolisen, mars 2000).
- Ulfving, Lars, (Furustig, Hans (red.)), *Den stora maskeraden*, FOA-R--94-00017-5.3–SE, augusti 1994.
- Ulfving, Lars, *Den stora maskeraden – Sovjetrysk militär vilseledning: Maskirovka sett i ett historiskt perspektiv*, Försvarshögskolans Acta C8, 2000.
- Unge, Wilhelm, *The Russian Military-Industrial Complex in the 1990s – Conversion and Privatisation in a Structurally Militarised Economy*, FOA-R–00-01702-170–SE, december 2000.
- Wiss, Åke och Stenström, Paula, *Pålitlig påverkan – Psykologisk krigföring som ett hot mot internationella insatser*, FOA-R--99-01057-170–SE, mars 1999.

Böcker

- Agrell,Wilhelm, *Konsten att gissa rätt: Underrättelsevetenskapens grunder*, (Lund, Studentlitteratur, 1998).
- Alibek, Ken med Handelman, Stephen, *Biohazard*, (Hutchinson, London, 1999).
- Bakatin, Vadim, *Att bli kvitt KGB*, (Förlags AB Wiken, Falun, 1993).
- Bell, B. och Whaley, Barton., *Cheating and Deception*, (Transaction Publishers, London, 1991).
- Betts, Richard K., *Surprise Attack – Lessons for Defense Planning*, (Brookings Institution, Washington, 1982).
- Bittman, Ladislav, *The Deception Game – Czechoslovak Intelligence in Soviet Political Warfare*, (Syracuse, New York, 1972).
- Bittman, Ladislav *The KGB and Soviet Disinformation – An Insider's View*, (Pergamon-Brassey's, USA, 1985).
- Bittman, Ladislav, *The New Image-Makers: Soviet Propaganda & Disinformation Today*, Pergamon-Brassey´s, 1988.
- Borg, Lennart. (ed.), *Informationskrigföring. Konsekvenser för samhälle och samhällsliv,* (FHS, FOA och SAF, Stockholm, 1997).
- Brown, A., *Bodygard of Lies,* (Harper & Row, New York, 1975).
- Carlsson, I., *På lögnens väg,* (Historiska Media, Lund, 1999).
- Clive, R., *The Soviet Propaganda Network,* (Pinter Publishers, London, 1988).
- Cook, Terry L., *Big Brother NSA and Its "Little Brothers" – The National Security Agency's Global Surveiillance Network*, (SCM Publishing, Oregon, 1998).
- Cruickshank, Charles, *Deception in World War II*, (Oxford University Press, 1979). (Behandlar bl.a. *Operation Graffham.*)
- Dailey, D. & Parker, P. (red.), *Soviet Strategic Deception*, (Lexington Books, 1987).
- Douglas H. Dearth och R. Thomas Goodden (eds.), *Strategic Intelligence: Theory and Application*, United States Army War College och Defense Intelligence Agency, andra upplagan, 1995.
- Dewar, Michael, *The Art of Deception in Warfare*, (David & Charles Military Books, 1989).
- Engberg, Peppe, *Sovjet och fredsrörelsen*, (Timbro förlag, 1985).
- Epstein, E., *Deception. The Invisible War Between the KGB and the CIA,* (Simon & Schuster, New York, 1989).
- Epstein, E., *Spionernas krig. Desinformation som vapen*, (Timbro, Stockholm, 1990).
- Forsén, B. och Forsén, A., *Tysklands och Finlands hemliga ubåtssamarbete*, (Söderströms förlag, 1999).
- Friman, Henrik, Sjöstedt, Gunnar och Wik, Manuel, *Informationskrig. Några perspektiv.* UI Conference Papers 18. (Utrikespolitiska Institutet, Stockholm, 1996).
- Furustig, Hans och Sjöstedt, Gunnar, *Strategisk omvärldsanalys*, (Studentlitteratur, Lund, 2000).
- Godson, Roy, May, Ernest R. and Schmitt, Gary, *Intelligence at the Crossroads – Agendas for Reform*, (National Strategy Information Center Inc., 1995).
- Gordievskij, Oleg och Andrew, Christopher, *KGB inifrån – 2 Spionskandalernas tid*, (Bonniers, 1990).
- Grant, N., *Deception, a Tool of Soviet Foreign Policy*, (Nathan Hale Institute, Washington, 1987).
- Handel, M. (red.), *Strategic and Operational Deception in the Second World War*, (Frank Cass, 1987).
- Herman, Michael, *Intelligence Power in Peace and War*, (Cambridge University Press, 1996).

- Heuer, Richards J. Jr., *Psychology of Intelligence Analysis*, (Center for the Study of Intelligence, CIA, 1999), http://www.odci.gov/csi/books/19104/index.html, hämtad 9 augusti 2001.
- Häggman, B., *Desinformation*, (Contra, Stockholm, 1990).
- Jacobsen, Carl G. (ed.), *The Soviet Defence Enigma: Estimating Costs and Burden*, (SIPRI, Stockholm, 1987).
- Lindsay,P.& Norman, D. (1972): *Human Information Processing*. NewYork: Academic Press. (appendix B, särskilt sid.674-678 om signaldetektionsteori, SDT).
- MacEachin, Douglas, *US Intelligence and the Polish Crisis 1980-1981*, Internet, http://www.odci.gov./csi/books/poland/index.htm, hämtad den 9 augusti 2001.
- McKay, C., *From Information to Intrique. Studies in Secret Service based on the Swedish Experience, 1939-1945*, (Frank Cass, London, 1993).
- MG Taylor Corporation, *Weak Signal Research* (1997), Internet, http://www.mgtaylor.com. (Behandlar svaga signaler på ett kreativt sätt utifrån ett företags perspektiv).
- Miller, J.G., *Living Systems*, (New York, McGraw-Hill, 1978). (En biologisk systemteoretisk framställning omfattande ca 1100 sidor, som bl.a. behandlar levande organismers svar på olika signaler. Millers framställning generaliseras av företaget Taylor ur organisationsteoretiskt perspektiv).
- Mitrokhin, Vasili och Andrew, Christopher, *The Mitrokhin Archive – The KGB in Europe and the West*, (Penguin Press, 1999).
- Nogee, Joseph L. och Donaldson, Robert H., *Soviet Foreign Policy Since World War II*, (Pergamon Press, 1984, andra upplagan).
- Nordblom, Charlie, *Industrispionage*, (Timbro förlag, 1984).
- Nordblom, Charlie, *Krig i fredstid*, (Timbro/Lettura, 1988).
- Nordlund, R. & Tubin, E. (eds, 1990). *Desinformation i öst och väst. Referat av forskning i Sovjetunionen och USA.*
- Pacepa,Ion, *Red Horizons*, (Hodder and Stoughton, Sevenaoks, 1989).
- Pincher, C., *The Secret Offensive,* (Sidwick & Jackson, London, 1985).
- Pincher, C., *The Truth about Dirty Tricks,* (Sidwick & Jackson, London, 1991).
- Radvanyi, J. (red.), *Psychological Operations and Political Warfare in Long-term Strategic Planning,* (Praeger, London, 1990).
- Samuelson, Lennart, *Plans for Stalin's War Machine: Tukhachevskii and Military-Economic Planning, 1925-1941* (London, Macmillan, 1999).
- Samuelson, Lennart, *Röd koloss på larvfötter – Rysslands ekonomi i skuggan av 1900-talskrigen*, (SNS förlag, Stockholm, 1999).
- Schwartau, Winn, *Information Warfare*, (Thunder´s Mouth Press, New York, 1994).
- Schwarze, Erika, *Kodnamn Onkel*, (Albert Bonniers förlag AB, Stockholm, 1993).
- Shulsky, A., *Silent Warfare. Understanding the World of Intelligence.* (Brassey´s, New York, 1993)
- Shultz, Richard H. och Godson,Roy, *Dezinformatsia – Active Measures in Soviet Strategy*, (Pergamon-Brassey's, USA, 1984).
- Sigurd, Bengt, *Språk och språkforskning*, (Studentlitteratur, Lund, 1991).
- Sudoplatov, Pavel m.fl. *Direktoratet – Stalins spionchef berättar,* (Stockholm, Little Brown and Company, 1994).
- Whaley, Barton, *Stratagem: Deception and Surprise in War*, (MIT, Center for International Studies, 1969).
- Wheatley, Dennis, *The Deception Planners – My Secret War*, (Hutchinson, London, 1980).
- *Vojennyj entsiklopeditjeskij slovar*, Moskva, 1986, andra upplagan.
- Wolf, Markus och McElvoy, Anne, *Mannen utan ansikte – En mästerspions memoarer*, (Norstedts Förlag AB, Stockholm, 1997). (Kap. 12 handlar om "Aktiva åtgärder").
- Woodward, Bob, *CIA:s hemliga krig 1981-87*, (Rabén & Sjögren, Stockholm, 1987).

Tidningar och tidskrifter

De tidnings- och tidsskriftsartiklar som är av partikulär natur rörande specifika sakfrågor listas ej. Dessa återfinns med fulla referenser i fotnoterna i den löpande. Endast längre artiklar av generellt värde och av rapportliknande karaktär listas här.

- FHS/IKK, Informationskrigföringskansliets månatliga nyhetsbrev *DELETE*, nr 1, juni 2000.
- Richelson, Jeffrey, "Examining US intelligence failures", *Jane's Intelligence Review*, september 2000.
- Whaley, Barton, "Toward a General Theory of Deception", *Journal of Strategic Studies*, 1982.

Andra källor

- Ljunggren, Boris, PM 1977.
- Rydqvist, John, *Why are early warning systems so poor at preventing surprises?*, uppsats vid King's College, London, december 1998.
- Sjlykov,Vitalij, *The Real Defense Burden in Russia*, paper förberett för FOA-konferensen "Russian Military Prospects" i Stockholm 12-13 mars 1998.
- STV 2, DOKUMENT UTIFRÅN (920328). (1) *PR-firman som vann kriget*. (2) Paneldiskussion. Videoinspelning, nr 50 i HF arkiv.
- Ulfving, Lars, PM, *Brännpunkt Sinai: Ett kompilat av opublicerat material om Oktoberkriget 1973*, 1978.
- von Braun, Joakim, arkivmaterial rörande AIDS-kampanjen.

Muntliga källor

- Samtal med representant för Försvarsdepartementet, juli 2000
- Samtal med representant för Säkerhetspolisen, februari och mars 2000.
- Samtal med representanter för Militära underrättelse- och säkerhetstjänsten, år 2000.
- Samtal med representant för försvarsindustrin, februari 2000.
- Samtal med Roger Roffey, FOI NBC-skydd, 2001.
- Samtal med Joakim von Braun, von Braun Consultants, Stockholm, april 2000.