Mediers beredskap

Informationsoperationer och mediers sårbarhet

Katrin Berggren (redaktör)

STYRELSEN FÖR PSYKOLOGISKT FÖRSVAR

Mediers beredskap

Informationsoperationer och mediers sårbarhet

Katrin Berggren (redaktör)

Styrelsen för
PSYKOLOGISKT FÖRSVAR

SPFs skriftserie

2004:1 Massmediernas elberoende. Elavbrottet den 23 september 2003
2005:1 Minoritetsmedier och minoritetsmediepolitik i Sverige – en kartläggning
2005:1 Minoritetsmedier i Sverige – en kartläggning
2005:2 Medieföretagens syn på hot, risker och sårbarheter – en kartläggning
2005:3 Mediers beredskap. Informationsoperationer och mediers sårbarhet

För tidigare publikationer se SPFs webbplats http://www.psycdef.se/reports

Utgiven av Styrelsen för psykologiskt försvar
ISSN 1401-2383
Stockholm, 2005
Omslagsbild Matton bildbyrå
Produktion Intellecta Tryckindustri, Solna 2005 – 16004

Innehållsförteckning

SPFs förord

Massmedierna är de viktigaste förmedlarna av händelser i samhället. Information och kommunikation är inte bara medel för att vidmakthålla medborgarnas förtroende för och tillit till samhället och dess institutioner utan också väsentliga för att kunna rädda liv och egendom i störda situationer. Massmediernas trovärdighet är en förutsättning för detta.

En angelägen uppgift för SPF är att på olika sätt förebygga och minska sårbarheten i viktiga mediers produktion och distribution – genom att skapa en säkerhets- och krishanteringsförmåga hos medieföretagen – så att samhällets krav och medborgarnas förväntan på information och kommunikation säkras och kan fungera oberoende av situation.

SPFs uppdrag inom området *medieberedskap* har förändrats i det nya krishanteringssystemet. Myndighetens roll fokuseras på att vara samtalspartner och kunskapsförmedlare till medieföretagen när det gäller verksamhet under störda förhållanden. Myndigheten ska ge råd och vägledning om inom vilka områden aktörerna bör stärka sin ordinarie förmåga att hantera normala och vardagliga störningar samt peka på allvarligare händelser som bör uppmärksammas, såsom svåra påfrestningar på samhället i fred. SPF ska även utarbeta underlag för regeringens beslut om beredskap för medieföretagen samt hålla sig informerad om den framtida utvecklingen inom medieområdet.

Det är i ljuset av detta uppdrag som studien om informationsoperationer och mediers sårbarhet ska betraktas. Studien har ett kunskapshöjande syfte och SPF vill med projektet påvisa och medvetandegöra riskerna att medierna i dagens mediestruktur utnyttjas i så kallade informationsoperationer i vid mening.

Jag vill tacka författarna Bertil Flodin och Anders Sahlstrand vid Gullers Grupp Informationsrådgivare AB och Hans Furustig vid Totalförsvarets forskningsinstitut (FOI) för mycket intressanta och lärorika bidrag och Arvid Kjell, omvärldsanalytiker vid Krisberedskapsmyndigheten (KBM), för värdefulla synpunkter på det sammanställda materialet. Ett tack också till Göran Stütz som skrivit det inledande avsnittet och som också svarar för projektets upplägg och genomförande.

Stockholm i maj 2005

Katrin Berggren
Avdelningen för medieberedskap, SPF

Om författarna

Bertil Flodin är docent i journalistik och masskommunikation och arbetar vid Gullers Grupp Informationsrådgivare AB i Stockholm.

Hans Furustig är fil kand och tekn dr, tidigare laborator vid Försvarets forskningsinstitut (FOA) och idag verksam som konsult vid Totalförsvarets forskningsinstitut (FOI).

Anders Sahlstrand är fil dr i journalistik och arbetar vid Gullers Grupp Informationsrådgivare AB i Stockholm.

Göran Stütz är fil dr, tidigare laborator och forskningschef vid Styrelsen för psykologiskt försvar (SPF).

Informationsoperativa bakhåll?

Göran Stütz

Innehållsförteckning

Inledning

Styrelsens för psykologiskt försvar (SPF) roll inom området *medieberedskap* har förändrats i det nya krishanteringssystemet. Myndighetens verksamhet på detta område ska vara till direkt nytta för medieföretagen och den ska stödja dessa inom områden som de av olika skäl inte själva kan bevaka fullt ut. SPF ska nu bl a ge råd och vägledning om medieföretagens planering för höjd beredskap (krig) och för svåra påfrestningar på samhället i fred samt hålla sig informerad om den framtida utvecklingen på medieområdet. SPFs roll fokuseras på att vara samtalspart och kunskapsförmedlare till medieföretagen. Enkelt uttryckt handlar det om att anlägga ett samhällsperspektiv på informationens och kommunikationens betydelse under störda förhållanden.

Medborgarnas rätt till information är grundlagsfäst i Sverige och medierna är de viktigaste förmedlarna av händelser i samhället och i omvärlden. Betydelsen av information och kommunikation, speciellt vid samhällsstörningar, är väl känt sedan länge och betonas allt mer. Inte minst SPFs tidigare forskningsverksamhet har bidragit till detta. Information och kommunikation är inte bara väsentliga för att vidmakthålla medborgarnas förtroende för och tillit till samhället och dess institutioner utan också medel att i störda situationer rädda liv och egendom. Trovärdiga massmedier är en av förutsättningarna för detta. Det gäller alltså att ”säkra” mediernas roll som oberoende förmedlare av information och kommunikation också vid samhällsstörningar, i kris och, ytterst, under höjd beredskap.

Att förmedla nyheter, att uppträda som samhällets och allmänhetens ombud, att iklä sig rollen som ”tredje statsmakten” är i grunden ingen filantropisk verksamhet och ska inte vara det heller i ett samhälle av det slag vi vill ha. Massmedierna är fria och deras verksamhet är till för att uppfylla en mångfald av syften, ambitioner och opinioner. Beredskapstänkande är, föga överraskande, ingen första ledstjärna för de kommersiella eller privata medierna. Skydd och säkerhet tenderar att bli en affärsfråga. Bilden är förstås i vissa avseenden annorlunda på public service-sidan genom olika avtal som slutits mellan staten och programföretagen.

En angelägen uppgift för alla berörda är att på olika sätt minska sårbarheten i viktiga mediers produktion och distribution. Målsättningen är att i samråd med medierna – såväl public service-företagen som kommersiella medier – skapa en godtagbar, oberoende, låt oss tillsvidare kalla det, *rapporteringsförmåga* och att denna förmåga utvecklas åtskiljd från den informationsberedskap som avser myndigheterna. SPF skall alltså verka för robusta informationssystem på olika nivåer i samhället för säker distribution av nyheter, krisinformation, varning, råd och anvisningar. Robustheten är av såväl teknisk som innehållsmässig karaktär och avser såväl produktion som distribution.

Under 2004 har SPF initierat och genomfört flera studier som har direkt bäring på medieföretagens arbetsförutsättningar i vid mening. Bland dessa kan nämnas den rörande konsekvenserna av elavbrott för medieföretagens produktion. I en annan studie kartläggs olika etniska minoritetsmedier för att deras verksamhet

skall ”sättas på kartan”. Medieföretagens beredskap inför störningar av olika slag kartläggs i en omfattande tredje studie för att ge en bild av beredskapen i nuläget och för att möjliggöra en analys av hur företagen själva önskar se sin beredskap i framtiden. I ett särskilt projekt fokuseras medierna i termer av så kallade informationsoperationer. Det är detta denna text handlar om.

Syftet med projektet

Syftet med det projekt vars inledande delar avrapporteras här är att fördjupa och bredda kunskaperna inom området mediers beredskap. Genom projektet vill SPF medvetandegöra risken att medierna i dagens medielandskap utnyttjas för avsiktlig vilseledning, det vill säga en aspekt av *informationsoperationer* (IO). Projektet pekar på angelägna frågeställningar för framtida forskning på området. Främst fokuseras informationens ”mjuka”, innehållsmässiga, delar. Självklart hänger informationens tekniska delar ihop med de kognitiva, men sådana aspekter lyfts fram i parallella SPF-studier.

Det skall noteras att projektet på nuvarande stadium är att betrakta som normativt, diskuterande. Sedan början av 1990-talet har mycken forskning bedrivits kring olika aspekter av informationsoperationer och forskningen på massmedieområdet är kompakt. När det gäller mediers sårbarhet i ljuset av tänkbara eller möjliga IO är dock kunskapen ännu knapp och osystematisk. Föreliggande projekt måste därför ses som explorativt och uppfattas som ett inledande steg i en önskvärd, längre forskningsprocess. Tankar bakom studien beskrivs i det följande och därefter kommer två bidrag som gäller informationsoperationer via medier respektive mediers sårbarhet.

Kommunikation och åter kommunikation

Utvecklingen på informations- och kommunikationsområdet under senare år – främst informationsteknikens och Internets accelererande betydelse samt sammansmältningen av olika medier och informations- och kommunikationskanaler – har förändrat såväl budskap som dialog. Även informations- och kommunikationsmönstren sett såväl ur ett sändar-, förmedlar- som ur ett mottagarperspektiv har förändrats. Information av allehanda slag flödar fram och tillbaka i dagens samhälle; samhället beskrivs som ”informationstätt”. Television och telefoni kan förmedlas via bredband, tv-signaler kan sändas genom telefonjacket. På så sätt går telefoni, datakommunikation och tv-tittande ihop. Inte bara infrastrukturen smälter ihop till en enhet, utan kanske blir också ”apparaten” en och densamma framöver.

Till detta skall förstås läggas det moderna samhällets ökande beroende av och medvetna satsning på data och information/kommunikation för att alls kunna fungera (t ex elektronisk förvaltning, kritisk informationsinfrastruktur, ledning, kontroll och övervakning). Produktion av tjänster och varor är i allt väsentligt beroende av fungerande tjänster från informationsinfrastrukturen. Fel och brister där kan medföra att verksamheter inom för samhället viktiga sektorer, som t ex telekommunikationer, energiproduktion, drivmedelsförsörjning, transporter, handel och banktjänster, transaktioner/överföring av olika slag, administration, övervakning och kontroll försvåras eller upphör helt.

Utvecklingen på informations- och kommunikationsområdet är i de flesta avseenden positiv och medger en rad intressanta och utvecklande möjligheter såväl för den enskilde som för samhället. Men man kan inte blunda för de hot och risker denna utveckling fört med sig såväl i stort som i smått.

Utan information och kommunikation i vid mening kan ett samhälle som institution knappast existera. Möjligheterna att sammanställa, använda och värdera information av allehanda slag påverkar såväl den enskildes vardag som samhället i stort. Detta förhållande medför konsekvenser för myndigheter, näringsliv, beslutsfattare och medborgare, för medierna själva och för samhällets mediestruktur i stort. Det är inte bara samhället i vid mening, dess infrastruktur och förvaltning som är beroende av och ställer krav på information och kommunikation; medborgaren är, t ex vid samhällsstörningar, beroende av information och inte bara förväntar sig adekvat sådan utan ställer också krav på dess innehåll, snabbhet, begriplighet och åtkomlighet.

Kampen om tanken

Massmedierna är bland mycket annat redskap för frihet och frigörelse då de öppnar vägar för möjligheter av skilda slag. Ett pluralistiskt samhälle är ett friskt samhälle där det finns en avsevärd variation på såväl individer som livsstilar samt att det i ett sådant samhälle erbjuds en arena på vilken sanningen till sist kommer att segra över falskheten. Demokrati bygger på att medborgarna i samhället får en så långt möjligt adekvat och objektiv bild av sakfrågorna och kan diskutera dem på ett förnuftigt och öppet sätt. Till det demokratiska samhällets basförmåga hör en pluralistisk mediestruktur.

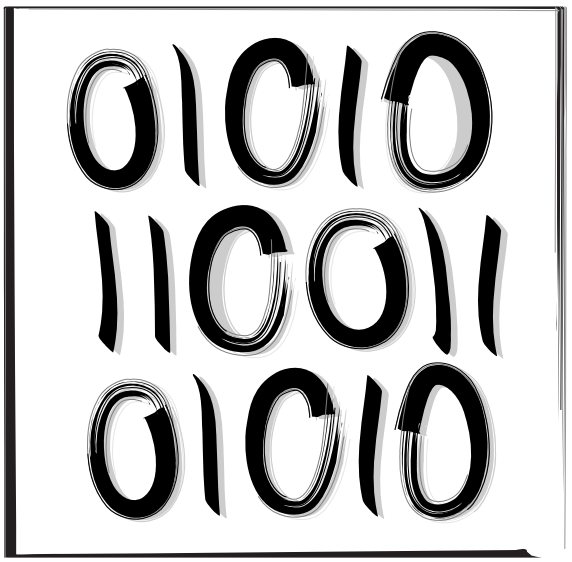
Medierna är den huvudsakliga kunskapskällan för individerna/medborgarna. Hur relationen medieinnehåll – mediekonsumtion ser ut är diffust men att medierna på sikt påverkar och t o m skapar opinioner i ett samhälle torde vara oomtvistat. Mediernas agenda och hur skeenden rapporteras i dessa, förklaras, diskuteras och kritiseras, påverkar åsiktsläget i olika frågor. Såväl mediemångfald som fri åsikts- och opinionsbildning är viktiga förutsättningar för det demokratiska samhällets existens. Massmedierna är en stark – den starkaste – psykologisk kraft i samhället inte bara i egenskap av nyhetsförmedlare och opinionsbildare utan också som sammanhållande kraft för samhällets kommunikationsströmmar. I en mycket allmän mening handlar kommunikation via massmedierna alltid om en transformation där något yttre blir till något inre, eller om något inre som blir till något yttre. Mediematerial i form av texter, bilder, föremål, rörelser, elektriska signaler, ljud och ljusvågor ges ett mentalt innehåll – ett *medvetandeinnehåll*. Sätten på vilket detta material presenteras har betydelse för om och hur vi tar till oss informationen, hur budskapen dechiffreras och vilken effekt detta får på vår bild av ”verkligheten”.

Försök till påverkan, opinionsbildning och annan styrning av vår verklighetsuppfattning utsätts vi mediekonsumenter dagligen för, alltifrån enkla reklambudskap till mer avancerad öppen eller dold propagandaverksamhet. *Kampen om tanken* är ingen ny företeelse, men medlen och teknikerna är idag mer förfinade än tidigare. Genast skall sägas att genom budskap eller i dialog försöka påverka eller rent av styra andras verklighetsuppfattning och möjligen i förlängningen också beteen-

den är helt legalt och behöver självfallet vare sig vara illasinnat, lagstridigt eller ens moraliskt förkastligt (verksamheter som t ex marknadsföring, försäljning, lobbyism, PR). Men man behöver inte ha en alltför livlig fantasi för att föreställa sig andra påverkanssituationer.

Informationsflödet och mängden intryck från en aldrig sinande medievärld blir allt kraftigare. Nya vägar öppnas ständigt till nya verkligheter, fakta och underhållning. *Mediemanipulation*, såväl av text, ljud som bild, är ett i sammanhanget välkänt begrepp. Sorteringsproblemen och våra begrepp om vilka mediernas uppgiftslämnare egentligen är blir allt svårare att hantera. Det är t ex mycket lätt att öppet, dolt eller maskerat sprida vilseledande, falsk, direkt lögnaktig information via Internet. Det är här som begreppet *informationsoperativa bakhåll* hör hemma. Medieutvecklingen går så fort och så djupt inpå den enskilde att många människor och institutioner upplever den som ett hot.

Begrepp som *påverkan* och *försök till påverkan, trovärdighet* och *förtroende* och *tillit* är viktiga begrepp inom området ”kampen om tanken”. I det sammanhanget är förstås begreppen *information* och *kommunikation* – budskap respektive dialog – självklara.



Varning, råd och anvisningar

Medierna, nyhetsmedierna, är emellertid inte bara den normala fataburen för vår omvärldsbevakning och kompassnålen i vår orientering. De har också en annan funktion, egentligen flera i ett demokratiskt samhälle, nämligen att ingå i samhällets varnings-, larm- och informationssystem. De bägge funktionerna kan till synes vara olika men tjänar i slutändan samma demokratiska mål.

Människan har i alla tider varit omgiven av fysiska risker och hot av olika slag. Många av dessa har varit väntade och synliga och därmed också i varierande grad kunnat åtgärdas. Vad som bl a kännetecknar samhället av idag är, att många risker och hot är obekanta, osynliga, oförutsägbara och därmed också opåverkbara av den enskilde själv. Ofta äger han eller hon inte tillräckliga kunskaper för att på egen hand ha kontroll på de risker och hot utvecklingen lett till och därmed har ansvaret för människors väl och ve allt mer lagts i händerna på andra (experter, politiker, kommentatorer med flera). Kravet på mediernas förmåga att agera i en krissituation som informationsförmedlare är omedelbart. Den medierade informationen om hotet eller riskens orsaker och om krishanteringen i sig, kan vara avgörande för krishanteringens effektivitet. Intressant här är de nya mediernas (t ex Internet, mobiltelefoni, sms) betydelse i sådana sammanhang.

Den upplevda *trovärdigheten* och *tillförlitligheten* hos medierna blir också här av central betydelse. Att som sändare effektivt ”nå ut”, att ha något som av mottagarna upplevs som relevant att säga, att mottagarna har förtroende för avsändaren och att informationskanalerna upplevs som trovärdiga och tillförlitliga av såväl sändare som mottagare är ett måste om försök till någon form av påverkan skall krönas med framgång. Detta gäller under normala vardagsförhållanden men speciellt vid samhällsstörningar när upplevda hot och risker måste ersättas med adekvat kunskap, råd och anvisningar.

I krishanteringssystemet – *krisberedskapen* – tillåts medierna ingen startsträcka utan ska idealt kunna agera omedelbart. Ställs samtidigt kravet att medierna ska vara vaksamma mot olika typer av manipulation krävs både kunskap och handlingsberedskap inom beredskapsområdet. Intuitivt tycker man att medierna själva borde ha ett intresse för det slaget av beredskap.

Kombination av funktioner

I det område SPF har att verka framträder massmedier tydligt som en av det demokratiska samhällets grundbultar där åtminstone två av deras roller sammanfaller: dels som en resurs i samhällets informations-, larm- och varningssystem, dels för upprätthållandet av en fri och oberoende nyhetsförmedling och opinionsbildning. De två funktionerna kan behandlas var för sig men ses lämpligen i kombination. Såväl i termer av ett samhälleligt sårbarhetstänkande som i våra enskilda, normala, dagliga liv är den kombinationen kanske viktigare och mer aktuell idag än någonsin tidigare! Ur ett beredskapsperspektiv är det väsentligt att i samråd med medierna utveckla förhållanden som skapar en acceptabel robusthet baserad på en väl underbyggd medvetande- och kunskapsnivå om sårbarheter inom mediestrukturen såväl på den offentliga som på den kommersiella sidan. Trovärdiga och tillförlitliga massmedier är i alla situationer grundläggande för ett demokratiskt samhälle.

Informationsoperativa bakhåll

Medvetna försök att påverka människor för att på så sätt skaffa sig fördelar har förekommit i alla tider. Formerna och verktygen för sådana försök har emellertid förändrats under historiens gång. Idag utgör inte bara människor måltavlan utan också informationsbaserade processer och system kan olika aktörer försöka styra till sin egen fördel. Sådana försök till påverkan behöver som tidigare sagts inte vara fientliga, kriminella eller ens skadliga utan är en normal del av vardagen.

Att massmedier, främst press, radio och TV, har stor betydelse som instrument för opinionspåverkan är helt klart. Väpnade konflikter t ex förs idag med både militära och mediala medel. Försök att styra och forma och att även manipulera opinioner är närmast en självklarhet för den stats- och krigsledning som har makt och kontroll över nyhetsmedierna. Propagandamakarens möjligheter att nå ut inte bara till hemmaopinionen och fiendesidan utan också till en större omvärld är idag bättre än någonsin genom den medietekniska utvecklingen. Tidigare upprätthöll man en gräns mellan krigstid och fredstida verksamheter. Idag är den gränsen diffus. Propagandainslag utformas ofta som en naturlig del i nyhetsförmedlingen, vilket vi sett många exempel på från konflikternas Balkan, från dagens Mellanöstern och Irak. Uppenbar cyberterrorism har vi ännu inte sett, men terroristorganisationers försök att t ex kombinera fysisk ödeläggelse med information och budskap över Internet, torde vara ett framtida scenario.

Den snabba teknikutvecklingen medför att informationsflödet och mängden stimuli från en outtömlig medievärld växer och växer. Nya tekniska vägar öppnas ständigt till nya verkligheter, fakta och underhållning. *Sorteringsproblemen* och våra begrepp

om *vilka* mediernas uppgiftslämnare egentligen är blir allt svårare att hantera. I ett växande flöde av nyheter, reklam och underhållning kan gränsen mellan självständig journalistisk rapportering och subtilt styrda budskap vara svår att se. Inte minst i en tid när hantverksmässig journalistik rationaliseras bort till förmån för industrialiserad nyhetsproduktion. *Det moderna mediesamhället är till synes den perfekta terrängen för informationsoperativa bakhåll*. Ju viktigare medierna blir för vår bild av världen, desto viktigare blir också dessa för aktörer inom ordinär t ex PR och lobbying och för aktörer med mer ”ljusskygga” mål för sina försök till påverkan. Det våldsamma informations- och kommunikationsflödet, underhållningsflödet, gör att det idag finns mycket att gömma sig bakom eller förklä sig till!

Globaliseringen har gett förändrade villkor för såväl medie- som nyhetsverksamheten, vilka bl a har genomgripande betydelse för journalistikens form och innehåll. Globala mediekonglomerat växer upp och lägger under sig många och skilda medier. Medielogiken styr rapporteringen. Redaktörsrollen blir också allt svårare att upprätthålla i en tid präglad av mediers sammansmältning och en expansion av nya kommunikationsredskap som inte är massmedier i traditionell mening. Gamla publicistiska ideal verkar få stå tillbaka för målsättningar av annat slag. Vem idag – medierna, medborgarna, mediekonglomeraten – avgör vad som är av ett ”oavvisligt allmänintresse”? *Infotainment* är ett aktuellt begrepp. Vad händer i ett samhälle (på sikt) när gränserna mellan information, kunskap, underhållning och kultur suddas ut? En synnerligen intressant fråga, som dock inte vidareutvecklas i detta sammanhang.

Människors mottaglighet för propaganda och lobbying och människors förmåga att genomskåda denna är en ödesfråga för det civiliserade samhällets utveckling. Det gäller bl a frågan om hur attityder, moraliska värderingar och beteenden påverkas, förändras och utvecklas över tiden – och vilka konsekvenser sådana förändringar i människors synsätt får på samhället och samhällsstrukturen, antingen i uppbyggande eller i negativt urholkande mening. Om allt fler människors verklighetsbild formas av krafter från reklam, underhållning, propaganda och lobbying, ”blogging”, är det uppenbart att det blir brister i den medborgerliga kunskaps- och idébildningen. Naturligtvis har detta betydelse för samhällsklimatet och samhällsberedskapen.

Att försöka styra bilden av verkligheten – Informationsoperationer

Begreppet *informationsoperationer* (IO) är ett överordnat begrepp för olika aktiviteter – fysiska, elektroniska, ekonomiska, militära, politiska och psykologiska – som idealt samordnas på en övergripande strategisk nivå. Begreppet står för olika former av riktade ”attacker” som möjliggjorts genom den snabba utvecklingen inom IT-området. Man brukar i sammanhanget tala om *hårda* fysiska delar (t ex rasera radiostationer) och *mjuka* psykologiska delar av informationsoperationer (t ex innehållsmässigt vinklade budskap). Avsikten med dessa aktiviteter är att styra

mottagarens/målets möjlighet att fatta rationella beslut genom att påverka beslutsunderlaget, det vill säga såväl informationens innehåll som dess bärare.

Sveriges regering har sedan några år definierat informationsoperationer. Ur Mats Bergströms studie *Informationsoperationer mot näringslivet* framgår bland annat följande (s 7):

> *Informationsoperationer är samlade och samordnade åtgärder i fred, kris och krig till stöd för politiska eller militära mål genom att påverka eller utnyttja motståndares eller annan utländsk aktörs information och informationssystem. Det kan ske genom att utnyttja egen information och egna informationssystem samtidigt som dessa också måste skyddas. Ett viktigt inslag är att påverka beslutsprocesser och beslutsunderlag. /…/*
>
> *Exempel på informationsoperationer är t ex informationskrigföring, massmediemanipulation, psykologisk krigföring och underrättelseverksamhet.*

Bergström lyfter fram några väsentliga aspekter vad gäller informationsoperationer: (1) IO förekommer över hela skalan – från fred, över kris till krig; (2) IO verkar genom att påverka eller utnyttja en motståndares information och -system, dvs både innehåll och bärarsystem/teknik; (3) IO påverkar, vilket kan sägas vara det yttersta syftet, beslutsprocesser och beslutsfattande; (4) IO är en angelägenhet för hela samhället (a.a. s 8). I övrigt hänvisas till Furustigs avsnitt i denna skrift.

I litteraturen om informationsoperationer hittas underordnade – ibland parallella – begrepp till sådana, t ex medieoperationer, informationsattacker, informationskampanjer och (i krig) psykologisk krigföring. Skillnader i upplägg och innehåll mellan dessa olika aktiviteter kan ibland vara svåra att ange på ett entydigt sätt. Detta kan naturligtvis skapa problem inte minst i samband med internationella insatser där de samverkande kan definiera aktiviteter på något olika sätt. Vad gäller medieberedskapen är detta problem mindre framträdande.

Begreppet IO, som har en militär bakgrund, rymmer i sig informationsteknologins möjligheter att utnyttja, påverka, undanhålla, överdriva, förändra eller förstöra informationen eller informationssystemen å ena sidan och, å den andra, skapa ett informationsinnehåll i syfte att t ex väcka eller påverka opinioner. Ett annat till sammanhanget hörande begrepp är *perception management* (perceptions- eller varseblivningsstyrning) som handlar om att på ett intelligent sätt påverka människors avsikter, känslor och beteenden genom att lägga till rätta, vinkla eller beskära verkligheten och/eller presentera en lögnaktig verklighetsbild.

Försök att direkt eller indirekt påverka andra har förstås förekommit i alla tider eftersom detta är en del i det sociala samspelet mellan människor. Detta innebär att begreppet informationsoperation måste användas försiktigt och får inte bli ett samlingsbegrepp för all form av påverkan. Bil- och modemässor, politisk propaganda, ordinär reklam och PR kan inte betraktas som informationsoperationer. Att i böcker eller på film humanisera diktatorer och krigshetsare kan inte heller

definieras som informationsoperationer. Att vandalisera eller slå sönder en informationsbärare är heller ingen informationsoperation. Operationer som avses här är sådana som syftar till att medföra att målet för aktionen inte uppfattar en förvanskad verklighet och som följd av detta fattar beslut som medför oönskade konsekvenser men som leder till fördelar för angriparen. För definitioner och övriga resonemang kring begreppet och exempel på informationsoperationer hänvisas till avsnittet om just informationsoperationer i denna skrift.

En generell definition som *skulle* kunna vara giltig för det nu aktuella projektet kan formuleras på följande sätt: ”*IO är sätt för en aktör att i en avsiktlig teknisk och/eller kognitiv påverkan via medierna uppnå ett kalkylerat inflytande över ett system eller annan aktör som medför effekter för dettas/dennes förmåga att återge eller registrera verkligheten. Avsikten är att på kort eller lång sikt skapa egna fördelar på andras bekostnad. Operationen kan vara unik men också samordnad med andra aktioner*”.

Hotbilder

Två, icke varandra oberoende eller uteslutande, IO-relaterade hotbilder kan skönjas vad gäller massmedier. Den ena gäller någon form av kollaps inom eller mellan de tekniska mediesystemen som alltså påverkar mediernas förmåga att producera och distribuera. Den andra avser risker för att medier utnyttjas kognitivt i vilseledande syfte genom att någon attackerar eller utnyttjar ”svaga punkter” hos medierna eller i mediestrukturen. Hoten kan också ses i kombination.

Sårbarheter

På mediesidan skall public service-företagen under normala betingelser ”stå i allmänhetens tjänst” men också enligt avtalen med staten ha beredskap att kunna verka så normalt som möjligt även under störda förhållanden. De privata medierna har utöver sina kommersiella mål även samhällsviktiga skäl att verka under s k svåra förhållanden, vid samhällsstörningar. Det synes väsentligt att för den privata och offentliga sektorn skapa en gemensam syn på behovet av säkerhet, beredskap, krishanteringsförmåga och samverkan inom mediebranschen. Gemensamma kunskaper om hot, risker, sårbarheter samt möjligheter att bistå varandra är nödvändiga förutsättningar för att under störda förhållanden – samhällsstörningar, kriser, katastrofer, ytterst krig – kunna agera adekvat, snabbt och effektivt. Inte bara samhället utan också medierna själva är betjänta av detta.

Här kan begreppet *rapporteringssäkerhet* föras in i bilden. Med det kan avses ett eller flera robusta system på olika nivåer i samhället för säker distribution och produktion av allehanda information och kommunikation. Säkerheten avser robusthet såväl i tekniskt avseende som innehållsmässigt och detta oberoende av situation.

Samhällets förmåga att skydda sig mot informationsoperationer är av flera skäl generellt sett låg. Ofta är ”man” på efterkälken – för sent ute. Möjligheterna att spåra angrepp är ofta små. Cyberrymden känner inga nationsgränser. Lagstiftning lägger inte sällan hinder i vägen för aktiva motåtgärder. Ett IT-incidentcentrum (SITIC) har dock etablerats vid Post- och telestyrelsen (PTS) som på olika sätt skall stödja samhället i arbetet med skydd mot IT-incidenter. Det ligger i sakens natur att samhällets möjligheter att ”avslöja” avsiktlig vilseledning, dvs mjuka informationsattacker, i en i allt väsentligt tillåtande mediemiljö är normalt små – vad är sant, vad är falskt? Vem känner sanningen? Samordnas attacken/-erna via medierna med annan påverkan är chanserna till avslöjande förstås större.

Projektets fortsättning

Vilka möjligheter ger – eller *skulle kunna ge* – dagens mediesamhälle den, som på ett avsiktligt tekniskt och/eller innehållsmässigt sätt önskar påverka eller manipulera sin omgivning med informationsoperativa förtecken? I vilken utsträckning har medierna förmåga att på dagens massmediemarknad upprätthålla en godtagbart robust rapporteringssäkerhet oberoende av situation?

Det är utifrån den problematiken de bägge följande studierna skrivits. Den ena gäller problematiken kring informationsoperationer via medier medan den andra är en diskussion rörande strukturella kännetecken i dagens mediestruktur. IO-hoten måste alltså identifieras och effekterna diskuteras. Vad är input? Vad är output? Hur och på vilket sätt kommer massmedier – eller skulle kunna komma – in som en faktor däremellan? Studierna måste på projektets nuvarande stadium ses som diskuterande och pekar ut riktningen för kommande forskningsinsatser.

Vem eller vilka som ligger bakom tänkbara hot kan variera från enskilda individer till hela stater eller skilda grupperingar inom dessa, företag, terrorgrupper. Självklart måste fortsatta hot- och aktörsanalyser göras i ljuset av informationsoperationer. Traditionellt inledande frågor i sådana sammanhang är: *vad* kan någon vilja göra? *Vem* skulle vilja göra detta? Har man *möjlighet* att genomföra aktionen? Det är också viktigt att bestämma ”nivån” på beredskapskraven, dvs vad det är robustheten skall täcka.

Är det möjligt att genom de IO-tekniker som lyfts fram i projektet attackera genom eller utnyttja strukturella egenskaper hos medierna i informationsoperationer? För att besvara sådana frågor krävs kompetens från flera håll, inte minst från – eller kanske framför allt från – medievärlden. Workshops är sannolikt rätt ansats för att studera sådana frågor. En diskussion av vilka beredskapsmässiga krav som *borde gälla* ingår också här. Den diskussionen sker bäst i dialog med företrädare för, framför allt, de kommersiella medierna.

Lyckas man identifiera egenskaper och förhållanden, *nyckelfaktorer*, hos medierna eller i mediestrukturen som aktörer skulle kunna utnyttja eller attackera i ett IO-sammanhang kan det sannolikt vara väsentligt – ur ett beredskaps- och sårbarhetstänkande – att lyfta fram dessa och följa över tid. Att empiriskt kunna mäta sådana faktorer eller förhållanden torde därför vara ett väsentligt mål. Sådana mätningar över tid kan då ligga till grund för bedömningen av medieberedskapen i landet och ge SPF vägledning rörande angelägen forskning inom detta medieområde.

Referenser

Delar av avsnittet har hämtats från eller inspirerats av följande texter:

Bergström, Mats (2004). Informationsoperationer mot näringslivet – hot mot nationell säkerhet?, Försvarshögskolan, Stockholm.

Ekdahl, Mats (2003). Människan, mediemångfalden och det öppna samhället – Historien om massmediernas pluralism och dess labyrintiska processer, Styrelsen för psykologiskt försvar, Stockholm.

Ekdahl, Mats, Lindmark, Göran & Stütz, Göran (2004). Informationskriget styr vår verklighet, FOI Framsyn nr 4.

Ekeblom, Mats (2002). Massmediernas beredskap och SPFs roll inom samhällets säkerhet och beredskap, stencil, Stockholm.

Gulliksson, Mikael (2003). Stäng fönstren och försök lyssna på radio, Mitthögskolan, stencil, Sundsvall.

Morge, Sara (1999). Krisinformation på Internet, Styrelsen för psykologiskt försvar, Utbildningsserien nr 3, Stockholm.

Nordlund, Roland (2000). Risk- och kriskommunikation: Myndigheter–medier–medborgare, I: Lidskog, Nohrstedt & Warg: Risker, kommunikation och medier – En forskarantologi, Studentlitteratur, Lund.

Riegert, Kristina (2002). Kampen om det kommunikativa rummet – Informationskrigföring under Kosovokonflikten 1999, Styrelsen för psykologiskt försvar, rapport nr 191, Stockholm.

Sjöstedt, Gunnar & Stenström, Paula (2002). Vilseledning på Internet – En analysansats, Styrelsen för psykologiskt försvar, rapport nr 183, Stockholm.

Tubin, Eino (2003). Förfäras ej – 50 år med det psykologiska försvaret. En biografi om en svensk myndighet, Styrelsen för psykologiskt försvar, Stockholm.

De refererade SPF-studierna och andra studier från SPF finns listade på myndighetens hemsida med adressen www.psycdef.se/Publikationer. Vissa publikationer kan hämtas hem i pdf-format. En projektförteckning återfinns också i bilaga 1 i biografin över SPF, ”Förfäras ej” utgiven år 2003.

Informationsoperationer via medier

Hans Furustig

Innehållsförteckning

Sammanställning av tabeller och figurer

Sammanfattning

Massmedier är de viktigaste kanalerna i samhället för att förmedla information. Olika aktörer kan emellertid ha intresse av att manipulera och störa den av medierna förmedlade verklighetsbilden. Möjligheterna att med olika medel påverka informationens innehåll och kommunikation är avsevärda. Det är därför viktigt att medierna bygger upp beredskap för att upptäcka och motstå penetrationsförsök och begränsa genomslagseffekten av informationsoperationer (IO), som normalt kännetecknas av negativa effekter för mottagaren.

Informationsoperationer är samordnade verksamheter i syfte att påverka motståndarens eller andra aktörers beslut till deras nackdel eller till sändarens fördel. Effekten av IO uppnås genom den planerade synergieffekten av ett antal olika ”nålstick”, en kombination av främst psykologiska (propagandistiska, missvisande, vilseledande etc) och tekniska (störande, fördröjande, penetrerande, belastande, blockerande, destruktiva etc) åtgärder i syfte att fabricera, dölja eller framhäva en avsedd verklighetsbild. Detta uppnås konkret genom att påverka källor och informationsinnehåll (saklighet, relevans, aktualitet, fullständighet) och olika hjälpmedel och teknisk infrastruktur (virtuella gränssnitt, elförsörjning, telekommunikation, datornät, datorprogram, databaser, satelliter) men även organisatorisk infrastruktur (”grindväkteri”, infiltration, rekrytering).

Syftet med IO beror av tidsperspektivet. Under en beslutscykel kan det exempelvis gälla att påverka ett ställningstagande, under en budgetperiod att svartmåla en produkt och under en mandatperiod att undergräva ett förtroende. Aktörerna återfinns på alla nivåer: stat, organisation, företag, nätverk, cell och individ. Om gränserna för vad som är tillåtligt och acceptabelt arbetssätt inom medierna skulle komma att förskjutas så att kriterier på gott arbete urholkas, försvåras tidig upptäckt av vilseledande information.

I löpande text återges korta exempel på olika former av IO. Exemplet ”Giftkatastrofen i Rhen” antyder att penetrationssårbarheten för medier inte får negligeras. Okritisk reproduktion av nyheter får inte ersätta granskning. Exemplen ”Fallet Emulex” och ”Pol Pot i Sverige” belyser att det skulle vara möjligt att med små medel och vid rätt tillfälle genomföra en IO.

IO kan motverkas genom att:

- *förutse* svagheter och angreppspunkter *genom* kompetensutveckling med sårbarhets- och hotbildsanalys, löpande omvärldsbevakning, utvärderingsverksamhet, stödjande forskning, utveckling av indikatorer, internutbildning samt genomförande av spel och åtgärdsprogram,
- *gardera och förmildra* sårbarhet, penetration och genomslagseffekt *genom* utveckling av strategi och policy, tekniskt skydd, reservförfaranden, kristeam samt genom övning och samverkan.

Inledning

Massmedier har en viktig uppgift när det gäller att informera. De når snabbt sina målgrupper, har påtaglig genomslagskraft och gynnas i övrigt av den kommunikationstekniska utvecklingen. Såväl press, radio, TV som Internet hämtar information från varandra, vilket kan leda till informationsmässig ”rundgång”. Alternativen för den som vill skaffa sig information på andra vägar är därmed begränsade, vilket har gjort att informationskonsumentens beroende av massmedierna har ökat och möjligheten till kritisk värdering av informationen kan ha försvårats. Det gäller inte bara för den enskilde konsumenten utan även för resursstarka aktörer. Tänk exempelvis på *CNN*s genomslagskraft i samband med bildexponeringen av amerikanska soldater som skändades i samband med operationen i Somalia i oktober 1993. Den kraftiga reaktionen från hemmaopinionen bidrog till den amerikanska urdragningen. Informationsförmedling spelar helt enkelt en viktig roll i vårt moderna samhälle. Det är därför olika aktörer, legitimt eller icke-legitimt, använder sig av medier som kanal för att påverka tittare, läsare och lyssnare.

Det bör emellertid påpekas att påverkan ofta är positiv. Utbildning, nyhetsförmedling, upplysning och samhällsbevakning är exempel på sammanhang där påverkan är önskvärd i synnerhet om konsekvensen är ökad kunskap och medvetenhet. Samtidigt finns det risk att önskvärdheten i sig kan leda till att både producerande och konsumerande parter kanske inte alltid är på sin vakt mot vaga källor och försåtlig manipulering från särintressen.

Manipulativ påverkan kan nämligen ge en skev verklighetsbild som i värsta fall försämrar förtroendet för utvalda målgrupper eller leder till att viktiga beslut påverkas på felaktiga grunder. Det är därför viktigt att upptäcka och försvåra manipulation av information, till exempel i sammanhang som påverkar den allmänna opinionens kännedom om viktiga händelser samt värderingen av olika aspekter i det egna samhället och samhällsskicket. Medierna behöver ha beredskap för att upptäcka försök till manipulation av information och informationsförmedling och även konsumenterna behöver ha en källkritisk grundinställning.

Med hjälp av modern teknik kan medierna förmedla nyheter i nära nog realtid (*instant news*) och spridningen kan vara global. Ursprunget till en bild, ett reportage eller en text kan emellertid ibland vara oklar. Är det en av särintressen influerad kanal (bildbyrå, radiostation, TV-kanal, webbplats) eller producent som ligger bakom spridningen av en viss nyhet? Det är risk att mediernas tid för källkritik, analys och eftertanke minskar på grund av ökad konkurrens samtidigt som det tillgängliga informationsflödet, och bruset, ökar. Dessutom tillkommer nya aspekter att beakta vid bedömning av information från Internet. [1]

Det leder till källkritiska problem både för producenter och konsumenter av information.

---

[1] Leth & Thurén (2000).

Med information*[2] menas här den meningsfulla innebörd som kan utvinnas ur data eller som finns i ett meddelande eller en kommunikation. Det är inte självklart att information i sig är värdefull; i samband med nyheter ska information exempelvis vara relevant, aktuell och sakligt korrekt. Resultatet kan emellertid oavsiktligt i delar bli partiskt eller missvisande därför att producenternas överblick av återgivna händelser och samband är ofullständig och osäker. Det är här det kan bli problematiskt, i synnerhet om situationen utnyttjas av särintressen.

Det har alltid förekommit medvetna försök att påverka den allmänna opinionen eller särskilda nyckelpersoner. Tänk på den gråtande flickan som på TV berättade hur irakier tagit sig in i ett kuwaitiskt sjukhus och där slitit spädbarn ur kuvöser. I själva verket, visade det sig senare, var flickan den kuwaitiske USA-ambassadörens dotter och barnen i fråga hade avlidit på grund av sjukhusets bristande resurser under kriget mot Irak. Den amerikanska administrationen hade anlitat specialföretag för att säkra allmänhetens stöd inför det förestående militära ingripandet mot Irak år 1991. Det gällde också att påvisa att kuwaitierna var eniga och beredda att kämpa för att befria sitt angripna land. För det syftet anlitades flera olika PR-byråer och reklamföretag i en samordnad operation. PR-byrån Hill & Knowlton samordnade, Ketchum PR-byrå arbetade för att skapa opinion, Wirthlin Group prövade olika utspel mot testpaneler och genomförde intervjuer och MediaLink skapade bildmaterial och distribuerade detta till medierna.[3]

Företag som arbetar med public relations anlitas ibland av statliga uppdragsgivare eller kommersiella intressen för att med massmedier som kanal påverka den allmänna opinionens verklighetsbild av något skeende, någon inträffad händelse eller något varumärke. För några år sedan anlitades exempelvis PR-företag för att stödja kinesiska myndigheter i kontakterna med internationella massmedier i syfte att ge en fördelaktig bild av Kina inför pågående förhandlingar om ett handelsavtal med USA.[4] Man ville komma ifrån bilden av förföljelser mot oliktänkande och skapa bättre mediekontakter. Sammanblandningen av yrkesrollen att granska och förmedla information med rollen att propagera och argumentera leder till att mottagaren får svårare att särskilja nyhetsförmedling och partsinlagor, vilket kan påverka opinion och beslutsfattare på ett försåtligt sätt.

Om privatpersoner med bildsändande mobiltelefoner och hemsidor på Internet agerar som frilansare är det tänkbart att informationsmaterial med osäker äkthet sprids till bildbyråer, nyhetsbyråer och massmedier och därigenom når en större publik, vilket kan påverka mediernas trovärdighet på sikt.

Inför en konferens om informationsoperationer i England år 2004 fastslogs att metoder som förknippas med begrepp som *perception management, strategic*

---

[2] För att underlätta läsningen finns en ordlista i slutet av denna rapport. Där återfinns ord som försetts med asterisk (*) vid första användningen i texten.

[3] *STV 2 Dokument utifrån*, 1992-03-28. Referat i Furustig, Ljunggren & Unge (2001b), sid. 35-37.

[4] *Dagens Industri*, 1994-03-24, sid. 56.

influence och *psychological operations* kommer till ökad användning i dag. Perception management handlar dels om att fokusera mot en sann men utvald verklighetsbild (lägga tillrätta), dels om att projicera en osann verklighetsbild (leda vilse). Målgruppen för strategisk påverkan kan bestå av opinioner, främmande statsledningar, policyrådgivare och maktcentra [5]. Om påverkan är försåtlig eller om information kan vara manipulerad finns det skäl att vara på sin vakt. Ljud, bild och text har förvisso makt att påverka både sinne och tanke.

Motsatsen, frånvaro av information i en situation där information efterfrågas, påverkar också konsumenten. Osäkerhet uppstår helt naturligt i den situationen och i värsta fall kan rykten komma att spridas och utgöra ersättning för nyheter i kritiska situationer. Det gäller även om ljud- och bildkanaler ”går ner” på grund av störningar eller avbrott. Ungefär samtidigt som detta skrivs råkade SVT ut för ett sändningsbortfall under ca 40 minuter på flera kanaler över hela landet [6], Svenska Dagbladet m fl drabbades av ett lokalt strömavbrott i centrala Stockholm under ca 3 timmar [7], ett större strömavbrott i nordvästra Stockholm berörde bland annat tidningstryckerier under ca 90 minuter [8], och datormasken Sasser har drabbat myndigheter, företag och privatpersoner världen runt.[9] Ett sändningsbortfall från etermedierna under en händelsemässigt kritisk period skulle kunna få allvarliga psykologiska konsekvenser, utebliven tidning på grund av ett eller annat tekniskt fel föranleder prenumeranterna att kasta sig på telefonen och angrepp av hackers* eller crackers* via Internet vållar globala kostnader och olägenheter. En smula tillspetsat riskerar vi att bli både missledda och störda till och med under normala förhållanden, såvida myndigheter och medier inte förutsett eller tillräckligt väl förberett sig för olika typer av tekniska störningar och informationsmässiga angrepp.

Den svenska statsmakten har länge studerat utvecklingen inom ledningskrigföring och informationskrigföring. Det är därför relevant att kort återge några grundtankar i det aktuella synsättet på informationsoperationer [10] (IO). *Informationsoperationer* beskrivs som samordnad verksamhet genomförd i syfte att påverka motståndarens eller andra aktörers beslut (underförstått: på ett sätt som gynnar sändarens intressen och/eller är till mottagarens nackdel). Under fredstid och kris riktar sig IO i huvudsak mot politiska, ekonomiska och tekniskt-vetenskapliga arenor. I en proposition [11] definierades IO på följande sätt:

---

[5] Richelson (2003), sid. 64-69.

[6] 2004-04-27 omkring klockan 19.00.

[7] *Svenska Dagbladet*, 2004-05-08, sid. 8.

[8] Hellberg & Ellemark: ”Stort strömavbrott i nordvästra Stockholm”. Hämtat från *Dagens Nyheters* nätupplaga. Internet www.dn.se 2004-05-04.

[9] *Svenska Dagbladet*, 2004-05-07, sid. 10.

[10] Utkast till ”Försvarsmaktens Grundsyn Informationsoperationer, IO”. Fastställt 2003-12-11 av HKV med beteckning 01 600:78657.

[11] Proposition 1999/2000:86 ”Ett informationssamhälle för alla”.

Informationsoperationer är samlade och samordnade åtgärder i fred, kris och krig till stöd för politiska eller militära mål genom att påverka eller utnyttja motståndares eller annan utländsk aktörs information och informationssystem. /.../ Exempel på informationsoperationer är t ex informationskrigföring, massmediemanipulation, psykologisk krigföring och underrättelseverksamhet.

De metoder som kan komma till användning under fredstid är elektroniska angrepp och ingrepp i vid bemärkelse (här kallade tekniska åtgärder) samt påverkan genom avsiktlig vilseledning* och psykologiska operationer* (här kallade psykologiska åtgärder). Under krigsliknande förhållanden tillkommer maktutövning med våld genom fysisk bekämpning och sabotage.

Informationsoperationer syftar till påverkan av specifika målgruppers uppfattning och attityd, påverkan av förtroendet för vissa aktörer, vilseledning av beslutsfattare och andra aktörer samt bekämpning av utvalda strukturer och nätverk, exempelvis för kommunikation och kraftförsörjning. Åtgärderna kan kombineras och riktas både mot tekniken i motståndarnas system (struktur, hårdvara och mjukvara) och mot människorna i systemet.

Psykologiska operationer är planerade aktiviteter för att förmedla utvalda budskap och signaler till målgrupper såsom motståndarens regering, befolkning, utvalda organisationer eller nyckelpersoner. Budskapen avser att förstärka attityder som är gynnsamma för avsändaren.

Militär vilseledning har definierats som 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. [12] Bortses från uttrycket ”vår strid” kan grundtankarna ovan vara tillämpliga även för vilseledning i det civila samhället under fredstida förhållanden. För övrigt kan gränsdragningen bli relativ. Sverige kan befinna sig i fred, men samtidigt vara involverat i ett internationellt FN- eller EU-uppdrag med militär trupp engagerad i psykologiska operationer i mållandet, operationer som kan tänkas få överspridningseffekter till hemlandet.

Informationsoperationer är tillämpbara under alla faser av en löpande konfliktskala i avsikt att genomdriva något prioriterat mål:

Förhandling & Övertalning —> Tvång & Hot —> Demonstrationer & Våld

I det moderna samhället överlappar olika konfliktfaser varandra; konflikt kan råda inom en avgränsad arena utan att beröra andra arenor. Ett exempel på internationell nivå kan vara de återkommande handelspolitiska konflikterna mellan EU och USA, vilka dock hittills inte berört den ännu viktigare säkerhetspolitiska arenan.

---

[12] Vilseledning. Broschyr från 1998, Försvarsmakten 7741-716001.
PM Vilseledning 1997-12-15 HKV 21 120:73579.

Vid intressekonflikter försöker parterna få den allmänna opinionens förståelse och kanske också skildra motparten i mörkast tänkbara färger. Det blir en kamp med information som vapen och där massmedierna utgör spelplan.

Massmedier har således en viktig roll, inte bara vid nyhetsförmedling utan även som potentiell kanal vid IO. Vid IO riskerar kommunikationen att ske på sändarens villkor, medierna att bli utnyttjade och mottagarna att bli manipulerade. Medier kan dessutom av konkurrensskäl tvingas återpublicera uppseendeväckande men osäker information som exponerats av andra medier eller på Internet.

Hur relevant är IO som hotbild*? Enligt en bedömning [13] kommer hotet från alternativa angreppsformer att bestå eller öka. IO är en alternativ angreppsmetod. Exempel på känsliga mål för attacker kan vara beslutsfunktioner, telekommunikationer, energiförsörjning och informationssystem. Det pågår därför forskning om hot mot civil infrastruktur (IT, tele) vid Totalförsvarets Forskningsinstitut, FOI. [14] Ett sådant angrepp kan beröra samhällets säkerhet. Det skulle också drabba massmediernas förmåga att inhämta, bearbeta och distribuera nyheter.

Olika expertbedömningar av nuläget är intressanta. Här följer några exempel när det gäller IT-relaterade manipulationer, det vill säga vad som skulle kunna vara tekniska åtgärder vid IO.

> ...Rådgivnings- och kontrollverksamheten har under det gångna året i ännu större utsträckning kunnat konstatera att de största svagheterna hos myndigheter i dag är IT-relaterade... Den enkla åtkomsten av information gör det lättare för en potentiell angripare... (SÄPO [15])

> ...Brister finns inom elförsörjning, telekommunikationer, IT samt beredskap mot massförstörelsevapen, det vill säga inom de områden som prioriterades i Planeringsinriktningen för det civila försvaret 2003... (KBM [16])

En internationellt inriktad studie av IT-säkerheten vid ledande företag inom finansiell service visade att 83 % av företagen under år 2003 hade attackerats elektroniskt utifrån, jämfört med 39 % enligt motsvarande studie år 2002. Ca 40 % av de attackerade angav att störningarna medfört finansiell skada. Den procentuella ökningen är värd att notera. [17] Undersökningen berör företag som, i likhet med medieföretagen, kan ha särskild anledning att skydda sina informationstillgångar.

---

[13] Bergström (2004).

[14] *Ny Teknik* 2004-09-29, del 2, sid. 8.

[15] Säkerhetspolisen verksamhetsåret 2003, sid. 41.

[16] Hamilton (2004): ”Ej godtagbar förmåga.” Sammanfattning från KBMs årliga uppföljning av samhällets förmåga att hantera svåra påfrestningar i fred hämtad från Internet www.krisberedskapsmyndigheten.se, 2004-05-15, ”visa nyhet”.

[17] Global Security Survey 2004 genomförd av företaget Deloitte. Internet http://www.deloitte.com.

Nydén gör i sin studie en bedömning avseende risken för psykologiska åtgärder riktade mot nationella intressen och anser att

> ...Risken är också stor att vi inte ser riskerna för desinformation och propaganda inom våra egna samhällssystem om vi fortsätter att fokusera på en yttre fiende... (SPF [18])

Det är dessa och liknande aspekter som denna studie kommer att handla om. Syftet är bland annat att väcka eftertanke om behovet av att medierna har beredskap mot avsiktlig informationsmanipulering.

[18] Nydén (1995), sid. 38.

Utgångspunkter och avgränsning

I det här avsnittet förs en diskussion om tänkbara tillvägagångssätt vid informationsoperationer där medier utnyttjas för manipulation av verklighetsbilden. Syftet är att väcka eftertanke om hur realistiska sådana informationsangrepp kan vara och att bidra till en diskussion om hur mediernas rapporteringssäkerhet skulle kunna säkras.

Med *medier* avses här i första hand press, radio och TV. Det finns anledning att inkludera Internet i detta sammanhang, därför att nätet bland annat används för att distribuera medienyheter. Manipulering syftar i första hand på att medier utsätts för en informationsoperation utifrån. Det hindrar inte att medier själva kan initiera missvisande information, exempelvis på grund av arbetssätt, tidsbrist eller andra resursbegränsningar. Förhållanden som avsiktligt kan missbrukas och utnyttjas av någon fientligt sinnad aktör bör identifieras i preventivt syfte.

Det är möjligt att analysera informationsoperationer ur angriparens perspektiv: Vad är syftet, hur går en informationskrigare tillväga för att upptäcka lämpliga angreppspunkter och med vilka medel kan en informationsattack genomföras? Det är också möjligt att se det hela ur offrets synvinkel. Om det nu skulle finnas en angripare – vem skulle det kunna vara och varför? Om den frågan kan besvaras på ett trovärdigt sätt skulle naturligtvis motivet att skydda sig mot informationsoperationer öka. Kan egna sårbarheter förutses? Vilka principiella handlingsalternativ har en eventuell motståndare? Kan offret ha en strategi för att skydda sig? Det perspektiv som väljs här är försvararens, den som kan bli utsatt för en informationsattack.

Under hela historiens gång har människor bedrivit maktutövning med mer eller mindre acceptabla metoder för påverkan. Under världskrigen och under det kalla kriget förekom ett stort antal vilseledningsoperationer, psykologiska operationer och så kallat ”aktiva åtgärder”, som finns dokumenterade. Efter det kalla krigets slut har utvecklingen när det gäller militär teknik och doktrin fortsatt och satt sina spår i benämningar såsom manöverkrig, ledningskrig och informationskrig. Objektet för verksamheten, *homo sapiens*, har samtidigt förändrats mycket litet under de senaste årtusendena. Det är därför inte nödvändigt att ”uppfinna hjulet igen”. De grundläggande mekanismerna för manipulering och påverkan är fortfarande de samma och kan därför behandlas principiellt. Vad som däremot i hög grad har förändrats är tekniska hjälpmedel och spelregler i olika sammanhang. Därför finns det motiv att sammanfatta några allmängiltiga mekanismer som kan utnyttjas vid försök att påverka och som således skulle kunna användas vid IO.

Det är vanligt att man inom sjukvård, polisiär verksamhet och underrättelsetjänst försöker spåra tecken på oönskad verksamhet så tidigt som möjligt. Ett sätt är att identifiera indikatorer på den oönskade verksamheten eller dess tidiga effekter. Den här studien utgår från ett liknande tankesätt.

- Det finns *aktörer* som har rationella *motiv* att påverka en målgrupp.
- De väljer i så fall *tillvägagångssätt* bland annat beroende av objektets *sårbarhet*.
- Samband mellan aktör –> tillvägagångssätt –> *indikator* möjliggör upptäckt och åtgärd.

När det gäller sårbarhet [19] i samband med informationsoperationer förefaller det praktiskt att särskilja (1) sårbarheten vid intrång eller tillträde i ett system, respektive (2) sårbarheten vid genomslag i systemet. Genom massmediesystem uppnås en genomslagseffekt både på målgruppen i egenskap av mottagare av en missvisande verklighetsbild och på den förmedlande kanalen på grund av den bad-will som det innebär att få försämrad trovärdighet på sikt.

Problematisering

Manipulativ påverkan avser att skapa en tillrättalagd, felaktig eller ofullständig verklighetsbild, det vill säga vara avsiktligt vilseledande eller missvisande. Sådan påverkan är inte acceptabel, med några möjliga undantag. Kan det finnas speciella ekonomiska och säkerhetspolitiska situationer där nationens bästa kräver en temporär nödlögn från myndigheter eller politiker? Antag att det förestår en ränteförändring från Riksbanken som in i det sista måste döljas för att förhindra fientlig spekulation, att det pågår någon utrikespolitiskt känslig förhandling där vissa spelkort måste framhävas medan andra hålls dolda, att säkerheten för människoliv äventyras om känslig information läcker ut vid fel tillfälle till fel personer, att liv besparas om information försenas, undertrycks eller ”anpassas” till en operativ situation. Även om det tydligen kan konstrueras situationer där manipulation av information vore acceptabel eller till och med nödvändig, gäller generellt att information ska vara aktuell, relevant, korrekt och så långt möjligt fullständig. Det måste vara rättesnöret!

Det kan inte uteslutas att en manipulativ effekt kan uppkomma ”oavsiktligt” genom samverkan av oskyldiga förhållanden, exempelvis tidsbrist, informationsbrus, resursbrist, bristfällig källkritik, objektivitet och naivitet. Det kan således finnas en gråzon där slutprodukten någon gång blir informationsmässigt otillfredsställande, men där det likväl inte behöver finnas någon ondskefull avsikt att vilseleda. Speciella omständigheter, exempelvis medias stressade arbetssituation, skulle kunna bidra till detta. Det *har* förekommit att missförstånd, tillfälligheter och speciella omständigheter har lett till att inkommande information inte har kontrollerats på föreskrivet sätt eller att utgående information blivit missvisande, skapat oreda eller oavsiktligt fått karaktär av rykte [20].

---

[19] Sjöstedt (1992). Sjöstedt belyser begreppen tillträdessårbarhet och genomslagssårbarhet.

[20] Exempel på bristfälligt kontrollerade inkommande uppgifter redovisas av Hanses & Tellström (1990). Exempel på ryktesspridning ges av Stütz & Tubin (1991).

En manipulativ effekt kan skapas avsiktligt utan något ont uppsåt. Det kan ske i underhållningssyfte (s k *infotainment*) och delvis förkläs till nyheter. Det har skett flera gånger att gränsen mellan underhållningsprogram och nyhetsprogram missuppfattats av lyssnare eller tittare. Ett klassiskt exempel är CBSs utsändning av radiodramatiseringen av Orson Wells *Världarnas krig* år 1938, som skapade lokal panik bland radiolyssnare i dåtidens USA. Ett helt annat exempel är konspirationsteorier som givits halvdokumentär form, exempelvis den om den första månlandningen. Ett antal indicier presenterades på ett trovärdigt sätt för att denna aldrig inträffat, utan var fejkad. Hos många TV-tittare uppstod en osäkerhet om vad som egentligen var sant.

I princip skulle det kunna vara fördelaktigt för den som vill påverka, att skapa en situation som i efterhand ser ut som ett förklarligt misstag eller ren naivitet för att därigenom dölja avsiktligheten bakom ett agerande. Ett led i professionellt utförda operationer är nämligen att dölja spåren eller att lägga ut falska spår för senare efterforskningar, om det är så att vilseledningen inte bör kunna avslöjas ens i efterhand. Det är därför som det är svårt att finna goda exempel på väldokumenterade och moderna vilseledningsoperationer.

Det kan kanske förefalla som om resonemanget ovan enbart berör psykologiska åtgärder som vilseledning och propaganda m m. Det har emellertid tillämpning även i tekniska sammanhang. När det inträffar avbrott eller störningar i tekniska system av typen energinätverk eller informationsbärande nätverk kan orsaken hänföras till endera extrem miljöpåverkan, konstruktionssvaghet, handhavandefel eller avsiktlig åverkan. Sabotage kan teoretiskt döljas genom simulering av någon möjlig teknisk felorsak eller ett möjligt operatörsfel. Konkreta situationer som orsakat informationsbortfall eller störningar kan därför vara lärorika att studera, inte bara för att förbättra arbetsrutinerna, utan också för att därigenom minska sårbarheten och försvåra manipulation genom psykologiska och/eller tekniska åtgärder.

Avgränsningar

Det finns en mängd situationer där varierande grad av informationspåverkan och våldsutövning förekommer. Kontexter där psykologiska och tekniska åtgärder överväger är exempelvis inom reklam, public relations, propaganda, perceptionsstyrning, underrättelsekrig, ekonomisk krigföring och politisk krigföring. Kontexter där även fysiska metoder med inslag av våld och destruktion förekommer i ökad utsträckning är exempelvis lågintensitetskonflikter, terroristverksamhet, internationell organiserad brottslighet och olika typer av militära insatser till och med fullskaligt krig. Gemensamt för alla dessa situationer är att IO med en kombination av psykologiska och tekniska åtgärder är tänkbara, sannolika och delvis nödvändiga över hela skalan. (Det är naturligtvis stor skillnad i hur önskvärda eller legitima olika åtgärder är under skilda konfliktnivåer, men det är en annan sak.) Vissa av kategoriseringarna ovan är överlappande och vaga, men likväl består

intrycket att psykologiska och tekniska åtgärder kan användas för att beskriva insatserna under ett flertal situationer på en tänkt konfliktskala.

Därför avgränsas den fortsatta analysen av IO till en kombination av psykologiska och tekniska åtgärder.

IO under krig behandlas inte här, då ledningskrigföring med informationskrigföring redan studeras inom statsmakten. Vissa konfliktfaser kan vara besvärliga att särskilja formellt när det handlar om internationella kriser. Exempelvis kan indikationer på ekonomisk konflikt och militär harmoni föreligga samtidigt. Formella beredskapsnivåer, som av tradition kopplats till graden av konfliktnivå i omvärlden, är därför mindre relevanta i denna diskussion, även om det är så att den förväntade frekvensen av IO rimligen ökar med högre grad av konflikt. Det innebär att när svenska medier rapporterar från internationella insatser och krigshändelser från utländska arenor är sannolikheten stor att medierna exponeras för någon form av IO från berörda parter i konflikten.

Medieföretag kan vara statliga, privata och kommersiella. Beroende av ägarstruktur har medier tecknat olika avtal med staten vilka reglerar spelregler och ansvar i kritiska situationer. Public serviceföretag har helt naturligt andra förväntningar att leva upp till jämfört med kommersiella företag. Sådana skillnader, formella eller efterfrågestyrda, kan ha betydelse för vilken typ av påverkan specifika medieföretag förväntas bli exponerade. Dessa förhållanden vägs inte in i den här delstudien, utan bör analyseras av respektive medieföretag i samband med lokal sårbarhetsanalys. Riskbedömning och medvetenhet om den egna sårbarheten behöver sedan kompletteras med motåtgärder för beredskap mot informationsattacker.

Genom skilda kanaler (radio, TV, sms, tryckeri, Internet etc) och spridningsvägar (kabel, länk, satellit etc) nås olika delar av landet och olika stora målgrupper. Även för en specifik kanal, exempelvis olika typer av radiosändningar, finns skilda spridningssätt och varierande yttäckning. Möjligheterna att tekniskt manipulera och störa sändningar varierar med dessa skilda förhållanden. De resonemang som förs här är principiella och beaktar inte de säkerhetsmässiga konsekvenserna av olika tekniska lösningar för skilda kanaler och spridningssätt. Även sådana aspekter vägs med fördel in av enskilda medier. Fokuseringen här är mot manipuleringen av mediernas information.

För att uppnå bästa möjliga totaleffekt av en informationsoperation (mer därom senare) måste psykologiska, tekniska och strukturella åtgärder inte bara planeras utan även samordnas. Manipuleringen kan med andra ord bestå av en avvägd kombination av psykologiska och tekniska åtgärder, samt utnyttjande av strukturella förhållanden. *Psykologiska* aspekter påverkar hur en individ uppfattar och tolkar inkommande information. Dit hör således innehållet i, utformningen och presentationen av ett budskap. *Tekniska* aspekter kan exemplifieras med intrång i system, störning eller förvrängning av datorprogram, signaler, programinnehåll och signalöverföring, samt mottagarnas mottagning. *Strukturella* avser exempelvis mediernas

organisationsform som kan påverka hur den inkommande informationen hanteras, bearbetas, paketeras och sprids. I en skarp informationsoperation kombineras och koordineras olika åtgärder. Den manipulering av information som avhandlas i denna delstudie är således i huvudsak psykologisk och teknisk. Ytterligare aspekter som inte behandlats närmare i denna studie är följande.

Rapporteringssäkerhet vid naturliga störningar
Studien har fokuserats mot hotet från avsiktliga (antagonistiska) störningar, typ informationsoperationer. Rapporteringssäkerheten är också beroende av mediernas robusthet mot olika former av naturliga störningar, till exempel: naturkatastrofer (översvämningar, stormar, stora elektromagnetiska störningar från solstormar), svåra olyckshändelser (miljökatastrofer, explosioner, felkonstruktioner, mänskligt felhandlande) samt bristsituationer (elavbrott, batterier, frekvensutrymme, tryckfärg, tidningspapper).

Avsiktlighet och tillåtlighet
Illasinnat eller brottsligt agerande blir ofta av nödvändighet systematiskt. Därmed kan sådant agerande eventuellt upptäckas och spåras. Men människor har självklart rätt att göra enstaka felbedömningar, misstag eller agera i god tro. Dessutom kan situationer skisseras där det goda handlingssättet inte är självklart, varken moraliskt eller juridiskt. Det kan också föreligga värderingsskillnader i vad som är god praxis inom yrkeskåren. Det kan inte uteslutas att tveksamheter i vad som är tillåtet (juridiskt, moraliskt, professionellt) kan utnyttjas i ekonomiskt, politiskt eller ideologiskt syfte. Några få hypotetiska exempel har nämnts i samband med gråzonsagerande. De juridiska frågorna har dock inte diskuterats närmare (se avsnittet om vilseledningsaspekter). Om och när är det straffbart respektive tillåtligt att desinformera och sprida rykten? Det är uppenbart att frågan om avsiktlighet är kritisk. En IO kan få konsekvenser inte bara för den nationella säkerheten utan även på regional och global nivå. Kanske finns det därför behov av global lagstiftning (eller strategi) rörande IO. Nyhetsförmedlingen har dessutom global och inte enbart nationell räckvidd.

Osäkerhet och policy
Inför ett beslut eller ställningstagande är det inte ovanligt att beslutssituationen kännetecknas av för mycket information, för litet information eller ont om tid (vad är sant, vad är relevant i allt brus, är det aktuellt etc). Vid informationsoperationer gäller det att upptäcka vad som pågår och besluta om motåtgärder, samtidigt som motaktörer försöker dölja sin verkliga verksamhet och på olika sätt sprida falsk säkerhet om felaktig eller motstridig information och sprida osäkerhet om korrekt information.

Omvärldsutvecklingen kan i sig dessutom vara sådan att osäkerhet råder om spelreglerna i den givna situationen. I en sådan extrem situation är det viktigt att

det finns en allmän handlingsberedskap, någon form av strategi och policy, samt ett nätverk av samverkande kollegor och myndigheter till stöd och ledning.

Skillnader mellan olika medier
Medierna kommunicerar genom helt olika kanaler och spridningsvägar. Som tidigare påpekats i samband med studiens avgränsning har de principiella resonemang som förts här inte avsett att väga in dessa väsentliga skillnader i arbetsförhållanden och sårbarhet.

Strategisk manipulering
Strategiska informationsoperationer bemöts sannolikt på högsta nivå inom företag och statsledning, kanske även inom EU. Aspekter som berör långsiktig undergrävande eller statsfientlig verksamhet kan tangera gråzonsagerandet, liksom att långsiktigt och avsiktligt på ett fördolt sätt försöka vända människors värderingar och attityder. Dessa aspekter har inte närmare behandlats här.

Underlag och framställningssätt

Mycket har tidigare skrivits om vilseledning, psykologiska operationer och olika former av IT-krigföring av Försvarets forskningsanstalt, Totalförsvarets forskningsinstitut, Utrikespolitiska Institutet, Styrelsen för psykologiskt försvar, Försvarshögskolan och Högkvarteret m fl. Motsvarande material har också under ett antal år cirkulerat i internationella publikationer och kurser, i synnerhet under kalla kriget. I den här studien har avsikten inte varit att sammanfatta detta material, även om författarens medverkan i olika studier och kurser helt naturligt satt sina spår, på gott och ont. Det är nämligen risk att det går trender i den säkerhetspolitiska debatten (liksom i andra debatter), att vissa tankegångar går rundgång på den internationella arenan och att det uppstår låsningar i tankesätt och terminologi.

Rapporten bygger på publicerade fallstudier och exempel – någon formell sammanhängande teoretisk ram kan man däremot knappast tala om. Det har efterhand utkristalliserats och publicerats tillvägagångssätt inom området. Även om syftet här inte är att lära ut vilseledning eller propaganda så ökar möjligheterna att skydda sig mot informationsmässig manipulering om något är känt om hur angripare kan tänka och agera. Här och var i texten finns korta verkliga eller belysande exempel insprängda. Däremot har utförligare fallstudier[21] valts bort, eftersom de oftast hänför sig till krigsförhållanden eller kalla kriget. Man kan lära sig av tidigare erfarenheter, men det är också viktigt att blicka framåt i en förändrad tillvaro.

Antag att det finns en angripare, konkurrent eller antagonist som genom rationell analys identifierar en motståndare eller ett offer. Angriparen formulerar strategiska och operativa mål för angreppet och bestämmer efter inhämtning av fakta

[21] Exempel på sådana fall finns sammanställda i Furustig, Ljunggren & Unge (2001b).

om motståndarens svagheter och lämpliga angreppspunkter att genomföra en IO. Med stöd av en ”verktygslåda” väljs tillvägagångssätt och en plan för operationen upprättas. Motparten, offret, analyserar å sin sida hotbilden och bedömer sannolikheten för ett angrepp. Analysen ligger till underlag för olika motåtgärder, beroende på riskbenägenhet, egna svagheter och andra faktorer. Både angriparen och försvararen genomför övningar och kontroller med motsatta syften. Uppgiften här är att fundera över vilka principiella tillvägagångssätt som angriparens verktygslåda kan innehålla. Konkreta detaljer, exempelvis stödjande datorprogram och specifik teknisk apparatur, diskuteras naturligtvis inte, då det vore kontraproduktivt.

Det är två metoder som kombinerats i föreliggande text: (1) analys av kända tillvägagångssätt i kombination med försök att tänka sig in i angriparens situation, att i någon mån spela rollen av ”djävulens advokat” i samband med manipulering av information och (2) belysande exempel som antingen hämtats från verkligheten (med angivande av källor) eller som är hypotetiska, men realistiska.

Referensram

Det är avsikten att här försöka skissera en användbar referensram för framställningen. För att kunna utöva påverkan på en målgrupps verklighetsbild krävs att en aktör (sändare) genom olika kanaler på ett genomtänkt sätt agerar och förmedlar budskap och signaler till en mottagare för att påverka attityder och handlande. I normalfallet är målgruppen under tiden exponerad även för konkurrerande intryck och budskap. Är det då möjligt att i princip och på kort sikt *manipulera* en målgrupps verklighetsuppfattning?

Anmärkning: Informationsoperationer utgör ett potentiellt hot mot medieföretag. När hot* mot system (företag, organisationer) diskuteras brukar man ibland särskilja organisatoriska hot, logiska hot och fysiska hot. Terminologin varierar. Det bör därför framhållas att organisatoriska hot berörs inom ramen för *psykologiska aspekter* nedan. Logiska hot, säkerhetsluckor* i IT-system och datorstöd, samt röjande signaler* kallas *tekniska aspekter*. Fysiska hot och skaderisker av typen skadegörelse, stöld, sabotage, vattenskador och brand, samt strukturella förhållanden som kan ha betydelse vid informationsoperationer hänförs till *övriga aspekter* i ett senare avsnitt.

Psykologiska aspekter

Det finns ett antal psykologiska principer[22] för hur vi människor hanterar information som kan utnyttjas och missbrukas när det gäller att manipulera vår verklighetsbild. Nedan anges några få exempel på metoder som kan komma till användning vid all påverkan, även vid informationsoperationer. Exempel ges efterhand.

Förutfattade meningar

Vi jämför ny information med tidigare erfarenheter. Det som stämmer med vad vi förväntar oss eller med vad vi sätter värde på tar vi till oss, det andra försöker vi bortse från. Genom att antyda en gemensam referensram, exempelvis genom ordval och minnesreferenser, kan en sändare skapa överdrivet positiva eller negativa attityder hos mottagaren.

Önsketänkande och osäkerhet

Vi ser vad vi vill se, hör vad vi vill höra och minns vad vi vill minnas. Vi tenderar att undvika sådant som skapar osäkerhet och oklarhet genom att reducera osäkerheten och oklarheten genom olika mekanismer och omtolkningar. Vi väljer tolkningar som skapar säkerhet och undviker tolkningar som skapar osäkerhet (kognitiv dissonans). Den enskilda människan försöker uppnå kontroll genom att reducera upplevd osäkerhet. Om det uppnås genom att vi drar felaktiga slutsatser eller blundar för vissa fakta gör vi kanske så, även om vi därmed hjälper till att lura oss

[22] Furustig (1996), sid. 11-12.

själva. En sändare kan försöka inducera falsk säkerhet eller omotiverad osäkerhet hos en mottagare inför ett valalternativ. En effektiv bluff måste emellertid alltid innehålla spår av sanning för att ge trovärdighet.

Mönster

Det vi upplever som viktiga nyheter är ofta det som avviker, har uppmärksamhetsvärde och påtaglighet (närhet i tid, rum och kontrast). Den som vill dölja någon känslig information kan öka det mentala bakgrundsbruset (informationsöverskott, avledande information) eller på andra sätt överbelasta mottagaren och skapa osäkerhet.

En verklig men irrelevant händelse (informationsbrus) kan framhävas på bekostnad av det som är känsligt och relevant och som därför behöver mörkas. I princip kan någon uppseendeväckande information (nyhet, händelse, ”affär”) aktualiseras eller tillskapas i syfte att *avleda* uppmärksamheten från någon pågående eller förväntad negativ informationsexponering.

Mänskliga behov

Fundamentala mänskliga behov måste tillgodoses. Det gäller självklart rena överlevnadsaspekter, men också hälsoaspekter och socialpsykologiska förhållanden. Det är önskvärt att personalen i en organisation eller ett företag är välmotiverad, känner samhörighet, trivsel och trygghet. Om så inte är fallet ökar mottagligheten för rykten och påtryckningar och slarv med säkerhetsrutiner. Detta ökar i så fall tillträdessårbarheten vid informationsoperationer. I värsta fall kan konflikter med arbetsgivare leda till illojalt agerande eller till och med brottslig verksamhet. Det har exempelvis förekommit datorbrott och sekretessbrott i samband med uppsägningar. Även om dessa fall normalt inte har med informationsoperationer att göra inses att organisatoriska och mänskliga svagheter utgör ett riskmoment även i samband med informationsoperationer.

Förebilder

Förebilder kan skapa trygghet hos människor, legitimera en livsstil och en uppförandekod. Det är därför viktigt att förebilder är goda. De kan skapas genom påverkan, på gott och ont. Ytterligare ett psykologiskt perspektiv på manipulativ påverkan diskuteras i avsnittet om vilseledningsaspekter nedan.

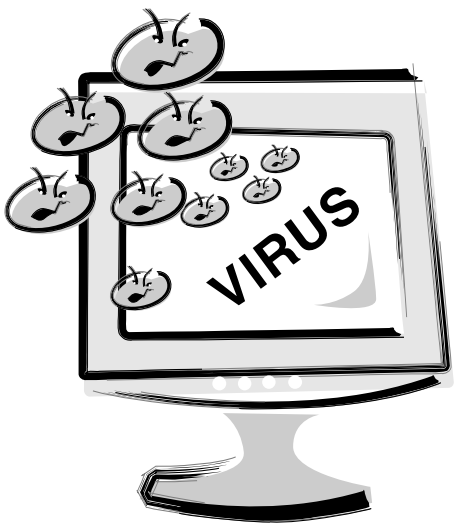
Tekniska aspekter

Komplexa tekniska system i samhället som råkar ut för störningar och funktionsavbrott skapar efter kort tid en överspridningseffekt till andra delar av samhället. Avbrott i energiproduktion och energidistribution kan föranleda svåra problem både för enskilda hushåll och industrier, inklusive massmedieföretag. Störningar i telekommunikationer och informationssystem påverkar samhällets räddningstjänst och olika nyhetsorgan, inte bara etermedierna. Störningar i transportsystem

kan leda till att tryckerier inte får tillgång till papper, tryckfärg m m och att tidningar inte når konsumenterna. Ledningssystem är ett annat exempel på ett kritiskt nätverk. Om ett tekniskt system slås ut finns det således risk att det uppstår dominoeffekter och att angränsande funktioner i samhället blir störda, i synnerhet om det är ett system som har en central funktion i ett nätverk. Effekten av olika typer av störningar och hot mot samhällets infrastruktur behöver därför studeras ur massmediernas sårbarhetsperspektiv. [23]

Gemensamt för de flesta komplexa tekniska system är att de är beroende av datorstöd för underhåll och drift. I stället för att störa eller slå ut en teknisk funktion lokalt på plats möjliggörs därmed angrepp mot utvalda centrala funktioner via nätverk och mjukvara. Både hårdvara och mjukvara kan från leverans vara försedda med dolda funktioner, som när givna villkor uppfyllts plötsligt sätter systemet ur funktion eller ändrar dess funktion. Lokalt kan hårdvara slås ut genom kraftiga mobila elektromagnetiska fält, signalförbindelser kan störas ut med mobila lokala störsändare. Mjukvaran kan angripas med trojaner*, maskar* och virus*. Dessa angrepp kan i princip drabba medier likaväl som andra företag och myndigheter.

Att något är tekniskt möjligt innebär naturligtvis inte att det måste ske; det krävs motiv, kunskap, tillfälle och aktörer för detta. Angriparen söker efter *säkerhetsluckor** i offrets tekniska system för att därefter attackera. Kraven på resurser för ett elektroniskt angrepp är begränsade, varför det är viktigt att försvararen har uppfattning om den aktuella hotbilden. En isolerad teknisk informationsattack leder knappat till något i sig, utan måste sannolikt följas upp, exempelvis av förhand-



[23] Grimvall, Jacobsson & Thedéen (2003). Se särskilt ”Infrastrukturens sårbarhet”, kapitel 12.

lingar med krav eller hot, av någon psykologisk åtgärd, eller av upprepning i syfte att urholka allmänhetens förtroende.

Nyligen slogs Försäkringskassans och Riksförsäkringsverkets datorsystem ut av ett kraftfullt datavirus[24] som sannolikt överbelastade serversystemen. Det ledde till att Försäkringskassans kundtjänst inte fungerade och att handläggningen av olika ärenden, såsom utredningar och vissa utbetalningar tillfälligtvis inte kunde utföras på grund av datorberoendet. Vid pressläggningen var det oklart om det rörde sig om en avsiktlig attack mot just Försäkringskassan eller ett dåligt skämt. Exemplet belyser att det är möjligt med små medel även för en enskild person (hacker*, cracker*) att genomföra en begränsad attack.

Det finns en utvecklad teknisk nomenklatur som behandlar olika detaljformer av funktion, tillgänglighet och sårbarhet i tekniska system som inte diskuteras här. Poängen är snarare att framhålla människans roll: *människan står i centrum* för de tekniska system och de informationssammanhang som berör oss i egenskap av medborgare, myndigheter och medier. Det är den totala funktionen av det överordnade systemet (företaget, myndigheten, staten) som är i fokus. Skarpa informationsattacker avser att uppnå en avgörande effekt på personal och ledning i företag, organisationer och myndigheter eller, i strategiska sammanhang, på opinioner, beslutsfattare eller statsledning.

Kommunikativa aspekter

Det finns många modeller som beskriver hur information hanteras i nyhetssammanhang, mellan människor och mellan människa och maskin. Den enkla modell[25] som används här avser informationsflödet mellan en sändare, en mottagare via en kanal och består av ursprunget till informationen (källan), aktören som sänder ett budskap (sändaren), de som bearbetar informationen och överför den (kanalen), mottagaren av signalen som tolkar informationens budskap (mottagare), samt någon form av reaktion på mottagandet (effekt och feedback). Under detta informationsflöde uppträder brus och störningar och olika typer av mänskliga filter (grindvakter) på vägen. Ordet *kanal* kan exempelvis stå för massmedier som har en medierande roll i detta sammanhang och syftar således inte nödvändigtvis på något tekniskt sambandssätt. Mottagaren utgör informationens destination, dess målgrupp.

SPF har introducerat ett konstruktivt synsätt för att framhäva de viktiga parterna vid samhällets kommunikation, låt oss kalla det 3M: Myndighet, Medborgare och Medier.[26] Den som vill utsätta oss för en informationsattack kan ha orsak att exempelvis föra fram vilseledande information till medierna, kontrollera kommunikationen till medborgaren och försena besluten från myndigheterna.

---

[24] ”Värmland: Kraftfullt virus slog ut datasystemet. Försäkringskassan lamslogs.” *Nya Wermlands-Tidningen*, 2004-06-24, sid. 4.

[25] (a) Windahl & McQuail (1978), sid. 18. (b) Furustig (1981), sid. 12.

[26] Nordlund (1994).

Sätten att förmedla information är legio. En aktör kan exempelvis producera pressmeddelanden, som distribueras av någon förmedlingstjänst (Internet Wire), som i sin tur kommunicerar med nyhetsbyråer och till sist hamnar på webbplatser eller i medierna om de bedöms ha allmänt intresse. Information kan emellertid spridas och kommuniceras på andra sätt än de önskvärda eller förutbestämda.

Ryktets vägar kan exempelvis vara både snabba och svårkontrollerade. Särskilda kanaler (små tidskrifter eller tidningar) kan tillskapas i propagandasyfte, eller så kan befintliga kanaler utnyttjas av s k infiltratörer eller inflytandeagenter för att införa tillrättalagda nyheter i det internationella mediesystemet, vilket skedde under kalla kriget. [27]

Genom olika nätverk, både formella och spontana, kan svårbedömbar information spridas, exempelvis med hjälp av Internet. Intressenter i ett maktspel kan kontrollera egna medier. Under krigsliknande förhållanden kan lokala nyhetskanaler blockeras och ersättas av externa sändare, vilket skedde under Gulfkriget 1991 genom amerikanska störsändningar mot irakiska stationer och amerikansk propaganda via sändningsutrustade Solo-flygplan.

Vilseledningsaspekter

Vilseledning, en extrem form av avsiktligt missvisande påverkan, är ett viktigt inslag i informationsoperationer. Tillvägagångssätten för att vilseleda är många och en uppräkning blir lätt svåröverskådlig. Bell och Whaley har emellertid presenterat en elegant och översiktlig strukturering av olika metoder, som i bearbetad form återges nedan. [28] Denna strukturering är till och med tillämplig på djur- och växtvärlden, något som Whaley har exemplifierat i en av sina böcker. Det handlar antingen om att *framhäva* det falska eller om att *dölja* det sanna, något som är relevant för alla som behöver skrämma sina naturliga fiender eller skydda sig mot motståndare.

Tabell 1. Strukturering av principiella metoder för vilseledning.

Dölja	Framhäva
Maskera (osynliggöra, undertrycka)	Imitera (kopiera, härma)
Förändra (lägga till, dra ifrån, förklä)	Nyskapa (mönster, egenskaper)
Förvirra (öka osäkerhet, sudda mönster)	Locka (skapa nyfikenhet, behov)

(Bearbetat från Bell & Whaley 1991 respektive Sjöstedt 1988.)

[27] Ett exempel är en grekisk tabloidtidning, Ethnos, som uppges ha skapats av KGB för att sprida sovjetisk propaganda. Det ska också ha förekommit att artiklar skrivits av statliga informationsorgan och lämnats till lokala förmågor för lokal publicering, exempelvis i Nigeria, i förhoppning om internationell vidarepublicering. Att särskilda kanaler spred tillrättalagd information i ”etern” är välkänt. United States Information Agency (USIA) bevakade sovjetisk desinformation i massmedierna och motpublicerade uppgifter om denna verksamhet. Samtidigt var USIA naturligtvis en aktör i sammanhanget.

[28] Bell & Whaley (1991), sid. 61. En liknande figur förekommer tidigare hos Sjöstedt (1988), sid. 16. Både Sjöstedt och Bell & Whaley använder huvudkategorierna simulering (att skapa en skenbild) och dissimulering (att dölja).

För att genomföra en vilseledningsoperation, eller för den delen en informationsoperation där vilseledning ingår, krävs systematik, samordning och tidskoordinering av resurser. De viktigaste stegen återges kort nedan. [29]

Tabell 2. Några led i en vilseledningsoperation.

Aspekt	Fokus
Lägesbild?	Kunskap om förutsättningar och krav!
Mål?	Vad som ska uppnås!
Målgrupp?	Vilka som ska påverkas att göra vad!
Förberedelser?	Logistik! Stödjande verksamhet! Beroenden!
Plan?	Operativ idé! Resursbehov!
Bete?	Vilseledningsidé—bjudningssätt—kanaler—samordning—utvärdering.
Kontroll, etc.	Återkoppling. Reserv. Avslut. Utvärdering.

(Bearbetat från Furustig 1996).

Är det ”tillåtet” att vilseleda? Frågeställningen är komplex och kan bara belysas allmänt här. I sammanhang där det kan anses vara ”god taktik” att dölja eller vinkla information, exempelvis vid vissa förhandlingar, är det i varje fall inte generellt olagligt att göra så. Det går också an att överdriva något i försäljningssammanhang. Men det strider mot god affärssed att avsiktligt lämna oriktiga sakuppgifter. Vid förolämpningsbrott och förtal är det ofta den drabbade själv som får föra talan. Bedrägeri är naturligtvis straffbart och att lämna oriktiga uppgifter i vissa ekonomiska sammanhang och till myndigheter är otillåtet. Olika typer av förfalskning och förvanskning av urkund är straffbara. Vilseledande beteenden i tekniska sammanhang, exempelvis att ändra i program och informationsbehandling för egen vinning, kan vara straffbara. [30]

Det finns även vilseledande agerande på den tekniska sidan som inte är straffbart och som missbrukas. Ett exempel har att göra med användandet av falska telefonnummer. Datorstyrd automatisk uppringning och avringning av ett stort antal mobilabonnenter med angivande av ett falskt telefonnummer föranleder sannolikt de flesta uppringda att ringa det nummer som framgår av teckenfönstrets uppgift om ”missat samtal”. Resultatet blir att numret, som kan gå till en telefonväxel på en myndighet, överbelastas. Oskyldiga abonnenter kan på det sättet luras att delta i en telefonattack mot något utvalt offer. Regler som tvingar teleoperatörer att radera ”obehövlig” samtalsinformation, försvårar dessutom spårning av de verkliga telefonsabotörerna. [31]

Yrkesetiken för informatörer uppfordrar till att ge korrekt och saklig information, att ej undanhålla relevant information och att ej sprida osann eller vilse-

[29] Furustig (1996 a), sid. 18-20.

[30] Svensson (1992), sid. 135-136.

[31] *Ny Teknik*, 2004-10-06, del 2, sid. 2.

ledande information. Att en uppgift är sann friar dock inte generellt från anklagelser om förtal. Att publicera vilseledande information är generellt knappast olagligt, det kan vara fråga om att föra fram åsikter (om än extrema) eller göra inlägg (om än osakliga) i en debatt.[32]

Att något agerande inte är formellt olagligt betyder emellertid inte att det är moraliskt försvarbart. Tyvärr är det kanske som det arabiska talesättet säger:

”En bra lögn färdas mellan Bagdad och Konstantinopel medan sanningen fortfarande letar efter sina sandaler.”

Principiella aspekter

Avsnittet inleddes med frågan om det går att manipulera en grupps verklighetsbild. Erfarenheten och de exempel som ges här visar att det är möjligt. Följdfrågan blir då hur aktörer kan gå tillväga för att attackera, respektive för att skydda sig mot angrepp. De hittills förda resonemangen sammanfattas i en enkel arbetsmodell nedan, som belyser detta. Angriparen förutsätts därvid ha tillgång till en abstrakt ”verktygslåda” ur vilken han väljer sina redskap efter omständigheterna. Verktygslådan konkretiseras i ett efterföljande kapitel som handlar om inslag i IO och frågan om skydd och motverkan diskuteras i det avslutande diskussionskapitlet. Arbetsmodellen kallas A-K-T-Ö-R, som är en akronym för modellens olika delar. Den beskrivs efter nedanstående exempel.

Det förda resonemanget kan ge ett intryck av att det är helt klart vad en IO är och att det därför är lätt att känna igen en sådan. Det finns orsak att varna för förutfattade meningar i sammanhanget. En professionell angripare agerar på det sätt som är rationellt för honom, i den situation han befinner sig. En skickligt genomförd IO mot ett oskyldigt offer avslöjas kanske inte alls eller först i efterhand såvida förebyggande åtgärder ej vidtagits.

Exempel

För några år sedan förekom en e-postattack mot fyra dagstidningar[33] som förenats i en kampanj mot nazismen. Under några timmar fick hundratusentals människor e-post med uppmaning och detaljerad instruktion att vidarebefordra ett tackbrev till tidningarna för dessa insatser. Resultatet blev att tidningarnas servrar för e-post mottog flera brev i sekunden. På grund av beredskap bröt inte servrarna ihop och effekten av e-postbombningen begränsades. De enskilda aktörerna hade inte ont uppsåt när de skickade tackbrevet vidare, tvärt om.

---

[32] ”Yrkesetiska regler för informatörer” ges ut av informatörsfacket. ”Spelregler för Press, Radio och TV” ges ut av pressens samarbetsnämnd.

[33] *Ny Teknik,* 1999, nr 49, sid. 9.

Figur 1. Arbetsmodell för angripare och försvarare vid informationsoperation.

A <–> K <–> T <–> Ö <–> R	
A står för attack.	Angriparen har rationella motiv för en attack och har uppställt operativa mål och identifierat målobjekt. Försvararen funderar över vilka konkurrenterna eller motståndarna kan vara och varför. Motiv, avsikt och kapacitet?
K står för kunskapande.	Angriparen har ett underrättelseunderlag som beskriver objektets egenskap, styrka och svaghet samt tidskritiska förhållanden. Objektets sårbarhet indikerar angreppsmöjligheter. Restriktionerna inför ett angrepp har identifierats. Handlingsbegränsning? Tidssamordning? Resursbegränsning? Försvararen skaffar sig en uppfattning om hot, hotbild, risker och egen sårbarhet.
T står för tillvägagångssätt.	Angriparen gör upp en plan som bygger på någon utvald operativ idé (bluff, ploj) som beaktar tillgängliga och realistiska verktyg i aktörens verktygslåda. Psykologiska, tekniska och andra åtgärder utväljs och kombineras för att uppnå den operativa målsättningen. Försvararen identifierar indikatorer på förestående aggression och signaler som ger förvarning. Motåtgärder förbereds (diskuteras i sista kapitlet).
Ö står för övning.	Angriparen genomför förberedelser och förövningar vid behov, dels i syfte att öka förmågan, dels med syfte att pröva försvararens penetrationsmotstånd i kritiska avseenden. Försvararen identifierar förberedelser, exempelvis tekniska händelser och andra åtgärder som kan vara sonderingar inför angrepp. Förstärkningsåtgärder vidtas.
R står för resultat.	Angriparen genomför en attack och är därvid beredd att utnyttja olika situationer som uppstår, vilket kräver flexibilitet i genomförandet. Under attackens förlopp erhåller angriparen löpande återkoppling om läget. Efter attackens genomförande sker en utvärdering. Försvararen förminskar effekterna av angreppet och bemöter det. (Diskuteras senare). Det sker en utvärdering av situationen.

<–> Dubbelriktad tidspil. Pilen indikerar ömsesidigt beroende mellan det som står före och det som kommer efter. Den markerar ett återkopplat samspel och är således inte en enkelriktad tidspil.

Ytterligare ett exempel

Ett exempel på en operation riktad mot kommunikationssamband kan hämtas från det amerikanska inbördeskriget. Sydstaterna genomförde upprepade lokala angrepp mot nordsidans järnvägs- och telegraflinjer. Dessa nålstickseffekter blev till sist så störande att nordsidan omkring 1864 avdelade omkring *hälften* av sina stridskrafter till ockupationsuppgifter och skydd av kommunikationslinjerna.[34] Exemplet är hämtat från krigsförhållanden och angreppsmetoderna inkluderade fysiska åtgärder av typen sabotage. Operationen kan därför hänföras till ledningskrigföring. Avbrott i telekommunikationer eller generellt i infrastrukturen i dagens informationskritiska samhälle skulle få stora effekter oavsett hur operationen klassificerades.

Effekten av sabotage, störningar, misslyckanden och katastrofer förstärks naturligtvis av målinriktad, illasinnad propaganda och svartmålning. Därför kan man förvänta sig att olika element kommer att kombineras i en skarp attack. Tekniska

[34] Libicki (1995). Not 10, sid. 14.

åtgärder är ett uppenbart exempel på en kategori av element som på ett *kreativt och därmed oväntat sätt* kan utnyttjas *tillsammans* med olika kognitiva åtgärder, det vill säga psykologisk manipulering och olika former av vilseledning.

> *Tekniska angrepp och psykologiska angrepp går hand i hand och förstärker varandra*

Ett tredje exempel

Slutligen ett anmärkningsvärt exempel från första världskriget, som tangerar en IO. Året var 1915. De allierade och de tyska stridskrafterna låste varandra på västfronten. Britterna försökte förbättra den strategiska situationen genom angrepp mot Turkiet (som då var allierat med Tyskland) vid Dardanellerna och Gallipoli. Konstantinopel hägrade. Hela operationen blev ett utdraget misslyckande. För att inte västfronten skulle verka nedprioriterad gick chefen för den brittiska expeditionskåren på västfronten till angrepp mot de tyska linjerna vid Neuve Chapelle. Britterna hade ont om granater och överraskade tyskarna utan den normalt förberedande artilleribeskjutningen. Britterna bröt därvid igenom de tyska linjerna (enda gången under kriget), men utnyttjade inte situationen. Till sist blev det som vanligt. Båda sidor fick förstärkning och återgick till artilleribeskjutning till ingen nytta. Angreppet blev ett misslyckande. Vems var felet? General French skyllde på granatbristen. Myndigheterna i Storbritannien skyllde i sin tur på de anställda i rustningsindustrin. Dessa anklagades för att tillbringa för mycket tid på pubar i stället för att producera krigsmateriel. Snabbt stiftades nya lagar som begränsade pubarnas öppethållande. De stängdes under eftermiddagen. Som Taylor har uttryckt saken: *”Alla som känner sig törstiga i England under eftermiddagen får fortfarande betala priset för Neuve Chapelle.”* [35]

Av politiska skäl behövdes en syndabock. Då myndigheterna hade informationsövertag i utgångsläget kunde den diskutabla verklighetsbilden förstärkas. Den följdes upp med en fysisk åtgärd, lagstiftning. Några särskilda åtgärder behövde således inte vidtas för att skapa *informationsövertag* gentemot någon motståndare. Behovet av insatser i försvarsproduktionen var förankrat i hemmaopinionen och förstärktes genom propaganda.

Svaret på den inledande frågan om det går att tillfälligt manipulera en målgrupps verklighetsbild är således jakande, under förutsättning att lämpliga motåtgärder inte vidtagits.

---

[35] Taylor (1963, sv 1967), sid. 76-77.

Aktörer och mål

Vilka är tänkbara aktörer vid informationsoperationer? Vilka skulle deras syften kunna vara? Av särskilt intresse här är operationer som direkt riktar sig mot medier eller som använder sig av medier som kanal. Av flera orsaker är det inte så enkelt att hänvisa till fallstudier. Först måste själva operationen identifieras, är den riktigt framgångsrik och skickligt upplagd uppfattas den inte som en operation, om den uppfattas alls, utan som en naturlig händelse. Sedan måste det kunna påvisas vem eller vilka som ligger bakom operationen; det kan vara svårt att finna bevis även om det inofficiellt skulle gå att peka ut någon aktör. Spåren kan dessutom vara flertydiga, så att fler tänkbara aktörer kan vara inblandade av olika motiv och i olika faser eller i en samordnad operation.

Erfarenheterna från moderna terroristoperationer tyder på att olika organisationer tillfälligt kan bilda operativa celler som efter genomförd verksamhet åter upplöses. En motsvarighet inom informationsoperationernas arena skulle kunna vara ett tillfälligt samspel mellan organisationer i syfte att nå något strategiskt informationsmål.

Exempel

Närmast diskuteras vad som kan ha varit en informationsoperation.[36] Under en period uppträdde Finland som spekulant på svenska Gripen (JAS). När det var dags för provflygning blev vädret så dåligt att provflygningen ställdes in med hänvisning till svenska flygregler. En utländsk korrespondent från konkurrenten tog tillfället i akt och kontaktade sitt nätverk på politisk nivå i Finland. Ett rykte spreds att den verkliga orsaken till den inställda flygningen var flygtekniska problem. Målgruppen var politiker som inte hade sakkunskap om flygreglerna. Det hela ”avslöjades” genom att en av de personer som ingick i nätverket var rådgivare till SAAB. En effekt av denna ”operation” var att svenska militära experter valde att gå ut med korrigerande information. Enligt Sjöstedt och Stenströms analys var:

- målet – att förhindra köp av svenskt flygplan,
- metoden – svartmålning av konkurrent,
- aktören – utrikeskorrespondent på uppdrag av företag eller stat,
- målgruppen – finska politiker via korrespondentens nätverk.

Exemplet belyser att steget mellan att upptäcka en informationsoperation och att avslöja initiatorn bakom operationen kan vara långt. Dessutom kan det vara svårt att bedöma effekten av en operation, i varje fall för en utomstående. Sverige fick som bekant inte någon order av Finland. Det *kan* ha berott på svartmålning. Det kan emellertid också ha andra förklaringar, kanske Finland inte avsåg att köpa JAS

[36] Fallet har hämtats från Sjöstedt & Stenström (2002), sid. 26-27.

därför att även andra faktorer än flygprestanda spelade in. Beträffande målet med operationen kan det även ha varit att försvåra eventuell försäljning till andra stater.

Aktörer

Ordet *aktör* används här i betydelsen av en som medvetet eller omedvetet spelar en tilldelad roll i informationsoperationen. Därmed finns det skäl att särskilja vilka olika typer av aktörer som kan vara inblandade:

- initiatorn – de(n) som har huvudintresset av och initierar, planerar, samordnar och kontrollerar en operation,
- specialister – som medverkar i operationen (omvärldsanalytiker, tekniker, språkexperter, m fl),
- källor – som meddelar eller läcker initierande signaler, information, budskap eller rykten,
- sändare – som bearbetar och utformar informationen för vidare spridning,
- kanal – de(n) eller det som sänder och sprider informationen, budskapet eller signalen till målgruppen,
- mellanhänder – som på olika sätt går initiatorns och sändarens intressen tillhanda,
- mottagare – som utgör målgrupp, antingen direkt eller indirekt.

I en numera klassisk studie av informationskrigföring[37] varnar författaren för att en attack kan drabba mottagare på alla nivåer: från den enskilde individen, företaget eller organisationen, till den statliga eller globala nivån. På individnivå riskerar ”offret” att förlora värdefull information eller kunskap genom att databaser, konton eller annan känslig dokumentation kommer på avvägar, förstörs eller förfalskas, att individens identitet ”stjäls” eller att personliga tekniska hjälpmedel virtuellt ”kapas”. Senare i rapporten återfinns ytterligare resonemang om tänkbara motiv.

Tankegången ovan kan vändas. Även den initierande aktören återfinns, i princip, på olika nivåer:

- mellan- eller överstatlig,
- statlig,
- multinationellt företag eller stort företag, inklusive medier och PR-företag,
- internationell organisation inklusive hjälporganisation,
- organiserade aktivister, utomparlamentariska grupper (nationella eller internationella är mindre relevant),
- nationell organisation, myndighet eller företag,
- cell,
- enskild individ.

---

[37] Schwartau (1994).

De två senast nämnda kategorierna bör kommenteras. *Cell* ska här uppfattas som en sluten organisatorisk enhet med operativa uppgifter. Övergripande beslut om operativ inriktning och mål har sannolikt tagits före eller i anslutning till cellens uppbyggnad, det vill säga cellen har en uppgift som den självständigt ska lösa. Initiatorn kan därvid ingå i cellen men kan alternativt befinna sig utanför, i likhet med sådana internationella terroristledare som initierar olika cellers aktiviteter. En *enskild individ* med tillräckliga tekniska kunskaper och lämplig utrustning kan i princip bedriva ett informationsmässigt miniatyrkrig på egen hand (förmåga). För att så ska inträffa måste det också föreligga ett tillräckligt starkt motiv (avsikt), vilket diskuteras i nästa avsnitt. Det ligger i sakens natur att begreppet ”aktör” är entydigt om angriparen är en enskild individ. Om informationsoperationen är komplicerad krävs att angriparens organisation i motsvarande grad är specialiserad, varvid innebörden av ”aktör” beror av specialiseringsgraden och syftet med beskrivningen.

Under det kalla kriget avslöjades några aktörer som beskrevs som infiltratörer alternativt inflytandeagenter och som var verksamma i massmediala sammanhang. Med en hårdför tolkning var deras uppgift att argumentera för en ideologi eller en ståndpunkt utifrån den position de fått hjälp att nå. Med en mjuk tolkning utnyttjade de tillfället att agera för sin egen övertygelse. Den ena tolkningen utesluter inte den andra, men resonemanget antyder att det kan vara svårt att på ett entydigt sätt avgöra människors drivkrafter och avsikter.

Exempel

En journalistisk inflytandeagent och aktör var Pierre-Charles Pathé.[38] Han rekryterades av sovjetiska KGB år 1959 och var verksam som en framstående skribent i Frankrike tills han där greps av polisen år 1980. Han hade ett kvalificerat kontaktnät och skrev artiklar under pseudonym i franska medier till fördel för sovjetiska intressen. Han gav också ut ett nyhetsbrev, *Synthesis*, med en utvald målgrupp av inflytelserika mottagare. Hans syften var exempelvis att tillrättalägga Warszawapaktens politik och att underblåsa motsättningar mellan USA och Frankrike. Han dömdes till fem års fängelse, men frigavs efter något år. Intressant information från nätverken förmedlades till KGB, men intressantare är att KGB gav idéer och bakgrund till blivande artiklar som Pathé kunde utnyttja.

Ett annat exempel

En annan journalist, författare, inflytelseagent och aktör var Arne Petersen i Danmark.[39] Även Petersen hade rekryterats av KGB. Han publicerade politiska böcker/pamfletter med angrepp på och svartmålning av premiärminister Margaret Thatcher och den västtyske politikern Franz Josef Strauss med flera och agerade

---

[38] Pincher (1985), sid. 99-100. Häggman (1990), sid. 92.

[39] Pincher (1985), sid. 100-101. Häggman (1990), sid. 27-28.

aktivt på andra sätt som talangscout, förfalskare, budbärare och agent. Han agerade bland annat för en kärnvapenfri zon i Skandinavien. Det är även här intressant att notera att KGB försåg honom med underlag till tillrättalagda artiklar som han bearbetade och publicerade. KGB betalade även Petersens omkostnader för kampanjer. Han greps av dansk polis år 1981, men den danska regeringen beslöt att inte åtala därför att danska intressen inte ansågs ha skadats ”tillräckligt mycket”. Däremot lämnades anklagelser och bevis ut offentligt av danska myndigheter!

Det är naturligtvis juridiskt besvärligt att driva fall som dessa. Skribenterna har all rätt att uttrycka sin uppfattning, men inte rätt att bedriva subversiv verksamhet eller att förfalska dokument, etc. Det är naturligtvis moraliskt förkastligt att avsiktligt vilseleda, men svårbevisat och ofta inte juridiskt straffbart (se utredningen i avsnittet om vilseledning).

Fler exempel på journalister och författare som agerat som inflytelseagenter skulle kunna nämnas. Dessa aktörer har oftast till syfte att på ett genomtänkt och systematiskt sätt sprida ett budskap som är propagandistiskt (exempelvis skönmålande) respektive missvisande (exempelvis svartmålande). Det kan i princip också vara fråga om motsatsen, att undanträngа något konkurrerande budskap, exempelvis genom att skapa opinion, åsiktsmonopol eller att förfalska dokument eller avbildningar eller att blockera tillträdet för viss information, tekniskt eller genom någon censurerande funktion (grindvakt) inom det nätverk som inflytelseagenten verkar.

Det finns naturligtvis ett stort antal ”aktörer” på informationsmarknaden som har ett gott syfte, exempelvis olika hjälporganisationer och övriga icke-statliga organisationer (NGOs). Men de tillgriper knappast informationsattacker som medel, utan förlitar sig på att förmedla sann information genom upplysning, reklam och PR.

Mål

Syftet är här att belysa att det måste till ett *motiv* för att en aktör, som har kapacitet och förmåga, i realiteten ska planera och genomföra en informationsoperation.

Vad som utgör ett tillräckligt motiv för en aktör beror bland annat på vilka nivåer den angripande respektive den angripne befinner sig. I militära säkerhetspolitiska sammanhang tar man planeringsmässigt i princip hänsyn till vilka stater som har *kapacitet* till angrepp och garderar sig planeringsmässigt för detta även om staten i fråga är vänskapligt sinnad och troligen saknar avsikt att angripa. Omvändningen, att gardera för stater som har illasinnade avsikter, är militärt intressant endast om de dessutom skulle ha militär kapacitet. När det gäller informationsoperationer är det värt att notera att även den aktör som har den minsta kapaciteten, den enskilde individen, mycket väl kan ha förmåga att allvarligt störa och skada högre nivåer, såsom företag, organisationer och myndigheter. Slutsatsen blir att när det gäller informationsoperationer är det klokt att ha en uppfattning om vilka aktörer som har ett känt motiv eller en uttalad avsikt att skada: vill man så kan man kanske.

Djurrättsaktivister kan släppa ut minkar för att ”rädda” dem trots att många djur sannolikt kommer att avlida till följd av stress. Handlingar av det slaget följs ofta upp genom att medierna rapporterar om aktionen och kanske även utvecklar ämnet i något debattprogram. Det är först i den situationen som handlingen har potens att bli meningsfull. En köttproducents transportfordon kan utsättas för anlagd brand eller allmän skadegörelse. Det är en form av militant demonstration och leder sannolikt inte till att någon enda köttätare får sympatier för det slaget av vegetarianer på kort sikt. På längre sikt kan dock effekten bli en annan om det uppstår debatt om rätten att ta liv. Miljöaktivister kan krama träd för att hindra avverkning och verka smått löjliga. Men om de klättrar upp i höga skorstenar som kanske är förorenande eller om de prejar stora oljefartyg med små gummibåtar för att förhindra farliga transporter kan handlingarna bedömas annorlunda. Det är tydligt att på kort sikt kan vissa aktioner verka irrationella. Det är först om det genom medierna blir debatt om de verkliga drivkrafterna bakom aktionerna som handlingarna kan få betydelse och i så fall på längre sikt. Ett agerande kan således verka irrationellt på kort sikt men vara rationellt på längre sikt. Om det finns motiv för en operation eller ej beror alltså på hur aktörerna, inte offren, analyserar situationen. Det kan vara värt att beakta.

Utgångspunkten här blir därför att titta på några motiv som har förekommit i verkligheten. Här återges emellertid inga fallstudier, utan resonemanget belyses med en generell och exemplifierande beskrivning av några typfall (tabell 3). Bakom dessa typfall finns dock verkliga händelser.

Tabell 3. Typexempel på mål och aktörskategorier.

Mål	Exempel	Aktörsnivå
Påverka konkreta beslut eller beslutsautonomi i viss fråga.	Skapa beslutsburar för politiker genom att provocera opinionen via medier och demonstrationer.	Stat
Sänka tilltro till viss ledare.	Svartmålning via medier, rykten och demonstrationer.	Stat
Sänka förtroende för produkter. Försvåra marknadsföring.	Ryktesspridning vid försäljning av vapensystem. Svartmålning vid introduktion av ny produkt. Illegal informationsinhämtning inför offertgivning.	Konkurrerande företag
Sänka förtroendet för myndigheter och statsledning.	Störa infrastrukturen (energi, tfn, bank, data). Störa utbetalningar (bidrag, pension, lön, postgiro, bank, börs).	Extremister
Ekonomisk vinning.	Valutaspekulation med stöd av utspel i medier. Förhandskunskap. Försäljning av känsliga produkter via nätet och med stöd av medier. Stöld av värdefull information. Stöld av identitet.	Organisation Individ
Egennytta.	Manipulera databas eller webbsida.	Hacker
Hämnd.	Intrång i datanät och ryktesspridning.	Anställd Cracker
Förstöra och skada.	IT-angrepp. Destruktion. Uppföljning av aktivistaktioner i medier.	Stat Extremist Särorganisation Cracker
Uppnå fördelar under förhandling.	Blockera eller fördröja kunskap. Överdriva styrka. Underskatta styrka.	Företag Organisation Stat
Beroende av perspektiv kan målen uttryckas på helt olika sätt.	För att ge spridning och nå målgrupperna är medierna kanal.	Alla nivåer kan i princip skada varje annan nivå.

Exempel

Här följer en kort beskrivning av en fallstudie som återgetts och analyserats av Sjöstedt och Stenström.[40] Nyhetsbyrån ”TASS.Net” meddelade år 1997 att Pol Pot anlänt till Arlanda i Sverige den 30 juni. Förhandlingar mellan organisationen Komintern och svenska regeringen skulle ha föregått besöket för att motivera Pol Pots (PP) status som flykting. Webbplatsen gav en bakgrundshistoria som belyste den svenska traditionen att ge skydd åt politiskt oliktänkande. Efterföljande dag meddelade samma webbplats att svenska UD inte kunnat dementera att PP befann sig i Sverige, att PP dementerade ryktet om att besöket skulle vara uppdiktat och att en rysk nyhetsbyrå genom Reuters förnekade att den hade något med saken att göra. Enligt Sjöstedts och Sjöströms analys var:

- målet – Reklam för nystartat företag. Experiment för att se vad som går att göra via en påhittad nyhetsbyrå,

[40] Sjöstedt & Stenström (2002), sid. 24-25.

- metoden – Skapa falsk nyhetsbyrå med falska referenser på nätet och en uppdiktad historia,
- aktören – Svenskt företag,
- målgruppen – Medieredaktioner, regeringar,
- resultatet – Internationella medier rapporterade nyheten. Viss förvirring skapades på UD.

Resultatet förefaller ha varit framgångsrikt på avsedd kort sikt. Operationen förbättrade sannolikt medvetenheten hos svenska medier om möjligheten att oavsiktligt medverka till vilseledning över nätet. Ett enskilt svenskt företag kunde således skapa osäkerhet och uppmärksamhet på internationell nivå under en kort period. Syftet var ”oskadligt” i den givna situationen. Men operationen kunde lätt fått allvarliga konsekvenser om den genomförts i ett politiskt tidskritiskt läge och förstärkts av samordnade utspel. I situationer där inflytande, ekonomi och förtroende står på spel kan rykten, skenmanövrer och lögner som sprids via medier påverka både opinioner och beslutsfattare.

Betydelsen av tidsperspektivet har berörts flera gånger i detta avsnitt. I tabell 4 presenteras en översikt av relationer mellan operativa mål och tidsperspektiv.

Tabell 4. Några exempel på approximativa samband mellan operativa mål och tidsperspektiv.

Operativt mål	Tidsperspektiv
Påverka konkret val eller beslut.	Kort sikt = aktuell beslutscykel.
Svartmåla konkurrent, företag eller produkt.	Medellång sikt = under budgetperiod.
Undergräva förtroende för myndighet, förvaltning, rättsväsen, försvar, finanser, politik. Att "vända" värderingar. Svartmåla eller skönmåla parter i konflikt eller internationella insatser.	Lång sikt = under förvaltningsperiod eller mandatperiod.

Exempel

En IO kan förberedas på lång sikt, vilket belyses av följande exempel. Under år 2002 avslöjades en underrättelseoperation av den svenska säkerhetspolisen, SÄPO. En anställd vid elektronikföretaget Ericsson hade värvats av rysk underrättelsetjänst och levererade material till uppdragsgivaren. Den anställde hade också ett par medhjälpare inom företaget. Det visade sig att syftet med operationen inte primärt var kommersiellt. Avsikten var framför allt att inhämta kunskap om hur moderna telekommunikationssystem kan manipuleras. Det kan tolkas som en kunskapsfas inför eventuellt kommande IO. [41]

[41] Bergström (2004). Fall 1, sid. 29-32.

Inslag i informationsoperationer

”...If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy not yourself, you will succumb in every battle...” [42]

Det som i fortsättningen diskuteras och exemplifieras är olika inslag (åtgärder, element) i informationsoperationer. Sådana inslag kombineras och tidssamordnas för att uppnå ett genomtänkt mål. Enstaka åtgärder kan i mindre komplicerade sammanhang stå för sig själva, men den resulterande effekten förstärks om flera åtgärder samverkar (synergieffekt). Uppgiften här är att exemplifiera olika typer av åtgärder som en motståndare och angripare skulle kunna kombinera och använda vid informationsoperationer genom medier. Det är i huvudsak två olika kategorier av åtgärder som behandlas, nämligen psykologiska och tekniska. Åtgärderna är med hänsyn till uppgiften ofta av icke önskvärd natur för mottagaren.

Med *psykologiska* åtgärder menas ”mjuka” åtgärder som påverkar innehållet i ett budskap och tolkningen av ett meddelande, exempelvis genom att kritisk information döljs eller att missvisande information framhävs. Det kan helt enkelt vara olika sätt att missleda mottagaren. Vilseledande påverkan sker i detta sammanhang med olika kombinationer av text, bild eller ljud genom massmedierna och ibland med hjälp av olika tekniska åtgärder.

Med *tekniska* åtgärder menas här ”hårda” åtgärder av typen elektronisk manipulering, störning eller utsläckning av elektromagnetiska signaler för produktion, transmission eller mottagning. Det kan också vara fråga om manipulering av mjukvara, programvara, exempelvis genom maskar, virus och trojaner. En satellitförbindelse kan störas eller avbrytas. Elavbrott kan komma olägligt och kan vara planerade. Intrång kan ske i program under vissa omständigheter. Omkopplingar i sändningsnätet kan arrangeras. Det kan vara fråga om att skapa informationsmörker genom att blockera medel för telekommunikation eller strömförsörjning.

Kanske kan informationskonsumenter uppfatta ämnesområdena ”desinformation” (vilseledning m m) respektive ”hacking” (”cracking” m m) som tillräckligt omskrivna, som vid det här laget rimligen bör ha garderats väl av myndigheter, företag och medier. Erfarenheten visar att det finns orsak att varna för denna förmodan. Från det att något fenomen är omskrivet till det att det är förstått och åtgärdat kan steget vara långt. Hur långt, kan endast empiriska studier avslöja.

Under kategorin *övriga* åtgärder återfinns strukturella åtgärder och fysiska åtgärder och händelser. Med strukturella åtgärder menas exempelvis åtgärder som

---

[42] Sun Tzu (ed. Clavell 1983).

bygger på juridiska, organisatoriska eller logistiska förhållanden inom det aktuella systemet. Det kan här vara fråga om att missbruka spelreglerna för mediers grindväkteri i något illasinnat syfte. Organisatoriskt finns det i princip alltid någon ”grindvakt” som avgör vad som processas. Kriterierna kan variera men nyhetsvärde och allmänintresse skapar efterfrågan, som i sin tur påverkar lönsamheten.

Låt oss konkretisera. Antag en debatt, t ex den om Viggen- och JAS-projekten. En svensk debattör hårdbevakade dessa projekt i ett tidigt skede[43] och drev tesen att flygplanen skulle bli en gökunge i ”budgetboet”, gjorde en propagandistisk film mot Viggen-projektet och publicerade efterhand ett stort antal inlägg i en spridd dagstidning där debattören anförde argument i olika detaljfrågor mot planerna. Det visade sig emellertid att de påståenden, som hade högt uppmärksamhetsvärde, innehöll felaktigheter. Därigenom hölls en debatt igång om olika detaljfrågor. När inläggen förblev osakliga minskade intresset från sakkunnigt håll att gå in i debatten: effekten blev bara nya påståenden. Eftersom tillrättalägganden i efterhand normalt ges mindre publicitet än ursprungliga påståenden, blev det allt svårare för experter att få debattutrymme för bemötanden och korrigeringar, medan däremot debattören fick stort utrymme för sina teser. Det publicistiska värdet av uppseendeväckande påståenden blev på det sättet, avsiktligt eller ej, större än värdet av korrigeringar i sak. Till slut dog ”debatten” ut. Efterhand publicerade försvarsmakten på eget initiativ en partsinlaga, en broschyr i vilken felaktiga påståenden bemöttes. Detta är visserligen exempel på en osaklig debatteknik[44], men framför allt ett exempel på en debatt som gick snett därför att tillträdesreglerna till sakdebatten blev skeva. Exemplet riktar uppmärksamheten mot *grindväktarfunktionen*, som borde vara kvalitetsnormerande. Frågan är om motsvarande agerande fortfarande kan vara ett sätt att sprida ensidig information, kanske även rena felaktigheter?

Därutöver bör fysiska åtgärder och händelser nämnas. Med fysiska åtgärder menas här att avsiktligt, med hjälp av fysisk maktutövning förhindra, kontrollera eller förstöra system för produktion eller distribution av information. Sabotage och krigsliknande handlingar diskuteras dock inte i detta sammanhang. Kanske är det mer sannolikt att oavsiktliga fysiska händelser inträffar, exempelvis naturliga händelser av typen miljö- eller naturkatastrofer, såsom åsknedslag, översvämning och stormskador eller naturligt uppkomna tekniska fel, t ex överhettning eller kortslutning. De berör inte informationsoperationer, såvida inte avsiktliga sabotage förkläs till naturliga fel. Det finns således både naturliga eller normala åtgärder som kan ha koppling till informationsoperationer. Detta utvecklas under avsnittet *Fejka och fela*.

---

[43] Furustig (1981), sid. 19-20.

[44] Ibid, samt Furustig (1982).

Tabell 5. Exempel på strukturering av metoder och åtgärder som kan utgöra inslag i informationsoperationer.

Metoder	Psykologiska åtgärder	Tekniska åtgärder	Övriga åtgärder
Fejka och fela	Rutinmässig kognitiv manipulering av ljud, text och bild.	Rutinmässig teknisk manipulering av ljud, bild och text.	Missbruk av spelregler i gråzon.
Fördröja och försvåra	Filtrera. Grindvakta.	Överbelasta. Blockera.	Censurera. Kontrollera.
Förstärka och förlänga	Dramatisera. Upprepa.	Understödja.	Agera stödjande.
Framhäva, försköna och favorisera	Skapa förebild. Skapa informationsberoende.	Understödja. Bildbehandla.	Demonstrationer. Stödjande aktioner.
Förtala, förgifta och svartmåla	Skapa nidbild. Sprida rykten. Drev.	"Spyware"*. Dold inspelningsteknik.	Inhämtning. Provokationer.
Förvirra och finta	Skapa osäkerhet. Bluffa. Spin.	"Spyware". Datamanipulering.	Fejka händelser genom skenagerande.
Förfalska och förvränga	Bild. Text. Ljud.	Falska källor. Dataintrång.	Överta satellit, radio, tv, tele och datanät.
Förhindra och förneka	Skapa låsningar. Förleda till –>	Denial of Service*. E-mailbombning*.	Fysisk blockering. Beslag. Störningar.
Förstöra	Förleda till kontra-produktiva åtgärder.	EMP*. HERF*.	Förklätt sabotage.

Tabellen innehåller exempel på åtgärder, men gränserna mellan cellerna är flytande och bestäms av den operativa uppgiften och situationen. En informationsoperation kännetecknas knappast av någon isolerad åtgärd inom en cell i tabellen, utan utgörs snarare av en kombination av åtgärder (samverkan mellan flera celler) i syfte att uppnå uppsatt mål.

Med *spyware* avses spionprogram och hjälpmedel för att avtappa information från ett objekt utan objektets kännedom. Mobiltelefoner kan avlyssnas, faxar och persondatorer likaså. Under vissa omständigheter kan avstängd utrustning aktiveras utifrån och fungera som avlyssningsutrustning, exempelvis en mobil.[45] Spyware kan också vara dataprogram eller filer som spårar och rapporterar en brukares datoranvändning utan att denne är medveten om detta.[46]

Den som är offer för ett informationsmässigt angrepp, antingen i form av att vara mottagare av den vilseledande informationen i egenskap av *konsument* (läsare, tittare, lyssnare) eller i form av att vara mer eller mindre oskyldig *producent* eller *kanal* (journalist, grindvakt, bearbetare, redaktör), har nytta av att tänka igenom dessa metoder och fråga sig: Har vi råkat ut för något liknande? Bidrar vi till detta? Gör vi själva så här? Kan vi förbättra våra rutiner och arbetssätt? Redan den kinesiske filosofen och strategen Sun Tzu, citerad ovan, betonar betydelsen av vetskap om den egna sårbarheten och motståndarens styrka, liksom om den egna styrkan och motståndarens svaghet.

[45] *Svenska Dagbladet*, 1999-01-28, sid. 4.

[46] *Ny Teknik*, 2003-11-05, nr 45, del 2, sid. 16.

Framställningen bygger på en omarbetning av Furustigs F-modell som ursprungligen är en modell för diskussion av hur man skyddar sig mot informationsoperationer.[47] Observera dock att det i enskilda fall mycket väl kan finnas naturliga händelseutvecklingar till vad som råkar likna några av ”metoderna”. Det gäller att vara på sin vakt mot *systematiska* tillvägagångssätt oavsett vem som är sändaren. I en verklig informationsoperation är det sannolikt att flera metoder som kompletterar varandra skulle komma till användning, vilket i så fall bidrar till en systematik i agerandet. Mönster kan dock vara svåra att urskilja mitt under en pågående händelseutveckling.

Exempel på IO-metoder

FEJKA OCH FELA

Den tekniska utvecklingen skapar ändrade arbetsvillkor för medierna. Ett exempel är möjligheterna att göra ljud och bildupptagningar med mobiler och andra små bärbara hjälpmedel, upptagningar som sedan direkt kan sändas från fältet via satellit. Sändaren kan vara vem som helst på plats. Materialet kan sändas till någon nyhetsagentur, till någon webbsida på Internet eller till något medieföretag. Ett sådant material, exempelvis från ett katastrofområde eller ett attentat, har högt nyhetsvärde och kan spridas mycket snabbt. Knivskarp konkurrens motverkar källkritisk bedömning därför att materialet kanske redan blivit offentliggjort på nätet och riskerar att kommenteras av någon konkurrent. En sådan situation har uppstått på grund av nya tekniska hjälpmedel, avancerade mobiler, satelliter och ett växande nyhetsutbud på Internet. Detta är emellertid också exempel på en situation som kan missbrukas av den som vill sprida tillrättalagd eller falsk information om något.

Ett exempel på en förkastlig metod att skapa nyhetsvärde är vad som nyligen kallats ”fejk och fel” i ett debattprogram på TV.[48] Programmet kritiserade enskilda mediers nyhetsförmedling i samband med det så kallade Knutby-mordet. Intervjuer och citat hade i några fall uppfunnits. Även i andra sammanhang har kritik riktats mot viss veckopress för att intervjuer uppfunnits eller tillkommit genom hopklippning av olika citat. Även bildmaterial kan användas på motsvarande sätt: arkivmaterial kan blandas på ett försåtligt sätt med färska reportage och bilder manipuleras med hjälp av datorprogram. Sådana metoder är naturligtvis inte representativa för massmedier i gemen, men de har förekommit och förekommer. Vad har nu detta med informationsoperationer att göra?

Exempel

Aftonbladet (AB) publicerade för några år sedan bilder på en maskerad nazist utanför hemmen till en välkänd polis respektive en programledare. Nazisten höll något i handen som liknade ett vapen. I sammanhanget misstänktes flera nazister för

[47] Furustig (1995), sid. 36-40.

[48] *SVT 2* (2004-05-16): Agenda om Knutby-fallet.

olaga hot och en ung reporter från AB anhölls för olaga hot och åtal övervägdes mot tidningen. Förloppet har skildrats så att det kunde uppfattas som om bilderna arrangerats av reportern och fotografen. I och med att filmen framkallats och publicerats framstod arrangemanget som ett hot.[49] AB upplevde den kritik som mediekonkurrenterna riktade mot tidningen som ”drev”. Här lämnas fallets vidare utveckling. Det anförda belyser i varje fall den principiella möjligheten att ”förstärka” en ”story” genom att arrangera en lämplig händelse.

Om sådana tillvägagångssätt etableras av kommersiella skäl är det risk att de till sist får genomslag som ett naturligt agerande, något som förekommer och accepteras i enskilda fall. Det kan i så fall missbrukas av illasinnade aktörer. Här inkluderas vardagsklantighet, naturligt mänskligt felhandlande och naturliga tekniska fel i diskussionen. Antag att en granskande journalist, påverkad av sin förhandsuppfattning, bedriver datainsamling, bearbetning och redovisning på ett sätt som är sakligt missvisande men i linje med förhandsuppfattningen. Antag vidare att förfarandet ursäktas med att det ”bara är fråga om detaljer, ett litet olycksfall i arbetet får accepteras”. Om förhandsuppfattningen skulle få systematiskt genomslag i en programserie med många tittare eller lyssnare utan att balanseras av andra perspektiv vore detta att bedriva propaganda. Gränsen mellan att upplysa och att avsiktligt vilseleda går över en gråzon, där gott och ont kan sammanblandas med rätt och fel. Det går att vinkla utan att direkt ljuga eller ta några egentliga risker avseende konsekvenserna.

Vid tillämpning av yttrande- och tryckfrihetens principer kan det uppstå avvägningsproblem där det finns en gräns för vad samhället accepterar om övergripande intressen skadas eller kan komma till skada. Det ligger i medias och mottagarnas egenintresse att inte oprofessionella arbetsmetoder etableras genom kommersiellt tryck eller påverkan från speciella aktörer eller särintressen. En grov omformulering av filosofen Immanuel Kants kategoriska imperativ kan kanske utgöra en poäng i sammanhanget:

> *”Du ska insamla, bearbeta och presentera information på ett sätt som svarar mot de rimliga krav som den kvalificerade mottagaren kan ställa på slutprodukten.”* [50]

FÖRDRÖJA OCH FÖRSVÅRA

En aktör som vill förhindra eller försvåra att någon speciell information når en mottagare genom medierna kan gå till väga på ett flertal sätt. Det kan vara fråga om information som under någon begränsad tidsperiod utgör en belastning för aktören eller som tillfälligt skulle innebära en värdefull kunskap för mottagaren som denne skulle kunna utnyttja till sin fördel, exempelvis i en förhandling. Följande principiella tillvägagångssätt kan tänkas.

---

[49] *Svenska Dagbladet*, 1998-02-28, sid. 4, tema ”Aftonbladets lögner i nazi-affären”.

[50] Furustig (1981), avsnittet om handlingsregler.

Inhämtning
Mediernas inhämtning av relevanta data försvåras och fördröjs avseende ingångsmaterial som förväntas leda till spridning av känslig eller stötande information vid fel tillfälle. Data kan komma på avvägar, skadas eller försvinna genom datorstödd manipulering eller fysiska åtgärder.

Bearbetning
Osäkerhet kring informationens sanningshalt och relevans skapas genom spridning av en mängd ovidkommande eller missvisande information som tangerar ärendet. Det kan leda till att den journalistiska bearbetningen försenas, men det kan också leda till att den journalistiska instinkten vaknar till liv.

Spridning
Mediernas spridning av känslig information till mottagarna fördröjs eller försvåras under viss tid, exempelvis genom att skapa osäkerhet om de juridiska konsekvenserna av att sprida uppgifter som formellt kan komma att ifrågasättas av någon aktör. Överskottsinformation eller motstridiga uppgifter som sprids av konkurrerande medier kan skapa mättnad hos mottagarna.

FÖRSTÄRKA OCH FÖRLÄNGA
Händelser som är till opinionsmässig fördel för en aktör kan leda till att denne vill njuta sötman av eventuell massmedial framgång så eftertryckligt som möjligt. Det finns därvid skäl att se upp med följande.

Mediedrev
Att ”drevet går” innebär att en överdriven och till synes samordnad och utdragen exponering (publicering, intervjuer, avbildning, etc) äger rum. Därvid kan följande frågor ställas: Hur eller av vem initierades drevet? Finns det någon part som har egenintresse i saken? Hur eller av vem tillförs medier nytt uppseendeväckande material? Varför sker detta just nu, finns det något tidssamband med angränsande (bakomliggande, kommande) händelser som kan förklara förloppet?

Vardagliga och aktuella exempel på extrem fokusering från mediers sida är Skandia-affären och Knutby-händelserna. Med hänsyn till vad som inträffat är det emellertid naturligt att medierna tar upp dessa skeenden. Händelserna kring försäkringsbolaget Skandia har kopplingar till principiella frågor som belysts av mediekritiken mot Skandias agerande. Den massmediala kritiken har sannolikt fått stort genomslag och påverkat politiker, anställda, aktieägare och allmänhet. Knutby-händelserna har en spekulativ koppling till en relativt sluten religiös gruppering och dramatiska inslag av passionsdrama.

Betraktarens intryck är att när många journalister bevakar samma händelse ökar sannolikheten för att upptäcka nya ”spår” att följa. För en aktör kan det då vara tillräckligt att sätta någon journalist ”på spåret” om ämnet är tillräckligt lockande

eller att ”lägga beten” utefter spåret för att underhålla ett drev som är på väg att avstanna.

Exempel

Som exempel på en informationsoperation kan nämnas de sovjetiska åtgärderna inför ”dubbelbeslutet” om utplacering av amerikanska Pershing II-robotar och kryssningsrobotar i Västeuropa under kalla kriget. Operationen[51] inleddes av en stor kampanj där olika särorganisationer relaterade till fredsrörelsen aktiverades. Den ”opinionsstorm” som frammanades byggde bland annat på samverkan mellan frontorganisationer med stora demonstrationer och politiska utspel i kombination. Mediefokuseringen var omfattande. Utan medierna som kanal hade det knappast blivit vad som föreföll vara en opinionsstorm. Någon enkel bedömning av resultatet kan emellertid inte göras kortfattat. Sovjet lyckades inte förhindra utplaceringen av medeldistansrobotar. Diskussionerna fördes i stället vidare vid förhandlingsbordet. En viss framgång bestod i förmågan att mobilisera stödorganisationer, iscensätta stora demonstrationer och skapa opinionstryck samt att utnyttja massmedierna för bevakning och skriverier. Förmågan att skapa opinion inför olika beslutssituationer är fundamental vid IO.

Gränsen mellan att som nyhet återge faktiska händelser (av typen demonstrationer och politiska uttalanden) respektive att överdriva och återupprepa vad som hänt, undertrycka motparters argument, överdriva minoritetsyttringars omfång och betydelse eller undertrycka deras splittring kan bli vag till följd av att någon part påverkar både händelseförlopp och den bild av förloppet som presenteras för konsumenterna.

Mediedrev kan initieras på olika sätt: av enskilda journalister till följd av gott undersökande arbete, av någon särorganisation för att driva en sakfråga eller i syfte att svartmåla eller skönmåla, av någon aktör för att få slut på missförhållanden, av politiska motståndare för att påverka (vända) opinionen i syfte att uppnå politiska eller ekonomiska mål. Ibland behöver mediernas medverkan säkras på något sätt, exempelvis genom samarbete med PR-företag eller inflytelserika påtryckningsgrupper.

FRAMHÄVA, FÖRSKÖNA OCH FAVORISERA

En presentation eller rapportering kan i olyckliga fall bli ensidig (skev). Om samma ämne eller typ av händelser systematiskt belyses på ett ensidigt sätt i media och alternativa synsätt undertrycks uppfylls inte kravet på balans och objektivitet i framställningen. Förutsättningen för resonemanget är att skönmålningen (respektive svartmålningen) är oberättigad.

Det är naturligt att reportrar med tiden specialiserar sig på något ämne. Det kan också leda till specialiserade personkontakter. I den situationen kan det uppstå

[51] Pincher (1985), sid. 218-230.

informationsberoenden mellan parterna. För inte så länge sedan kritiserades en välkänd inrikeskommentator vid *Sveriges Television* för sin dubbla roll att i det fördolda följa statsministerns vardagsliv för långsiktig framtida dokumentering och dessutom löpande uppträda som objektiv kommentator i inrikespolitiska sammanhang. Detta omnämnt för att påminna om att det helt naturligt kan uppstå intressekonflikter utan ond avsikt. Det måste inte leda till en ensidig arbetsprodukt, men kan göra det. Denna tanke utvecklas med idémässig koppling till informationsoperationer.

Favorisera

En aktör som vill skapa god PR för sin egen person, sin ideologi eller verksamhet kan ”odla” någon journalist eller något specialiserat program på radio eller TV. Journalisten kan exempelvis få förtur till intressant information, bli inbjuden till specialarrangerade resor eller kurser med koppling till det gemensamma intresset om personen efterhand erhåller en välvillig behandling i medierna. En sådan relation som odlas i ett bestämt syfte kan leda till ett informationsberoende från journalistens sida. Om mediekonsumenterna dessutom inte känner till detta beroende kanske de överskattar journalisten som källa. Alla kan förlora på sikt, utom ”aktören”.

En raffinerad metod att favorisera någon är att ge förhandsinformation, värdefull information för fri användning exempelvis i yrkesgärningen, kanske i form av svåråtkomliga fakta, intressanta idéer eller tips. Tillvägagångssättet skulle för en journalist kunna leda till ett beroendeförhållande, genom vilket arbetsprodukterna kunde påverkas externt.

I underrättelsesammanhang talar man om att rekrytera eller värva någon. De olika stegen i denna process har beskrivits i följande termer: kartläggning, kontakt, kultivering och kapning av målobjekt med genomförande av motprestation. Det behöver kanske inte utvecklas närmare. I samband med informationsoperationer vore journalister en värdefull rekrytering.

Skönmåla

Att i politiska sammanhang via medier, diplomatiska kanaler, särorganisationer och andra kanaler genomföra ”kampanjer” i syfte att lägga tillrätta beskrivningar och förklaringar av ett händelseförlopp (timat eller stundande) är inte något nytt. Det är en form av icke-kommersiell påverkan, propaganda. Tänk på PR-operationerna inför Gulfkriget i början av 1990-talet. Ett annat exempel är medieexponering (och andra inslag) inför valkampanjer, i synnerhet om det är fråga om personval, exempelvis presidentval i USA. Det blir då en fråga om skönmålning av den egna sidans idéer och persongalleri och inte sällan en svartmålning av motståndarsidan med inslag av sakliga upplysningar inför valet, betalt reklamutrymme och politiserad propaganda. Även public serviceföretag kan dras in i sådana kommunikationsprocesser därför att processen i sig och dess olika spin-off effekter kan

presenteras som nyheter. Detta gäller även tillsättningsärenden i högre befattningar i synnerhet vid internationella positioner. Om en maktkamp kan förkläs till något positivt för den egna kandidaten, exempelvis i form av förhärligande av visioner, enstaka insatser, betvingande av orättvisor och uppväxtförhållanden kan en förebild skapas, samtidigt som det finns ett nyhetsvärde i inslaget. I en gråzon mellan nyhet och PR kan alltid nyhetsmotivet förstärkas av motiverade aktörer.

Genom att skapa förebilder kan opinionsmässiga genomslag uppnås. I idealfallet skapas inte förebilder, de växer fram till följd av uppskattade insatser. I en gråzon mellan objektiv beskrivning av verkligheten och förskönande, välvillig och även avsiktligt vilseledande tolkning av vad som inträffat öppnas möjligheter till omtolkning av verkligheten. Senare tiders försvar eller förnekande av omfånget av de avrättningar som ägde rum under både Stalins och Hitlers maktutövning bygger på skapade förebilder och vilseledande skönmålning, dock med genomslag inom mycket begränsade målgrupper.

FÖRTALA, FÖRGIFTA OCH SVARTMÅLA

Att svartmåla är motsatsen till att skönmåla och bygger på liknande mekanismer. En förutsättning är viss ensidighet i den bild av verkligheten som presenteras. Skönmålning av A utesluter emellertid inte att A kan ha dåliga egenskaper som förtigs, eller att B (konkurrent, produkt eller ideologi) kan ha goda egenskaper. Svartmålning av A förnekar goda egenskaper hos A och underförstår att B däremot har bättre egenskaper, vilket dock återstår att bevisa. Svartmålning skadar, medan skönmålning stödjer.

Förtal och rykten

Information som är till belastning för A kan spridas genom Bs försorg eller stöd med hjälp av medier. Det kan ske genom avsiktliga ”läckor” vid rätt tillfälle till någon journalist, under omständigheter som gynnar spridning. Snabb spridning av uppgifter försvårar källkontroll och eftertanke. I princip kan informationen vara sann, befinna sig i en gråzon där delar är sanna, eller vara helt lögnaktig och illasinnad. Om informationen är sann kan det vara viktigt att den når beslutsfattare i tid, exempelvis inför beslut om en större upphandling. Om den är osann kan den vålla stor skada.

Exempel

Ett exempel på detta är Kockums försök att sälja ubåtar till Thailand. Förhandlingar pågick när Svenska Freds- och Skiljedomsföreningen gick ut i *Dagens Nyheter* (DN) och beskyllde Kockums för att ha mutat Thailands premiärminister för att erhålla ordern i den hårda konkurrensen. Anklagelserna fick stort genomslag i medierna och påverkade inrikesdebatten i mållandet. Kockums förlorade affären. En revisionsbyrå undersökte utlandsbetalningarna på uppdrag av Kockums och kom fram till att de endast gällde normal marknadsföring. Krigs-

materielinspektionens granskning visade att Svenska Freds- och Skiljedomsföreningen inte kunde eller inte ville precisera sitt påstående. [52] Misstanken att någon konkurrent utnyttjade Svenska Freds- och Skiljedomsföreningen för sina syften har inte bevisats, men kan inte heller negligeras. Agerandet skadade inte bara Kockums, utan kanske även svensk försvarsindustri på angränsande marknader, tidningen och slutligen Svenska Freds- och Skiljedomsföreningen själva. Det är gravt att publicera, och låta publicera, kränkande påståenden som inte kan beläggas. Men det finns uppenbart en gråzon, där det kan vara svårt att avgöra frågan om skuld eller oskuld. Bättre då att ta tid till källkritik än att riskera att gå oklara intressen till mötes.

Exempel

Den egyptiska tidningen *al-Ahram* publicerade en falsk nyhet om att Israel injicerat aidsvirus i 400 palestinska barn. Källan angavs vara en artikel i Israels största tidning, men den referensen var falsk. Artikeln spreds som en nyhet inom arabvärlden och skapade stor irritation. Den israeliska tidningen som falskeligen utpekats som källa protesterade hos Egyptens ambassadör i Tel Aviv. Den israeliske ambassadören i Kairo protesterade också mot beskyllningen. Till sist agerade den egyptiske presidenten Mubarak och tidningen al-Ahram införde en ursäkt, vilket var något ovanligt. Det är däremot inte ovanligt att egyptiska medier framför extrema beskyllningar mot Israel. [53]

FÖRVIRRA OCH FINTA

Osäkerhet

Grundprincipen bakom detta generella tillvägagångssätt är att dölja något genom att göra mottagaren osäker om hur det verkligen förhåller sig, för att därefter lättare kunna bjuda en speciell verklighetsbild. Om det i princip finns ett mönster som skulle kunna avslöja det verkliga förhållandet gäller det att otydliggöra detta mönster. Avledande händelser och sidoordnad information kan överexponeras som ett led i att skapa informationsöverskott och förvirra. Rykten kan förstärkas och spridas. I debattsituationer förekommer det att parterna inför beskyllningar mot varandra, för in detaljer som möjligen har med saken att göra men som är oväsentliga, eller för fram svårbedömda uppgifter introducerade via mer eller mindre okända experter (som i princip kan ha rätt).

Bluff

Ett mer aktivt men också mer riskabelt sätt att förvirra och lura motparten är att direkt bluffa i syfte att ominrikta intresset. En bluff kan dock synas av offret. För sändaren kan det räcka med att den inte avslöjas för tidigt.

---

[52] Furustig, Ljunggren & Unge (2001b), sid. 55-56.

[53] ”Mediemyter om Israel”. *Dagens Nyheter*, 1997-02-26, sid. A8.

Exempel

En framgångsrik bluff är Indiens döljande och avledande agerande inför sina kärnvapenprov år 1998. Det var frågan om en kvalificerad vilseledning av amerikanska CIA. Indierna lyckades dölja både aktivitet och plats. Genom inhemska spårningssatelliter kunde de följa de amerikanska spaningssatelliterna och agera därefter. Förberedelsearbeten inför provsprängningarna doldes för fotospaning genom maskering och aktiviteter under jord. Underjordiska prov detekteras för övrigt i första hand genom seismiska instrument och inte genom satelliter. Inför provserien genomfördes en avledningsmanöver genom att personal och försöksutrustning drogs samman i ett område där robotar brukade provskjutas, men som låg ett hundratal mil från den verkliga provplatsen. Valet av skenbar provplats stred således inte mot ett tidigare mönster och kanske heller inte mot observatörernas förväntningar. Genom samtidiga provsprängningar försvårades analytikernas separation och analys av proven. Både den amerikanska och den kinesiska signalspaningen lurades avseende plats. [54]

Denna bluff visar att det är möjligt för en mindre aktör att vilseleda även de största aktörer. Det är möjligt att vilseleda omvärldsanalytiker. I själva verket är de en målgrupp för vilseledning och informationsoperationer. Till denna kategori kan även större medier hänföras. För att en operation i denna storleksklass ska vara möjlig krävs tidssamordning och en kombination av olika metoder.

Exempel två

Ett betydligt enklare exempel på att bluffa är att lura en stor grupp människor att skicka e-post till en utvald mottagare i syfte att skada dennes verksamhet genom överbelastning av berörd server. Bluffen skulle i så fall bestå i att med missvisande argumentation eller fakta lura sändarna att i god tro ge uttryck för en opinionsyttring. Den typen av vilseföring kan kallas att *inducera* ett önskat beteende.

FÖRFALSKA OCH FÖRVRÄNGA

Gråzonsproblematiken har berörts tidigare i denna skrift. Även i detta sammanhang kan den skönjas. Var går den moraliska gränsen mellan att förbättra en information och att manipulera den? Om vi i stället kontrasterar förädling av information mot degradering är svaret enklare. Att degradering och i extremfallet ren förfalskning är förkastligt är det ingen tvekan om. De metoder som diskuterats kan komma till stånd genom insatser av aktörer utanför det berörda mediesystemet, men också genom agerande eller underlåtelse att agera internt inifrån systemet.

---

[54] Se ref. i not 52, sid. 101-102.

Bilden

En bild ljuger inte, brukar man hävda. Oavsett om det är fråga om stillbild eller rörlig upptagning kan bilden emellertid missleda eller direkt ljuga på flera sätt. Även en äkta och omanipulerad dokumentär bild kan trots detta vara orepresentativ och missvisande i ett vidare sammanhang.

Exempel

Vi utgår tills vidare från att en bild är äkta och omanipulerad förutom att fotografiska skönhetsfläckar kan ha retuscherats. Även ett sådant enkelt ingrepp kan emellertid bli tvivelaktigt. En närbild av president Saddam Husseins ansikte förekom som omslag på ett augustinummer av *Time* år 1990 med texten ”Iraq On The March”. I början av september publicerade *The New Republic* samma bild med en liten ansning av mustaschen och med texten ”Furor in the Gulf”. Likheten med Adolf Hitler – *der Führer* – var uppenbar.[55] Smärre sådana förändringar av en bild kan kanske försvaras som satirisk framställning, men kan också vara ett led i en propagandistisk framställning. Från Sovjettiden och från Kina finns exempel på personer som blivit misshagliga och helt enkelt försvunnit (klippts ut, raderats) från fotografier och uppslagsverk.[56]

En omanipulerad bild kan också sättas in i fel sammanhang eller på ett sådant sätt att betraktaren får en felaktig uppfattning om bildens hemvist. I TV-sammanhang brukar arkivbilder ge bakgrund till händelser som rapporteras och där dokumentation saknas. Med då ska det framgå att det är fråga om arkivbilder. Bildmaterial är tillgängligt på öppna marknaden varför det kan uppstå osäkerhet om bildens ursprung och äkthet, i synnerhet när material ställs till förfogande av olika aktörer. En felbedömning kan leda till oavsiktligt missvisande publicering. Från Gulfkriget på 1990-talet finns det en bild av en oljeskadad fågel som förknippas med irakiska oljesabotage. Fågeln lär emellertid ha härstammat från ett helt annat bildmaterial. Från kriget i forna Jugoslavien finns det en bild av en extremt smal och utmärglad man som befinner sig bakom nätstaket i ett läger. Han förknippas intuitivt med svåra umbäranden. Mannen lär emellertid ha varit inlånad som fotoobjekt för ändamålet. Sant eller inte, exemplen belyser att mycket små medel kan ge stora effekter.

Bilder kan vara äkta men likväl missvisande genom att de arrangerats. Soldater på post förmås börja skjuta vilt inför kameran; folk på gatan att dansa av glädje. Motsvarande metoder kan naturligt komma till användning i traditionella vardagsreportage för att försköna eller dramatisera en framställning, exempelvis genom att

---

[55] Nordström ”Bildens roll i nyhetsförmedlingen”, sid. 69-70 i Nordlund (red 1992). Se också Pettersson ”Trovärdiga bilder”, SPF rapport 180 och Pettersson ”Bildmanipulering”, SPF rapport 181 samt skriften ”Nyhetsbilder etik – påverkan”, SPF meddelande nr 154.

[56] Jaubert (1986).

fotoobjektet poserar i utvald miljö. Värre är om metoderna kommer till användning även i nyhetsreportage, i sammanhang där felaktiga politiska och säkerhetspolitiska slutsatser skulle kunna dras.

Datorstödd manipulering är en metod som erbjuder obegränsade möjligheter att presentera den önskade verklighetsbilden. Det är möjligt att förändra bakgrund, förgrund och huvudmotiv efter önskemål. En tecknad rörlig streckgubbe kan kläs på med valfri kroppsform, ansikte och kläder. Metoden kan användas för att skapa ett bildmaterial som återger en händelse så korrekt som kunskapen medger, i brist på äkta material. Syftet skulle då vara att rekonstruera ett faktiskt förlopp. Tyvärr kan syftet lika väl vara att illustrera ”sin bild av verkligheten”.

När en prototyp av JAS kraschade under landning inför publik i Linköping år 1989 filmades förloppet av SVTs nyhetsprogram *Aktuellt*. Av säkerhetsskäl beslagtogs emellertid filmen omedelbart för att efter kort tid återlämnas. Under mellanperioden animerades förloppet för att kunna visa (*sic*) att och hur olyckan ägt rum och detta konstruerade förlopp lades ut i en extrasändning innan den riktiga filmen återlämnats två timmar senare. Bilder från tidigare tagningar kom till användning och manipulerades med datorstöd. Sekvensen uppfattades som äkta och publicerades i finska tidningar. [57]

En hypotetisk och extrem variant av att manipulera enstaka bilder eller en bildserie vore att ”ta över” ett visst program eller en hel kanal för att temporärt återutsända något annat i stället eller för att störa ut det misshagliga. Huruvida det är möjligt eller inte beror på hur sändningen sker: markbaserat, via satellit, via kabel, etc. De tekniska och fysiska alternativen till att eventuellt genomföra sådant diskuteras inte här.

Orsaken till att bildmanipulering har behandlats så relativt utförligt är bildens stora genomslag på konsumenterna, att bildjournalistikens betydelse ökar och att bilden (statisk eller dynamisk) dominerar över texten som kommunikationsform. Som ett exempel kan nämnas att de bilder som amerikansk TV sände från Somalia efter interventionen där och som återgavs i skilda medier, bland annat med en avklädd och skadad amerikan som släpades efter ett fordon, bidrog till det amerikanska tillbakadragandet.

Text och ljud

Satir och humor ger möjligheter att kritisera och driva med negativa företeelser. Frihetsgraden är hög för olika former av litteratur, sång, revy och dans. Artisten Karl Gerhard angrep nazismen i satirisk revyform under 1930- och 40-talen. Imitatörer har en tacksam roll i sammanhanget. Avigsidan är att imitatörer kan lura lyssnare i allvarliga sammanhang, exempelvis genom att ge sken av att vara någon officiell

[57] Alling-Ode & Tubin (1993), sid. 111-114.

person och uppmana till åtgärder som inte är önskvärda. Politiskt material kan spridas under satirens täckmantel, till exempel komikern Michael Moores film *Farenheit 9-11*.

Hemsidor

Att manipulera databaser och olika myndigheters (mediers?) webbsidor är ett hackernöje och en metod för olika typer av aktivister att visa sina färdigheter och preferenser. Det finns minst en webbplats som innehåller exempel på hackade webbsidor (http://www.flashback.se/hack). I Sverige har för övrigt Post- och Telestyrelsen tillskapat ett IT-incidentcentrum (www.sitic.se) som sammanställer aktuell hotbild från virus, maskar och trojaner samt ger goda råd hur man skyddar sig.

FÖRHINDRA OCH FÖRNEKA

Det är i praktiken stor skillnad mellan att försvåra och försena en kommunikation och att förhindra den, även om syftet fortfarande är att dölja något under viss tid. Myndigheter kan med hjälp av sekretesslagar legitimt reglera tillträdet till viss information eller, vilket inträffade någon enstaka gång under andra världskriget i Sverige, införa beslag av tryckt material. Ingreppen mot *Göteborgs Handels- och Sjöfartstidning* kan exemplifiera det senare.

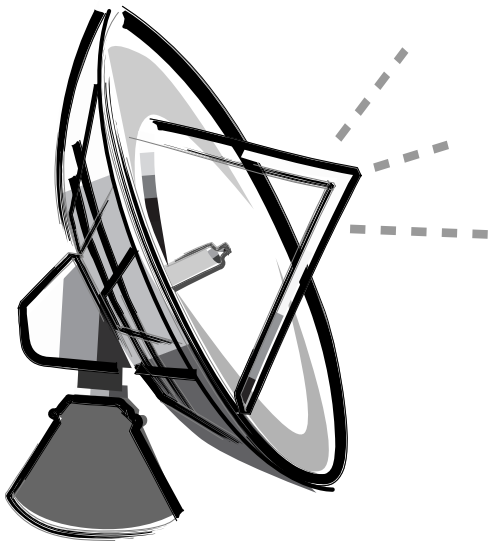
Ser man informationsprocessen ur mediernas perspektiv, och med viss fantasi, kan följande inträffa. Vissa kritiska indata som behövs inför en journalistisk bearbetning har raderats eller så är aktuella databaser inte längre tillförlitliga på grund av åverkan. Bearbetningen av information i Intranet blockeras genom att befintliga hjälp- och analysprogram har skadats. Eventuellt är server och datasystem överbelastade och tillfälligt blockerade eller utslagna, liksom övriga teletekniska kommunikationssystem. Elektronisk bearbetning av slutprodukt, liksom spridning av denna är inte att tänka på med befintliga störningar på kraftförsörjning och kommunikationsnätverk. Kort sagt, med hjälp av olika tekniska och programmeringsmässiga metoder kan arbetsrutinerna störas och enstaka fel kan sannolikt induceras mer permanent. Det mesta är emellertid åtgärder som varar endast på kort sikt på grund av de motåtgärder som vidtas. Om informationssystem ska slås ut på längre sikt krävs mer destruktiva åtgärder.

Exempel

Hackers eller crackers ska tillfälligt ha ”övertagit” kontrollen av en av Storbritanniens militära kommunikationssatelliter och begärt en lösensumma för att inte störa satellitens omloppsbana.[58] Om informationen verkligen är korrekt belyser den möjligheterna att manipulera eller störa en satellit, alternativt att bluffa.

---

[58] *Ny Teknik* 1999 nr 9, sid. 18.



FÖRSTÖRA

Informationskrigföring eller ledningskrigföring behandlas inte närmare här, men några korta kommentarer till vad som kan inträffa motiveras av att det är fråga om det sista ledet i en upptrappad händelsekedja som avslutas genom maktutövning genom våld.

Kanske är det möjligt att förleda personal anställd i en myndighet eller ett företag till att i god tro vidtaga någon felaktig eller kontraproduktiv åtgärd som bidrar till att ett IT-system eller nätverk slås ut eller förstörs. Orsaken skulle kunna skyllas på kategorin ”den mänskliga faktorn”. Det är emellertid knappast möjligt om arbetsrutinerna är goda.

Med tekniska hjälpmedel kan utrustning förstöras för gott. Elektronisk utrustning kan slås ut lokalt genom elektromagnetiska pulser med hög energinivå. Anläggningar och nätverk kan på olika sätt förstöras fysiskt. Personal kan drabbas av akuta sjukdomstillstånd genom avsiktlig förgiftning i personalmatsalen. Dessa metoder gränsar till ”övriga åtgärder”.

Gråzonsagerande

Med *gråzon* menas ett svåravgränsat område mellan ett agerande som är professionellt och moraliskt respektive ett som strider mot yrkesprofessionalitet och god sed, avtal eller moral. Ett sådant agerande kan inte enkelt klassificeras som rätt eller fel, bra eller dåligt. Det kan till exempel vara bra att brott, missförhållanden och skandaler avslöjas samtidigt som det är fel eller tveksamt att systematiskt använda (brotts-) provokation och dolda registreringsmetoder i detta syfte, metoder som inte är tillåtna för vår brottsbekämpande polis. Arbetstekniken kan exempelvis kännetecknas av Wallraffande, dold inspelningsteknik, provokativt och falskt uppträdande etc.

Följande principiella exempel på olika former av gråzonsagerande har tidigare omnämnts, om än i något andra ord:

- Särintresse döljs under någon annan roll för att lättare uppnå tillträde till mediekanaler.
- Vidarepublicering motiveras av konkurrensskäl på bekostnad av källkritik. Rundgång.
- God tro och mänskliga brister utnyttjas för att dölja avsiktligt agerande.
- Uppseendeväckande påståenden utnyttjas för att skapa nyhet och genomslag.
- Försåtlig blandning av fejkade och ihopklippta intervjuer och arkivbilder.

Det föregående får naturligtvis inte tas till intäkt för misstänkliggörande av medarbetare som råkar begå enstaka misstag i sin yrkesverksamhet. Det är mänskligt. Vad som här avses med att agera i gråzon, är ett systematiskt och därmed avsiktligt agerande, där bortförklaringen är täckmantel.

Till detta kan läggas ytterligare några aspekter av gråzonsagerande.

KRISHANTERING

I samband med svåra olyckor i samhället har det visat sig kunna bli problem med störda kommunikationsmedel, exempelvis överbelastade telefonnät. Kris, bristande information och kommunikation är goda grogrunder för ryktesspridning. Det kan leda till svårigheter för medierna att samla in fakta och att distribuera information. Samtidigt inträffar väldigt mycket. Det kommer kanske in uppgifter från tidigare okända källor. I ett akutskede torde det vara samhällets informatörer och talesmän (exempelvis räddningsledare och polis) som ska lämna besked till allmänhet och medier. I övergångsfaser kan det vara svårt att leva upp till källkritik, informationsvärdering och strukturering av materialet för alla parter. I en sådan situation kan vilseledande information och rykten spridas. Kanske kan valda delar av samhällets och mediernas kommunikationsvägar avsiktligt störas ut för att därmed lättare medge spridning av falska budskap. Skulle det kunna tänkas att någon försökte utnyttja konkurrens och skillnader i arbetsbetingelser mellan lokala medier och regionala (centrala) medier i en krissituation? Vore att så split mellan nyhetsförmedlande konkurrenter ett sätt att lättare få spelrum för att föra fram falska budskap?

KONFRONTATION

Konfrontationsjournalistik och skjutjärnsjournalistik kan skapa blottor. Om den part journalisten tar ställning för kan presenteras som den svagare erhålles omgivningens stöd i kampen mellan David och Goliat. Det är sannolikt risk att myndigheter och politiker alltid får spela Goliat i detta spel, vilket kan öka politikerförakt och avståndstagande. Det är gott och väl att avslöja brister i samhället. Det är inte bra om det fabriceras (provoceras fram, insinueras) svårbedömbara situationer som ser ut som brister. Metoden kan missbrukas.

OPINIONSMÄTNING

Medierna eller någon annan aktör kan genomföra opinionsmätningar på eget initiativ och om resultatet visar sig vara i linje med den egna favorithypotesen har en nyhet skapats och frågan kan drivas. I annat fall är det risk att resultatet läggs åt sidan, även om det vore en lika stor nyhet om alternativhypotesen hade bekräftats. Detta kan vara ett sätt att få underlag för kritik mot enskilda beslutsfattare, samhällsfunktioner eller företag. Det kan framför allt vara ett sätt att skapa opinionslåsning bland allmänheten och beslutsburar för politiker och andra beslutsfattare. Metoden kan således missbrukas.

Face value

Det är naturligtvis viktigt att kunna skydda strategiska intressen mot informationsoperationer. En förutsättning för att kunna exponera mottagaren (offret) för det avsedda budskapet är att överföringen och spridningen av budskapet säkerställs. Penetrationsvägen för detta går med fördel via medierna, varvid metoder av den diskuterade typen används. För att minska penetrationssårbarheten och mottagligheten för inplanterad information och rykten är det viktigt att medierna ägnar sig åt aktiv nyhetsbevakning och nyhetsförmedling. För att exemplifiera vad som avses, diskuteras här en viss aspekt av nyhetsförmedlingen i samband med giftkatastrofen i floden Rhen. Exemplet handlar om den förorening av floden som inträffade 1986.[59] En nyhetsnotis såg ut på följande sätt:

> ***”Stasi kan ha legat bakom giftkatastrof***
> *SCHWEIZ. Giftkatastrofen i Rhen år 1986 efter ett utsläpp från den schweiziska kemikoncernen Sandoz var resultatet av ett sabotage av den dåvarande östtyska säkerhetstjänsten Stasi. Det hävdar en tidigare officer inom USA:s underrättelsetjänst CIA. Motivet skulle vara att leda bort uppmärksamheten från de enorma miljöskador som Tjernobylkatastrofen ett halvår tidigare hade orsakat.”* [60]

Det som startade mediebehandlingen var ett TV-program i den tyska kanalen *ZDF* under temat ”History” den 19 november 2000. Inom ett par dagar förelåg cirka 10 artiklar på nätet om händelsen i engelska, tyska och franska medier. Det är anmärkningsvärt att alla artiklar utom en återgav samma information. Endast en källa skiljer sig från de övriga vad gäller sakinnehåll. En journalist, Vogel vid *Basler Zeitung,* granskade nämligen fallet på egen hand och återgav inte enbart TV-programmets innehåll och påståenden.

---

[59] En fallstudie om detta har ursprungligen publicerats av Furustig, Ljunggren & Unge (2001b), sid. 117-124.

[60] *Metro*, 2000-11-25, sid. 3. Metro i sin tur anger Tidningarnas Telegrambyrå, Norska Telegrambyrån (TT-NTB) som ursprungskälla. Författaren har inte noterat att denna information återfunnits i andra svenska medier.

Det påstods att en inspektionsrapport från ett försäkringsbolag i Schweiz rörande säkerheten vid kemiföretaget Sandoz i Schweizerhalle kommit i händerna på den östtyska säkerhetspolisen Stasi, vilket sedan utlöste kemikatastrofen med stöd av kännedom om svagheterna i anläggningen. Det uppstod sedermera en omfattande brand i Sandoz anläggningar och i samband med släckningsarbetet läckte miljöfarligt avfall ut i floden Rhen. Efter branden sägs inspektionsrapporten ha överlämnats till en representant för De Gröna i förhoppning om att den miljömedvetna opinionen i väst skulle mobiliseras. Uträkningen skulle ha varit att avlänka mediekampanjen från reaktorkatastrofen i Tjernobyl och påvisa att väst var lika goda kålsupare som öst.

Den *enklaste* tolkningen av fallet är att någon ”miljömedveten” person skickat de berörda dokumenten (delar av rapporten) till en representant för miljöpartiet De Gröna för kännedom och eventuell åtgärd. Utsläppen i Rhen skulle kunna förklaras med läckage av förorenat vatten från släckningsarbetet inne på kemilagret. Branden kan i och för sig ha haft en naturlig orsak.

Utan att gå in på enskildheter visade materialet att många aktörer eller intressenter varit eller påståtts vara inblandade. Men detaljerna lämnas därhän här. Det visade sig att preskriptionstiden skulle löpa ut 2001-11-01. Schweiziska myndigheter var beredda att ta upp fallet till ny granskning om det framkom nya fakta med bevisvärde. Kanske skulle den nytillkommande informationen via TV-programmet 2000-11-19 utgöra incitament till förnyad prövning? Vissa nyhetsmässiga ”kryddor” i affären (detaljer återges inte här) skulle kunnat vara ett inslag för att öka uppmärksamhetsvärdet men hade också koppling till juridiska påföljder och därmed intresset för myndigheterna att fortsätta utreda fallet. En tidigare utredning som utfördes av schweiziska myndigheter ledde till att mordbrand inte kunde beläggas, men inte heller uteslutas.

Händelsen kan *möjligen* tolkas som en informationsoperation med ursprungligt syfte att avlänka fokuseringen mot Tjernobyl. Fallet kan senare ha övergått till en annan IO i syfte att aktualisera en juridisk nyprövning. (Utgången av fallet har inte följts upp och är inte poängen här.) Fallet visade sig vid granskning ha mycket anmärkningsvärda och uppseendeväckande inslag och borde ha väckt stor uppmärksamhet och föranlett kritisk granskning från olika mediers sida. Av ett tiotal nyhetsreportage i medierna var emellertid endast ett enda kritiskt granskande och de övriga var reproducerande. Det granskande reportaget innehöll intervjuer och kompletteringar av händelseförloppet enligt TV-programmet. Det okritiska återgivandet antyder en potentiell penetrationssårbarhet inom berörda utländska medier vid detta tillfälle.

Uppenbarligen litade de reproducerande medierna på uppgifterna i TV-programmet. Både medier och informationskonsumenter bör begrunda sentensen ”*accept nothing at face value*”.

Diskussion

Massmediernas betydelse som kanal i samband med informationsoperationer har exemplifierats tidigare. Här följer några av de bidragande orsakerna:

- Medier sätter agendan. Att bestämma vad som fokuseras är en förutsättning för att kunna influera.
- Medier kan bestämma urvalet, det vill säga vilka inlägg, fakta och indata som prioriteras i informationsflödet.
- Medier har meddelarfrihet. Källor måste skyddas.
- Medier når ut till en stor målgrupp, även om allmänhetens förtroende kan vara sjunkande idag.

Naturligtvis kan man inte misstänka att det är fråga om en informationsoperation varje gång medier påverkas av någon aktör med ett mer eller mindre uppenbart motiv. Det sker ständigt. Intresset kan nämligen vara osjälviskt eller i övrigt helt legitimt. Det kan till exempel vara så att aktören har någon specialkunskap som gör det motiverat att agera och försöka väcka förståelse för eller insikt i en viss fråga. Antag att någon kontaktar en kvällstidning med ny och uppseendeväckande information om något allvarligt brott, en olyckshändelse eller något tänkbart hot. Är det fråga om ett uppslag till undersökande journalistik med ett verkligt ”scoop” som belöning, ett försök att locka till engagemang i en ”story” med helt andra bottnar än vad första intrycket antyder, eller bara dumheter?

För att förhindra medierna från att utnyttjas vid informationsattacker kan det vara skäl att inledningsvis betänka följande frågor av typen ”*att se upp med*”:

- Vem försöker påverka agendan?
- Varför just nu?
- Vem erbjuder bakgrundsmaterial?
- Försöker någon avlänka den rådande fokuseringen?
- Vem drar nytta av eventuell publicering?
- Är fakta kontrollerbara, har de kontrollerats, när kontrollerades de och av vem?

Några analysansatser

Uppgiften här har varit att diskutera tänkbara tillvägagångssätt vid manipulation av verklighetsbilden i samband med informationsoperationer via medierna. Syftet på sikt är att fundera över hur medierna skulle kunna skydda sig mot missbruk i rollen som omedveten aktör eller redskap. Det kan därför vara motiverat att avslutningsvis föra ett principiellt resonemang och antyda några strategier för att skydda verksamheten mot sådana operationer som ett led inför fortsatta studier.

Ett traditionellt angreppssätt är att granska den egna konkreta verksamheten med hjälp av kvalitativ riskanalys. Det handlar (1) om att identifiera de svaga punkterna i systemet. Hur ser sårbarheten ut? (2) Hur sannolikt är det att olika

hot[61] ska utlösas eller inträffa? (3) Vad blir konsekvensen om så sker? Har systemet råd med det? Med ”system” avses här en organisation som arbetar med information eller ett medieföretag. Ett sådant ”system” kännetecknas av följande faktorer som bör granskas systematiskt ur sårbarhetssynpunkt: [62]

- En teknisk kärna med hjälpmedel för exempelvis kraft, tele och informationsbehandling.
- En organisatorisk infrastruktur där människor och tekniska hjälpmedel samverkar.
- En mänsklig resurs som kännetecknas av värdefull kompetens och tillgänglighet.
- Ett fysiskt gränssnitt (skal) mot omgivningen (yttre skydd <—> inre skydd?).
- Ett virtuellt gränssnitt mot omgivningen (informationsflöden).
- En formell struktur som reglerar tillåtlighet (juridik, konventioner, avtal).

Homo Informaticus[63] är en egendomlig art som står i centrum för den moderna tekniken när det gäller att inhämta material för att bearbeta, producera och distribuera detta till förädlad information. Tyvärr blir inte all information förädlad utan snarare degraderad, antingen genom olyckliga omständigheter, naturkatastrofer eller genom avsiktligt agerande från representanter av samma egendomliga art. Frågan är hur degradering genom informationsattacker kan hanteras. En systematisk ansats till motverkan kan vara att:

- förutse (exempelvis genom analys av egna svagheter och yttre hot),
- försvåra tekniska angrepp (av typen störningar av informationshanteringen),
- förhindra vilseledande information (exempelvis genom källkritik, grindväkteri, goda rutiner etc),
- förmildra effekter av angrepp (exempelvis genom beredskap, övning och tekniska motåtgärder).

KNISLUND & KNASLUND

Ett sätt att göra detta skulle kunna vara att ta angriparens roll, det vill säga skifta perspektiv, vara ”djävulens advokat”, och med kännedom om egna svagheter inse hur en kunnig angripare skulle kunna gå till väga. Ett annat sätt vore att anlita pålitliga experter, som genom egna attacker objektivt kunde kartlägga brister och föreslå motåtgärder, till exempel genom så kallade *Red teams*. Myndigheter, nätverk inom

---

[61] Ett hot är ett möjligt scenario med negativa konsekvenser vid utfall. En risk i teknisk mening är en sammanvägning av sannolikheten för en händelse och dess konsekvens. En kvalitativ riskbedömning av hotet ”x” kan vara ”låg sannolikhet och stor konsekvens”, vilket kan innebära att risken som förknippas med ”x” bedöms som ”oacceptabel” och slutsatsen skulle kunna bli ”omedelbar åtgärd”. (Ordet risk kan emellertid användas även i andra mer vardagliga betydelser.) ”x” skulle kunna vara något specifikt säkerhetsfel i ett kärnkraftverk.

[62] Med sårbarhet menas här de svagheter som finns i ett system när det gäller att motstå hot; skillnaden mellan önskad säkerhet och faktisk säkerhet.

[63] Furustig (1996). Från Friman, Sjöstedt & Wik (eds 1996), sid. 141-158.

den egna branschen och säkerhetsorganisationer utgör resurspool. Vid hot om allvarligt storskaligt angrepp kan internationellt samarbete kanske vara motiverat.

GRUNDLÄGGANDE ANALYSMETODER

Systematisk riskanalys, sårbarhetsanalys och hotbildsanalys har tidigare berörts. De är fundamentala verksamheter som tillsammans med omvärldsanalys förbättrar verklighetsbilden av den egna verksamheten och dess miljö.

INTERNA VARNINGSSIGNALER

Drucker[64] har betonat betydelsen av en organisations föreställningsram vid utvecklingen av organisationen. Frågan som väcks är om organisationens policy är adekvat, förlegad eller i värsta fall ogiltig för den tid och det sammanhang som den är verksam i. För diskussionen här åsyftas den policy som bestämmer attityderna till strategiskt tänkande, kvalitetstänkande och säkerhetstänkande i vid bemärkelse i ett informationsbearbetande företag. Om föreställningsramen blivit obsolet kan det redan vara sent att göra något åt saken. Finns det några varningssignaler som kan indikera ett förändringsbehov, innan?

Drucker nämner följande allmänna kännetecken som kan utgöra varningssignaler. Om de uppfattas på rätt sätt utgör de incitament till förbättringar och nya möjligheter!

- Oväntade misslyckanden och bakslag kan indikera felaktiga föreställningar.
- Oväntade framgångar kan (förutom ett gott arbete) bero på brister i verklighetsbilden.
- Snabba och okontrollerade förändringar inom organisationen.
- Allt går som vanligt sedan länge.

De kan avse arbetsrutiner som blivit sediment, det vill säga ej följt med i utvecklingen, missade nyhetsreportage, uppseendeväckande inlägg som efteråt visat sig tveksamma (källkritik, ”grindväkteri”, praxis) och kritiserade reportage typ ”drev” (policy, praxis), samt störd och försenad produktion (IT-säkerhet).

Den första försvarslinjen består i att se verkligheten. Den som inte tittar, ser inte. Den som inte lyssnar, hör inte. Den som inte tror på egna svagheter, finner dem inte. Den som inte aktivt och kritiskt granskar signaler och värderar information upptäcker inte varningssignalerna.

Människan har en selektiv varseblivning, hon tar till sig det hon vill ta till sig och hon tolkar information på ett subjektivt sätt efter förväntningar och önskningar. Något liknande förekommer inom organisationer. Ett organisatoriskt klimat och

---

[64] Drucker (1995). Framställningen har hämtats från Furustig (sid. 154-155) i Friman, Sjöstedt & Wik (eds 1996).

arbetssätt kan filtrera det nya och bevara och bekräfta det gamla. Om den organisatoriska attityden i ett informationsbearbetande företag är ”vi är professionella, vi är inte sårbara, vi begår knappast misstag, vi blir inte lurade och vi fortsätter som vi alltid gjort” är det troligt att man är sårbar, begår misstag och blir lurad, den korta tid man är kvar på marknaden.

Indikatorer [65]

Vilka varningssignalerna är och hur de kan upptäckas är ett viktigt problemområde inom många verksamhetsområden, exempelvis vid finansiella tjänster, underrättelsetjänst och marknadsföring, för att nämna några. Omvärldsanalys förutsätter någon form av inriktning, fokusering. För medias del är det viktigt att kunna särskilja falska, missvisande och korrekta insignaler från varandra och från bruset. Dessa insignaler utgör representationer av omvärlden och om dessa representationer är felaktiga blir också medias presentation av verkligheten missvisande, vilket torde vara målsättningen för aktörerna vid en informationsattack.

Analys av *för verksamheten kritiska* signaler är numera ett forskningsområde (weak signal research). Att ge konkreta kännetecken (indikatorer) på tidiga signaler i samband med en informationsoperation via medier är en uppgift i sig. Här kan endast några introducerande reflexioner göras.

I en artikel [66] påpekas sambandet mellan tidpunkten i en händelseutveckling och styrkan av motsvarande signaler.

- Vaga signaler. Mycket tidiga signaler är så svåra att upptäcka att de kräver kvalificerad expertis. Samtidigt ger de utrymme både för reaktionstid och också handlingsutrymme innan ”krisen” bryter ut.
- Svaga signaler. Ofullständig information kan tolkas med viss kunskap. De kan medge relativt lång svarstid och handlingsutrymme.
- Starka signaler. Uppenbar information uppfattas av varje god observatör. De kan ge utrymme för motreaktion.
- Hyperstarka signaler. Föregår det omedelbara utbrottet av en kris (motsvarande). Informationen är uppenbar även för en icke-expert. Begränsat handlingsutrymme och knappast någon tid för reaktion.

Exempel

Adolf Hitlers bok *Mein Kampf* ger en relativt rättvisande bild av vilka politiska mål som Hitler eftersträvade. Boken kan uppfattas som en signal till sina mottagare, en avsiktsdeklaration. Det är många aktörer som inte underlättar för mottagarna

---

[65] Avsnittet grundar sig på Furustigs ”Analys av svaga signaler” i Furustig, Ljunggren & Unge (2001a), sid. 125-132.

[66] Sauerwein (1993), sid. 355.

genom att avge avsiktsförklaringar. Samtidigt behöver inte en politisk signal vara uttryck för en politisk avsikt, det kan vara fråga om en försöksballong. För nutida läsare, med facit i hand, upplevs nog denna signal som *stark*. Detta till trots, tolkades bokens agenda, så som vi idag uppfattar det, knappast på ett adekvat sätt av dåtidens informationskonsumenter. Hitler var visserligen inte etablerad politiker vid bokens utgivning, men den var *tillgänglig* för alla presumtiva läsare. I dag är den inte längre tillgänglig på bokhandelsdiskarna. Dåtidens ”normalbild” var synnerligen turbulent, ekonomiskt och politiskt. Det kan ha försvagat signalens relativa styrka i förhållande till denna bakgrund av *brus*. Boken kunde ha tolkats som en varningssignal med vår terminologi. Den uppfattades tydligen inte på det sättet. Det kan ha berott på att den tidens föreställningsram och referenser var annorlunda än dagens, men här skall dock inga ytterligare resonemang föras kring detta. Poängen är att det budskap som i bokform spreds till den allmänna opinionen kan sägas ha representerat:

- en avsiktsförklaring,
- en tidig signal,
- en stark signal,
- ett tillgängligt ostört budskap.

Det gäller att finna former och kriterier för att:

- uppmärksamma förekomsten av, för sammanhanget kritiska, signaler,
- identifiera egenskaperna hos de kritiska signalerna,
- bedöma hur dessa signaler ska hanteras under osäkerhet och tidsbrist,
- ”känna” signalen (sammanhanget, närmiljön, omvärlden, sambanden),
- ”känna” bruset (normalbilden), som möjliggör att signalen kan särskiljas.

Motverkan

I föregående avsnitt diskuterades betydelsen av att upptäcka och indikera varningstecken, kriterier på signaler som ingår i informationsoperationer. Det nämndes också att organisationens attityd till hot från omvärlden påverkar dess möjligheter att göra något åt dem, det vill säga minska sin sårbarhet. Kanske finns det skäl att separera vad som i princip kan påverkas och förbättras, respektive vad som inte kan påverkas av den berörda organisationen (systemet), men där effekterna likväl kan förmildras och bemötas *ad hoc*. I tabellerna 6 och 7 görs ett försök att systematisera några av tankarna.

Tabell 6. Exempel på strukturering av angrepps- och försvarsaspekter vid informationsoperationer.

Operationens karakteristika?	Skyddsaspekter. Psykologiska åtgärder.	Skyddsaspekter. Tekniska åtgärder.	Skyddsaspekter. Övriga åtgärder.
Attack med påtagliga psykologiska åtgärder.	Korrigera, bemöta. Mediesamverkan. Snabbhet. Nätverk.	Skydda äkta källa. Spåra falsk källa. Skydda kommunikation.	Beredskapsåtgärder? Myndighetsstöd?
Attack med påtagliga tekniska åtgärder.	Centrala incidentrapporter. Webbaserat infosystem. Intern snabb-info. Upplys enligt policy.	Statlig rådgivning. Säkerhetssystem. Kontrakterade experter. Reservförfaranden. Spårning.	Beredskapsåtgärder? Myndighetsstöd?
Attack med påtagliga "övriga" åtgärder.	Samverka med nationella myndigheter. Beredskapsåtgärder –>	Samverka med nationella myndigheter. Beredskapsåtgärder –>	Se tabell 7. Är attacken internt eller externt riktad?

I normalfallet utgör Internet en värdefull kanal både för inhämtning och utbyte av information. Det kan sedan missbrukas på olika sätt, exempelvis för att föra in osäker eller felaktig information, för att angripa användarnas system genom s k virus, maskar och trojaner, eller för att kartlägga vissa målgrupper utan deras vetskap. Men webben kan också användas som en nationell svensk portal för krisinformation, för webbsidor till olika myndigheters och kommuners meddelanden och till ett webbaserat informationssystem. (Se till exempel SPFs utbildningsserie 3 och publikationer tillgängliga på myndighetens hemsida www.psycdef.se.) I själva verket väger de positiva möjligheterna över de negativa för normalanvändaren, men konsekvenserna av en nätattack gör att det är rationellt att skydda sig mot en sådan, även för normalanvändaren. Det gäller i än högre grad för den som är beroende av informationshantering.

Tabell 7. Exempel på strukturering av försvarsstrategier vid informationsoperationer.

Attack mot –> Motverkan typ	Inre systemmiljö	Gränssnitt	Yttre miljö
Förebygga innan.	Utbilda. Policy. Intern riskanalys. Kvalitetssäkra. Inre skydd. Skapa kristeam. Försäkra. Förbättra. Uppföljа. Testa!	Skalskydd. IT-skydd. "Grindväkteri". Källkritik. Riskanalys. Samverka i nät. Återförsäkra funktion. Testa!	Skapa nätverk. Branschnätverk. Finna indikatorer. Omvärldsanalys. Förvarning.
Reagera på.	Beredskap. Jour. Reservförfaranden. Kristeam. Rapporteringsvägar. Upplysa och informera.	Rutiner. Back-up. Funktionssäkra. Rapportera. Samverka.	Återförsäkra. Samverka myndigheter. Samverka kollegialt. Samverka expertföretag. Informationssamverka.
Agera.	Internutbilda –>	Öva krishantering –>	(Psykologiska åtgärder). (Polisiära åtgärder). (Tekniska åtgärder). (Juridiska åtgärder). (Forska och utreda).

ETT EXEMPEL – FALLET EMULE [67]

Följande händelse, som är verklig, är ett exempel på konsekvenserna av bristande nyhetskontroll.

Bakgrund. Det Kalifornienbaserade företaget Emulex tillverkar fiberkabel och mjukvara som möjliggör snabb nätverkshantering och system för att lagra information. Verksamhetsområdet är konkurrensutsatt. Under år 1999 uppnådde företaget en vinst, men i april år 2000 föll aktien från 218 till 41 enheter. Investerare hänförde det till att företagets speciella nätverksstandard utsattes för hård konkurrens från Ethernet- och Internetprotokoll. Aktievärdet återhämtade sig emellertid och steg till 113. Därefter inträffade vad som kan kallas för en informationsoperation.

Indikation. Emulex aktievärde sjönk plötsligt över förmiddagen med 57 %, vilket motsvarade en förlust av ungefär 2 miljarder dollar.

Händelser. I samband med att börsmarknaden öppnade för dagen återfanns en pressrelease på Internet som hävdade att Emulex vinst under första kvartalet skulle förändras till en förlust, att revisorer undersökte tveksamheter i redovisningen och att ledningen skulle träda tillbaka. Företaget förnekade häftigt denna information.

Moteld. Emulex kontaktperson gentemot medierna, en kvinna, förnekade helt uppgifterna och omtalade att ett pressmeddelande förbereddes och att källan till den falska informationen på Internet skulle spåras med hjälp av Nasdaq och Securities and Exchange Commission. Av eftermiddagens pressmeddelande framgick att en kontroll av budgetårets resultat inte visade behov av någon korrigering utan att affärerna befann sig på ”record levels”. Dessutom skulle företaget bedriva en egen undersökning av bedrägeriet.

Spridning. Den falska pressreleasen återfanns först på Internet Wire omkring klockan 09.30 fm lokal tid. Därefter spreds den till några olika nyhetstjänster, särskilt Bloomberg. Men den återfanns inte på de ledande Business Wire eller PRNewsWire och inte heller på Yahoo!Finance. Omkring kl 10 började det komma indikationer på prisfall. Efter kl 10.30 fm började ledande nyhetsorganisationer till exempel Dow Jones News Service och CBS Marketwatch uppmärksamma och avrapportera. Nasdaq avbröt handeln kl 10.35 fm. Det var först omkring kl 11 som Emulex förnekande uppmärksammades på webbsidor och TV-kanaler.

Sårbarhet. Fallet påvisar att både aktiemarknaden och det enskilda företaget var sårbara för den falska informationen. Även ett annat företags aktier, ett företag som tidigare tillhört Emulex, gjorde förluster under morgontimmarna. Det falska ryktet levde visserligen endast under ”kort” tid, men på den korta tiden blev svängningarna på marknaden i storleken miljarder dollar.

Aktör. Det visade sig att det var en 23-årig hacker från Kalifornien som förfalskat pressmeddelandet. Någon uppföljning av om någon konkurrent anlitat hackern eller av det rättsliga efterspelet har veterligen inte gjorts i detta sammanhang.

---

[67] http://abcnews.go.com/Business/print?id=89443. Fallet har också kommenterats i nyhetsbrevet *Delete*, nr 3 år 2000.

Av exemplet framgår att det är möjligt att avsiktligt uppnå stora effekter med små medel. Alla ovanliga händelseförlopp behöver inte vara utstuderade och avsiktliga, men kan bli nog så komplicerade av inneboende kraft, i synnerhet om medierna utan ond avsikt hjälper till och om nyhetskontrollen är bristfällig.

Fortsatt arbete

En allmän framställning om informationsoperationer och *modus operandi* kan behöva kompletteras med att systemnära, i direkt anslutning till den egna organisationens arbetsvillkor och miljö, arbeta igenom tänkta och möjliga hotbilder, egen sårbarhet och vilka konsekvenser sårbarheten skulle kunna medföra.

Medierna utgör inte någon homogen bransch. De olika produktions- och spridningssätten och slutprodukternas olika former, till exempel radioprogram eller tidningar, påverkar inte bara mediernas teknik, arbetssätt och organisation utan även deras sårbarhet. Därför behövs den *systemnära* och konkreta verklighetsanknytningen.

En sådan anknytning skulle kunna ske i form av analyser och spel eller simuleringar, vid behov med stöd av lämpliga samarbetspartners. Det synes också viktigt att genom samverkan inom branschen och med berörda myndigheter skapa nätverk för stöd och hjälp i kritiska situationer. Följande moment skulle kunna vara fruktbara:

- definiera strategi och taktik för bemötande av informationsoperationer,
- genomföra systemnära analyser (bedöm risk, hot och sårbarhet),
- forma nätverk för stöd och samverkan,
- genomföra utbildning med relevanta spel eller simuleringar,
- öva,
- testa penetrationssårbarhet (göra avtalade försök att bluffa eller göra intrång),
- fördjupa och utreda konkreta frågeställningar,
- inrikta och följa forskning (exempelvis rörande förvarning, indikatorer och andra metodfrågor),
- bedriva någon form av lägesuppföljning och omvärldsanalys.

Referenser

Litteratur

Bell, J.B. & B. Whaley (1991): "Cheating and Deception". Transaction Publishers.

Clavell, J. (1983 ed): "The Art of War" från Sun Tzu.

Drucker, P. (1995): "Managing in a Time of Great Change". Butterworth & Heineman.

Furustig, H. & G. Sjöstedt (2000): "Strategisk omvärldsanalys". Studentlitteratur.

Grimvall, G., P. Jacobsson & T. Thedéen (2003): "Risker i tekniska system". Studentlitteratur.

Häggman, B. (1990): "Desinformation". Contra.

Jaubert, A. (1986): "Making People Disappear". An Amazing Cronicle of Photographic Deception". Pergamon Brassey's.

Libicki, M. (1995): "What is Information Warfare?" National Defense University.

Pincher, C. (1985): "The Secret Offensive". Sidgwick & Jackson.

Schwartau, W. (1994): "Information Warfare". Thunder's Mouth Press.

Sun Tzu: "The Art of War" bearbetad av Clavell.

Svensson, T. (1992): "Företagens skydd och säkerhet". Industriförbundet.

Taylor, A.J.P. (1967): "Världskriget 1914-1918". Prisma.

Windahl, S. & D. McQuail (1978): "Kommunikationsmodeller". Studentlitteratur.

Rapporter med mera

Alling-Ode, B. & E. Tubin (1993): "Falska kort?" SPF rapport nr 161.

Bergström, M. (2004): "Informationsoperationer mot näringslivet – hot mot nationell säkerhet" FHS.

Friman, H., G. Sjöstedt & M.W. Wik (1996 eds): "Informationskrig. Några perspektiv". UI Conference Papers 18.

Furustig, H., B. Ljunggren & W. Unge (2001a): "Skydd mot strategisk vilseledning. Del 1. Definitioner, metoder, diskussioner". FOI-R-0294-SE.

Furustig, H., B. Ljunggren & W. Unge (2001b): "Skydd mot strategisk vilseledning. Del 2. Kommenterade referenser, fallstudier och bevakningslista". FOI-R-0296-SE.

Furustig, H. (1996a): "Militär vilseledning. Några grunder". FOA rapport FOA-R-96-00365-SE.

Furustig, H. (1996b): "Informationsbaserad krigföring. Teknik med människan i centrum". Från UI Conference Papers 18 med H. Friman, G. Sjöstedt & M.W. Wik (eds).

Furustig, H. (1995): "Vilseledning mot företag". FOA rapport FOA-R-001130-5-SE.

Furustig, H. (1982): "Debatt och försvarsdebatt". FOA C-rapport 56036-H2.

Furustig, H. (1981): "Etik och teknik i informationens värld". FOA D-rapport 56003-H9.

Hanses, Y. & R. Hellström (1990): "Moln över Kola". SPF meddelande nr 126.

Johansson, A. & C. Karlsson (1997): "Ny tid. Ny krigskonst. Klarar vårt psyke framtidens informationsattack?" Försvar i Nutid, nr 3.

Leth, G. & T. Thurén (2000): "Källkritik för Internet". SPF rapport nr 177.

Nordlund, R. (1994): "Ett triangeldrama. Myndigheter, medborgare och medier i kris". SPF meddelande nr 136:a.

Nordlund, R. (1992 ed): "Svenskarna, medierna och Gulfkriget". SPF rapport nr 158-1.

Nydén, M. (1995): "Hotet från IT. Den informationstekniska utvecklingen". SPF meddelande nr 138.

Rolf, B. & H. Furustig (1984): "Att bedöma information". BN rapport nr 127.

Sjöstedt, G. & P. Stenström (2002): "Vilseledning på Internet". SPF rapport nr 183.

Sjöstedt, G. (1992): "Som en saga... lögnen som maktmedel". SPF rapport nr 159.

Sjöstedt, G. (1988): "Desinformation, vilseledning och nationell säkerhet". SPF rapport nr 148.

Stütz, G. & E. Tubin (1991): "Ett ryktes anatomi". SPF meddelande nr 132.

Tidningar

Dagens Industri 1994-03-24.

Dagens Nyheter 1997-02-26.

Nya Wermlands-Tidningen 2004-06-24.

Metro 2000-11-25.

Svenska Dagbladet 1998-02-28, 1999-01-28, 1999-02-08, 2004-05-08, 2004-05-07, 2004-06-13.

Tidskrifter

Bulletin of the Atomic Scientists, mars-april 2003.

International Defense Review, 1993, nr 5.

Ny Teknik: 1999 nr 9, 2003-11-05, 2004-09-29, 2004-10-06.

Radio och TV-program

SVT 2: Dokument utifrån 1992-03-28, Agenda 2004-05-16.

Internet

www.deloitte.com

www.dn.se, hämtat 2004-05-04.

http://abcnews.go.com/Business/print?id=89443.

www.krisberedskapsmyndigheten.se, hämtat 2004-05-15.

Nyhetsbrevet Delete, www.krisberedskapsmyndigheten.se

Övrigt

FM (1998): "Vilseledning". Broschyr. Beteckning 7741-716 001.

HKV (2003): Utkast till "Försvarsmaktens Grundsyn Informationsoperationer". Beteckning 01 600 : 78 657.

HKV (1997): "Vilseledning". PM. Beteckning 21 120: 73 579.

Säkerhetspolisen (2004): "Verksamhetsåret 2003".

Ordförklaringar

Ord som vid första användningen i texten markerats med asterisk (*) är upptagna i nedanstående ordförklaringar. Kommentarerna är inga formella definitioner utan avser endast att vara påminnelser om vad begreppen står för.

Ord/begrepp	Förklaring
Cracker	Avancerad datoranvändare som utan behörighet och genom olika former av intrång avsiktligt skadar andra datoranvändares data, program eller hårdvara. Intrång kan vara "beställda".
Denial of Service	Blockera sambandsmedel för utvalda offer avseende tele- och datorkommunikation.
Desinformation	Avsiktligt vilseledande information.
E-mail	Elektronisk post som förmedlas genom datornät.
EMP	Elektromagnetisk puls. Elektronik är störkänslig för EMP. Telemotmedel.
Hacker	Avancerad datoranvändare som utan behörighet genomför olika former av oskadliga men besvärande intrång i andras datorsystem.
HERF	(High Energy Radio Frequency) Radiofrekvent strålning med högt energiinnehåll kan skada elektronik. Telemotmedel.
Hot	Möjlig händelse med negativa konsekvenser.
Hotbild	Samlad bild av de hot som föreligger mot något (någon).
HPM	(High-Power Microwave) Elektromagnetiskt strålvapen med pulsad mikrovågsstrålning med hög effekt. Telemotmedel.
Information	Den meningsfulla innebörden i ett meddelande eller budskap.
Informationsoperationer	Samordnad verksamhet i syfte att påverka motståndares eller andra aktörers beslut till egen fördel eller till motståndarens nackdel.
Infrastruktur	Basen för en verksamhet, till exempel elkraftnät, järnvägsnät och telekommunikationer.
IT	Informationsteknologi eller informationsteknik.
Mask	Fientlig kod som sprids genom elektronisk post över Internet eller Intranet eller genom svagheter i operativsystem och som skapats för att dolt sprida någon information genom ovetande datoranvändare.
Perceptionsstyrning	Planerad verksamhet för att genom information påverka en målgrupps verklighetsbild (= perception management).
Psykologiska operationer	Planerad verksamhet för att genom *information* påverka en målgrupps värderingar, attityder och handlande.
Risk	Sammanvägning av sannolikheten för skada och dess konsekvens. Alternativt: Sannolikheten för en skadlig händelse.
RÖS	Röjande signaler. Tekniska kommunikationsmedel, datorer och tangentbord ger upphov till signaler som kan avlyssnas/registreras.
Spyware	Olika hjälpprogram som används för att upptäcka svagheter i datasystem eller utföra kodknäckning, dataintrång och informationsinsamling, eventuellt utan mottagarens vetskap.
Sårbarhet	Svaghet i en funktion, ett system eller en verksamhet. Grad av oförmåga att motstå ett hot.
Säkerhetslucka	Sårbarhet i ett datorsystems programvara.
Trojan	Fientlig kod som dolt sprids i programfiler. "Trojanska hästar" kan utföra skadliga uppdrag på smittade datorer.
Vilseledning	Avsiktligt missvisande påverkan (inkluderar förutom desinformation även handlingar, exempelvis skenåtgärder, finter, maskerande åtgärder, m m). Överordnat begrepp.
Virus	Fientlig kod i dataprogram som sprider sig mellan program eller dokument och som ofta skapas för att störa eller skada mottagarens datasystem.

Mediers sårbarhet

En studie om konsten att mäta mediers förmåga att möta påfrestningar

Bertil Flodin

Anders Sahlstrand

Innehållsförteckning

Inledning

Benjamin Vanderford, San Francisco, ville se om det gick att lura nyhetsmedierna. I ett garage spelade han in en video som utgav sig för att visa avrättningen av amerikansk gisslan i Irak. Med hjälp av högläsning ur koranen, en vän som höll i kniven och rödfärg lyckades han lura nyhetsbyråer och ansedda medier att under flera timmar förmedla den fejkade nyheten (*Dagens Nyheter* 2004-08-08).

Det inträffade kan möjligen beskrivas som ett smaklöst och harmlöst skämt, men det pekar på någonting centralt och problematiskt: nämligen hur medier skall kunna genomskåda avsiktliga försök att utnyttja medierna till att förmedla en verklighetsbild som gynnar avsändaren.

Medierna spelar en synnerligen viktig roll i vårt samhälle. De bevakar och beskriver, analyserar och kritiserar, lyfter fram och tonar ned olika skeenden i samhället. De är ständigt utsatta för försök till påverkan. De är djupt involverade i varje kris och människors kunskaper om vad som sker i samhället kommer till stor del via mediernas beskrivningar.

En av mediernas uppgifter är att beskriva och analysera hur olika aktörer sköter och skött sig under olika former av påfrestningar. Var myndigheten väl förberedd? Tog företaget sitt ansvar? Lyckades polis, räddningstjänst och sjukvård koordinera sina ansträngningar? Kunde myndigheten motstå försök till korrumpering? Hur kunde en anställd under så lång tid lura sin arbetsgivare? Varför agerade inte politikerna tidigare?

Bakom många av frågorna ligger antagandet att olika aktörer måste vara förberedda på att hantera olika slag av påfrestningar, allt ifrån elavbrott till avsiktliga försök att t ex manipulera börsens värdering av företag. Medierna har här en helt central uppgift att fortlöpande bevaka skeenden, beskriva dem och påtala försök till manipulering och egennyttigt agerande som i någon mening skadar vårt samhälle.

För att medierna skall kunna fullfölja denna viktiga uppgift krävs att de själva är rustade att stå emot olika påfrestningar. Om inte de lyckas genomskåda falska budskap och vinklade nyheter, om inte de har en robusthet i sin organisation som fungerar under svåra påfrestningar, och om inte de lyckas fortsätta sitt arbete när krisen drabbar dem själva, så är inte bara medierna illa ute utan det är stor risk för att även samhället lider svår skada. Det finns därför all anledning att studera mediernas sårbarhet.

Syfte

Styrelsen för psykologiskt försvar (SPF) har bl a uppgiften att i samråd med medieföretagen medverka till att dessa har en sådan medvetenhet och robusthet, att verksamheten kan fortgå vid svåra påfrestningar på samhället i fred.

SPF har startat projektet ”Informationsoperationer och mediers sårbarhet”. Projektet ska försöka identifiera vilka nyckelegenskaper hos medierna som skulle kunna

påverkas vid en svår påfrestning samt finna indikatorer som speglar nyckelegenskapernas tillstånd. Vårt avsnitt ingår i detta projekt.

Syftet med den här studien är att problematisera svenska mediers förmåga att tåla svåra påfrestningar och avsiktliga försök till omfattande påverkan av dem, samt att peka på möjliga vägar att bestämma nyckelegenskaper hos medierna och att finna lämpliga indikatorer på dessa egenskaper.

Vi är framför allt intresserade av att belysa försök och skeenden som påverkar mediernas verklighetsuppfattning, mediernas arbetssätt och mediernas möjligheter att förmedla sina intryck.

Starkt förenklat kan vårt arbete beskrivas som ett försök att studera vilka förutsättningarna är att medierna förvandlas till en omedveten kanal som enbart förmedlar och inte förädlar den verklighetsbild och analyserar de försök till påverkan som medierna utsätts för.

Vår grundsyn är att genom att göra en bred problematisering så skapas förutsättningar för medierna att möta alla typer av påfrestningar, alltifrån snöstormar till iscensatta informationsoperationer. Studien skall med andra ord medverka till mediernas rapporteringssäkerhet.

Att studera mediers sårbarhet

I vår studie ser vi på medierna som en särskild organisationsform som interagerar med en mängd aktörer inom en viss given samhällelig kontext. Denis McQuail har föreslagit en modell där fyra olika kraftfält riktas mot medierna (McQuail 2002):

- Alla de händelser och all den information som medierna exponeras för.
- De ekonomiska intressen som påverkar verksamheten, till exempel konkurrenter, annonser, ägare och fackföreningar.
- Gällande lagstiftning och olika former av politisk kontroll och stöd.
- Den kraft som riktas mot medierna genom dem som konsumerar mediernas utbud.

Mediernas sårbarhet är i detta sammanhang ett uttryck för hur mycket och hur allvarligt medierna påverkas av en händelse. Graden av sårbarhet bestäms av förmågan att förutse, hantera, motstå och återhämta sig från händelsen (Krisberedskapsmyndigheten 2003). Vi utgår ifrån att alla medier strävar efter låg sårbarhet. En låg sårbarhet är, enligt oss, lika med en hög rapporteringssäkerhet, det vill säga medierna förmår fullgöra sina uppgifter trots svåra påfrestningar.

Speciellt intressant blir det att relatera mediernas sårbarhet till så kallade informationsoperationer (IO). Detta är samordnade och tidskoordinerade verksamheter med syfte att påverka verklighetsbild, beslut och handling hos utvalda mottagare på ett sätt som gynnar den initierande angriparen. Målobjekten kan vara opinioner eller beslutsfattare (se Furustig i denna skrift). På vilket sätt kan medierna gardera

sig mot denna typ av påverkan? Vilka dimensioner är relevanta att studera för att kunna konstatera om mediernas förmåga att motstå informationsoperationer ökat eller minskat?

Vi har även försökt väga in de starka förändringar som råder inom mediernas värld. Produktionen digitaliseras. Journalisterna har nya verktyg som tillåter dem att söka nyheter mer vidsträckt och snabbare än vad som hittills varit möjligt. De interna arbetsrutinerna präglas också av den nya tekniken.

Även distributionen har digitaliserats, inte minst genom Internet. Internet tillåter även nya former av samarbete och informationsförmedling. De gamla gränserna mellan traditionella medier och IT- och telesektorn tenderar att suddas ut.

Kraven på den enskilde journalisten har förändrats. Färre medarbetare ska göra mer, antalet specialreportrar med egna bevakningsområden minskar, den redaktionella styrningen ökar.

De medier som vi i första hand studerar är press, radio och TV. Vi väger även in den nyhetsförmedling som sker via Internet. Denna tar sig ett otal former, men vi avgränsar oss till att studera nyhetsförmedling via nätet såsom den tillämpas av nyhetsbyråer och medier i Sverige.

MEDIERS SÅRBARHET UR OLIKA PERSPEKTIV

Vi har valt att inte låsa vår problematisering till ett särskilt perspektiv, utan tvärtom arbetat eklektiskt och hämtat inspiration och tankemodeller från ett flertal perspektiv: risk- och sårbarhetsanalyser, perceptionsstyrning, agenda setting, mediernas föreställningsramar, krishantering samt kommunikationsvetenskap.

RISK– OCH SÅRBARHETSANALYS

Sverige har antagit ett nytt system för analys och bevakning av risker och sårbarhet inom det svenska samhället. Ett viktigt led i detta arbete är att varje statlig myndighet årligen skall lämna in en risk- och sårbarhetsanalys till Regeringskansliet.

Enligt Krisberedskapsmyndighetens synsätt bör en sådan analys omfatta följande steg (Krisberedskapsmyndigheten 2003):

- Vad kan hända?
- Varför kan det inträffa och hur ofta?
- Vilka blir konsekvenserna för samhället?
- Vad kan förebyggas?
- Hur kan sårbarheten minska?
- Sammanställning av resultaten.

Att systematiskt analysera sin sårbarhet och riskerna för verksamheten kan ha fördelar för en organisation. Det skärper förståelsen och krismedvetenheten och det underlättar för organisationen att förutse och tidigt upptäcka oroande händelser samt att ha en beredskap för att hantera svåra påfrestningar. Vi använder oss av

detta perspektiv i första hand för att diskutera mediernas krismedvetenhet och planläggning av sin beredskap.

PERCEPTIONSSTYRNING

Vad vi än gör och hur vi än gör det så gör vi intryck på vår omvärld. Detta gäller för varje individ, för grupper, föreningar, organisationer och företag. Att vårt agerande gör intryck på omvärlden är vi ofta omedvetna om. Många organisationer väljer dock att på ett mycket medvetet sätt försöka styra hur omvärlden uppfattar organisationen, det vill säga man använder sig av så kallad perceptionsstyrning (*perception management*).

Detta perspektiv är synnerligen användbart i vår studie. Det har relevans såväl när vi betraktar olika aktörers försök att påverka medierna, som när vi ser hur medierna väljer nyheter och förmedlar dem vidare till sin publik.

Aktörerna kan försöka styra mediernas upplevelse av en situation på ett antal sätt: vem man väljer att föra ut en viss information till, när man väljer att göra det, i vilken miljö informationen presenteras. Försöken att formulera problem och att sätta en viss agenda är så vanligt förekommande att journalister rent rutinmässigt bedömer varje sådan situation som han eller hon hamnar i.

Men vid urvalet av vilka händelser, aktörer och situationer som skall bevakas gör även medierna val och den bild av verkligheten som medierna sedan återger till sin publik blir därmed också en form av perceptionsstyrning. I augusti 2004 var det till exempel ett sådant kompakt utbud av sändningar från de Olympiska spelen i Aten att man lätt kunde få för sig att medierna ansåg att tillvaron i huvudsak bestod av dessa spel.

Men även den enskilde individen, mediekonsumenten, ägnar sig åt perceptionsstyrning. Av allt som han/hon upplever och gör under en dag är det bara vissa fenomen som lyfts fram, vissa åsikter som framförs och vissa aktiviteter som äger rum.

Perspektivet med perceptionsstyrning har vi tillämpat genomgående i studien. Det hjälper oss att beskriva försök till styrning och påverkan av medierna, men även att analysera mediernas egen förmåga att hantera och återskapa verkligheten.

AGENDA-SETTING

Att sätta agendan innebär att flera förespråkare för olika områden konkurrerar om mediernas och allmänhetens uppmärksamhet. Eftersom utrymmet i medierna är starkt begränsat innebär processen ofta att ett problem får minskad uppmärksamhet på bekostnad av ett annat (Dearing & Rogers 1996). Teorierna om agenda-setting omfattar såväl en *public agenda*, som en *media agenda* och en *policy agenda*.

Medierna har en nyckelroll i och med att de genom att uppmärksamma ett problemområde fäster allmänhetens och politikernas uppmärksamhet på detta område. Forskningen har visat att mediernas bevakning av ett område har ett samband med hur viktigt allmänheten uppfattar detta område. Ju mer framskjuten placering

en händelse har i medierna, desto viktigare bedömer allmänheten att den är (Dearing & Rogers 1996).

Vi använder oss av forskningen om agenda-setting för att bedöma förutsättningarna för en aktör att formulera ett problemområde eller en åsikt så att den accepteras av medierna och därmed potentiellt sett kan påverka mediernas publik att uppmärksamma problemområdet eller åsikten.

MEDIERS FÖRESTÄLLNINGSRAMAR

En viktig aspekt att uppmärksamma när man studerar mediers sårbarhet är rimligtvis de föreställningar medierna har om vad som är värt att ta upp och hur det ska behandlas. Det finns etablerade schabloner inom medierna såväl för olika genrer som för värdering av nyheter (McQuail 2002). Forskningsfältet är mycket rikt. Vi har valt att utgå från Bengt Johanssons tolkning och utveckling av Shoemakers, Changs och Brendlingers tre grunddimensioner (Johansson 2004):

- Nyheter handlar om olika former av avvikelser.
- Nyheter rör saker som är socialt betydelsefulla händelser och skeenden.
- Nyheter rör sådant som är nytt och nära.

Medierna har generellt sett många ramar, tankemönster, schabloner och stereotyper som effektiviserar produktion och som underlättar för publiken att tolka mediernas utbud. Journalister har även generella strukturer för att bedöma det material som man väljer att uppmärksamma. McQuail har sammanfattat forskningen om vilka faktorer det är som styr mediernas urval av nyheter (McQuail 2002):

- Makt och berömmelse hos individer som är inblandade i händelsen.
- Reporterns personliga kontakter.
- Var händelsen äger rum.
- Var maktcentrum finns.
- Grad av förutsägelse och rutin.
- Närheten till publiken hos dem som porträtteras i medierna.
- Händelsens aktualitet och timing.
- Timing till nyhetscykeln.

Framväxten av Internet har tillfört nya dimensioner till det journalistiska arbetet. Det har både förändrat de journalistiska arbetsrutinerna och medfört nya källkritiska problem. Information som presenteras på Internet bjuder på särskilda problem och möjligheter. Leth och Thurén har analyserat Internet ur ett källkritiskt perspektiv och ger följande praktiska rekommendationer för journalister och andra som vill använda sig av Internet som källa (Leth & Thurén 2000):

• Var noga i valet av hjälpmedel för sökningen.
• Identifiera den nätplats du har valt ut.
• Ta reda på när nätplatsen är uppdaterad.
• Ta reda på i vad mån nätplatsen är tendentiös.
• Fundera över hur trovärdig den som står bakom en nätplats är.

Aktörer som önskar påverka mediernas innehåll måste beakta såväl vilka kriterier som styr nyhetsvärderingen som de källkritiska aspekter som styr journalisternas arbete. Det gäller att presentera sitt material eller sin aktivitet på ett sådant sätt att den fångar mediernas uppmärksamhet och har sådana kvaliteter att de passar in i mediernas sätt att beskriva verkligheten. Journalisterna måste även göra en bedömning av om nyheten har en sådan attraktionskraft hos publiken att den förtjänar uppmärksamhet. Vi använder oss av forskning om mediernas föreställningsramar för att fånga upp de viktiga interna processer som lägger grunden till nyhetsbevakningen och därmed också grunden till att avslöja försök till manipulation och bedrägligt förfarande (Sahlstrand 2000).

KRISHANTERING

Kriser har så gott som alltid högt nyhetsvärde och ägnas en betydande uppmärksamhet från mediernas sida. SPF har genom åren publicerat en rad studier som dokumenterat mediernas förmåga att följa, beskriva och kritisera katastrofer, humanitära kriser och extrema händelser (se till exempel Martinsson & Säljö 1996, Dahlgren, Carlsson & Uhlin 1998 samt Granström 2002).

Mot bakgrund av andras och egna erfarenheter anser vi att mediernas insatser vid kriser något hårddraget kan beskrivas på följande sätt:

• Medierna är ovärderliga som nyhetsförmedlare vid kriser.
• Medierna är ofta först på plats.
• Medierna publicerar nyheter oavbrutet.
• Mediernas granskande funktion ersätts av öppna dörrens princip.
• Medierna når inte alla.
• Medierna vill vara så nära olycksplatsen som möjligt.
• Medierna vill intervjua offer och anhöriga.
• Medierna beskriver och granskar.
• Medierna vänder sig till auktoriteter.
• Medierna har svårt att vara professionella.
• Medierna använder i hög grad Internet som källa.

Den forskning som bedrivits har oftast varit inriktad på hur medierna följer och bevakar en kris i samhället (Jarlbro 2004). Däremot är det mycket ovanligt att forskningen studerat vad som händer när medierna själva hamnar i krisens centrum, antingen det beror på att samhällskrisen också påverkar medierna, till exempel vid elavbrott, eller att medierna själva äger krisen, till exempel vid fejkade nyhetssändningar eller bristande källkritik.

Forskningen om krishantering ger oss värdefulla insikter om hur medierna agerar vid svåra påfrestningar, men vid en studie om mediernas sårbarhet är det viktigt att detta inte får bli det enda perspektivet. Hur sårbara medierna är beror också på i vilken utsträckning medierna lyckas motstå de försök till påverkan som riktas mot dem under vardagliga förhållanden.

KOMMUNIKATIONSVETENSKAP

Vår studie är förankrad i en kommunikationsvetenskaplig referensram. Detta ger oss till exempel möjlighet att studera sändarnas trovärdighet men också att reflektera över de budskapsstrategier som olika aktörer använder sig av. Mediernas roll i kommunikationsprocesser i samhället har studerats intensivt. Speciellt intressant i detta sammanhang är i vilken mån som en aktör kan få medierna att enbart fungera som en förmedlare av information, det vill säga vara en kanal (Sahlstrand 2000).

Vi är också intresserade av situationer där informationsflödet får sådana proportioner att en ordinarie nyhetsbevakning inte längre är möjlig. Mediernas kunskaper om hur deras läsare, tittar och lyssnare agerar under olika situationer och på olika former av budskap har också relevans (Flodin 1999).

Tillvägagångssätt och avgränsningar

Denna studie baserar sig huvudsakligen på litteraturstudier, kompletterat med förutsättningslösa intervjuer med journalister och andra personer med god insyn i det journalistiska arbetet.

Vid litteraturinventeringen har vi utgått från vår förförståelse av problemområdet, vidsträckta litteratursökningar i publika databaser och sökningar via Internet.

Vår generella bedömning är att medan forskningen om medier är oerhört omfångsrik, så är forskningen om mediernas sårbarhet, beredskap och rapporteringssäkerhet inte särskilt omfattande.

Vid vår sökning har vi varit upptagna av att hitta infallsvinklar och dimensioner med relevans för analys av mediernas sårbarhet. Studien är således i allt väsentligt explorativ till sin karaktär.

Vi har även anlagt ett pragmatiskt angreppssätt så till vida att vi försöker finna dimensioner och ansatser som både har relevans och är möjliga att beskriva i termer av egenskaper och indikatorer på dessa egenskaper.

Studien gäller journalistiskt arbete under normala förhållanden och svåra påfrestningar. Det innebär att vi tagit del av studier som granskar svenska mediers bevakning av krig i utlandet (till exempel Nohrstedt, Höijer & Ottosen 2002, Nordström 2002). Vi har också tagit del av rapporter som behandlar terroristattacker mot USA (till exempel Nord & Strömbäck 2002).

Vi har avgränsat vår studie till att gälla rapporter som berör det redaktionella materialet. Det innebär inte att det skulle vara ointressant att studera till exempel annonser i dagspressen. Inför utdelningen av nobelprisen 2003 bedrevs det till exempel en omfattande kampanj med helsidesannonser av en amerikansk forskare som ansåg sig blivit förbigången vid utdelningen av nobelpriset i medicin.

Disposition

Vi har i denna inledning beskrivit bakgrunden till studien, syftet med den samt vilka perspektiv som styr vårt arbete och hur vi gått till väga. I nästa avsnitt lyfter vi upp till diskussion ett antal dimensioner som vi anser påverkar mediernas sårbarhet. Studien avslutas med att vi pekar på möjligheter att konkretisera dessa dimensioner i termer av nyckelegenskaper, vilka i sin tur bör kunna mätas empiriskt.

Problematisering

Fyra områden om mediers sårbarhet

Vi har valt att dela in frågor om mediernas sårbarhet i fyra övergripande områden: Mediernas krismedvetenhet och trovärdighet, Fånga in – förädla – förmedla, Organisation och psykosocialt omhändertagande samt Teknik och säkerhet.

Medierna är beroende av en hög trovärdighet för att deras verksamhet skall accepteras och deras budskap ha hög legitimitet. Att omvärlden accepterar medierna och deras verksamhet räcker dock inte, utan personalen inom medierna måste dessutom ha en hög krismedvetenhet, det vill säga vara inställda på att den vardagliga rutinen kan brytas och att olika försök till manipulation av mediernas verksamhet kan äga rum.

Mediernas arbetsprocess delar vi in i tre skeden: fånga in, förädla och förmedla. Inom vart och ett av dessa områden finns möjligheter att påverka och störa det journalistiska arbetet. Men det är inte bara den enskilde journalistens arbete som påverkar utfallet utan även den organisatoriska strukturen och hur väl medierna har förutsett kraven på ett psykosocialt omhändertagande av den egna personalen vid svåra påfrestningar. Att den egna säkerheten är tillfredsställande och att de tekniska förutsättningarna är tillfredsställande är en grund som hela produktionsprocessen vilar på.

MEDIERS KRISMEDVETENHET OCH TROVÄRDIGHET

Här är vi intresserade av att fånga i vilken utsträckning som medierna är medvetna om möjligheten att själva hamna i en kritisk situation. Vi använder här krisbegreppet i en mer vidsträckt bemärkelse än vad som vanligen är fallet. Kriser handlar här inte bara om de situationer som brukar kännetecknas av följande:

- Situation som uppstår hastigt, oväntat och utan förvarning.
- Situationer som kräver brådskande beslut och samverkan.
- Situationer som allvarligt påverkar mediernas funktionsförmåga eller tillgång på nödvändiga resurser.
- Förmågan att hantera mycket allvarliga situationer inom mediernas arbetsområde.

Beskrivningen ovan är en lätt modifiering av den definition som Krisberedskapsmyndigheten använder i sin skrift om risk- och sårbarhetsanalyser för statliga myndigheter (Krisberedskapsmyndigheten 2003).

Vi räknar även in möjligheten att medierna kan utsättas för en informationsoperation eller annat försök till påverkan utan att övriga kännetecken på en kris är vid handen.

En särskilt aspekt av mediernas sårbarhet är om mottagarna inte accepterar de utsagor som medierna förmedlar. Om mediernas trovärdighet ifrågasätts elimineras helt eller delvis deras möjligheter att utföra de uppdrag som de själva påtagit sig

och som medborgarna i det svenska samhället förväntar sig (Petersson & Carlberg 1990). Vi har därför valt att även lyfta fram trovärdighetsaspekten som en viktig dimension i mediernas sårbarhet.

FÅNGA IN – FÖRÄDLA – FÖRMEDLA

Om man ser mediernas verksamhet som en produktionsprocess är det vanligt att dela in den i tre funktioner: insamlande, bearbetande och distributiv. Vi har valt att använda tre parallella begrepp: fånga in, förädla och förmedla. I ”fånga in” vill vi både få med journalisternas egna aktiva sökande och att man exponeras för och uppmärksammar ett fenomen till följd av andra krafters initiativ.

Begreppet ”förädling” betecknar alla de typer av bearbetningar som förekommer inom det journalistiska, bild- och ljudmässiga samt redigeringstekniska arbetet.

Förmedling står för den process där mediernas produkter distribueras till sin publik, antingen det är en tidning på Internet, en lokaltidning eller ett rikstäckande TV-program.

Inom ramen för denna treställighet tänker vi också diskutera mediernas möjligheter att kontrollera sitt innehåll under olika förhållanden och i ljuset av de förändringar som ägt rum de senaste åren.

ORGANISATION OCH PSYKOSOCIALT OMHÄNDERTAGANDE

Den journalistiska arbetsprocessen är beroende av en rad andra funktioner inom medieföretaget. Den journalistiska insatsen kan till exempel tillintetgöras om tryckeripersonal går i strejk, eller inslag försenas till följd av felaktiga interna rutiner och oklara befogenheter.

Sett ur ett sårbarhetsperspektiv finns det anledning att studera planläggning, personalplanering och andra organisatoriska inslag som kan hjälpa eller stjälpa.

Händelser vid den tragiska branden på Hisingen i Göteborg 1998 visade på betydelsen av att medieorganisationen inser att även den egna personalen måste ha tillgång till en god psykosocial miljö (SOU 1999:68). Sårbarheten berör såväl människor som organisationer, men även teknik och säkerhet måste beaktas.

TEKNIK OCH SÄKERHET

Vi blir fortlöpande uppmärksammade på att medierna till stora delar är beroende av att teknik och säkerhet fungerar. När medierna inte lyckats sända eller trycka eller publicera på nätet har det ofta ett tekniskt fel som orsak. Teknik och säkerhet är förstås sedan länge föremål för myndigheters och företags uppmärksamhet. I sin analys av samhällets informationssäkerhet skriver Krisberedskapsmyndigheten följande:

> *På samhällsnivå tenderar sårbarheterna att öka till följd av att ömsesidiga beroendeförhållanden mellan infrastrukturer blir mer komplexa. Samhällskritiska infrastrukturer förlitar sig allt mer på ett fungerande IT-stöd och dessa infrastrukturer växer allt mer samman… Detta syns tydligast inom IT-området, då IT-system*

krävs för att styra elsystemen, vilka i sin tur är beroende av telesystemen, vilka i sin tur är beroende av elkraft. Eftersom både el- och teleinfrastrukturerna är bärare av IT-kommunikation kan denna komplexitet bidra till att om det ena systemet faller påverkas även det andra. (Krisberedskapsmyndigheten, 2004, s.12)

Medieföretagen är synnerligen beroende av att såväl el som tele- och IT-teknik fungerar. Det här är ett eget problemområde, för omfattande att behandlas inom ramen för vår studie. Frågorna uppmärksammas dock kontinuerligt inom många medieföretag och belyses också inom ramen för SPFs medieråd. Rådets verksamhet syftar till att för den privata och offentliga sektorn skapa en gemensam syn på behovet av säkerhet, beredskap, krishanteringsförmåga och samverkan inom mediebranschen (www.psycdef.se/media).

Vår uppmärksamhet skall istället riktas mot de problemområden som redovisats ovan och vi börjar med att granska mediernas krismedvetenhet.

Mediers krismedvetenhet

Tisdagen den 27 april 2004 blev det plötsligt svart i TV-rutan. Sändningsavbrottet varade i 40 minuter. Vi fick sitta och vänta på att få en förklaring. Felet visade sig vara att en överkoppling från en modersynkgenerator till andra backupsystem inte fungerade. Felet orsakade detta anmärkningsvärt långa sändningsuppehåll i SVTs båda marksända kanaler, ettan och tvåan, samt den digitala SVT 24.

En talesman för Sveriges Television sa efteråt att man relativt snabbt konstaterat vad som orsakat felet, att man insett att det skulle ta en halvtimma att reparera och att man därför inte dragit igång reservkapaciteten.

Det här är enligt vår mening en indikator på en låg krismedvetenhet. I den värld vi lever i idag, förväntar vi oss att medierna finns tillgängliga dygnet runt, året runt. En halvtimmas sändningsavbrott skapar onödig oro och osäkerhet och sänker mediernas trovärdighet.

Vad är en god krismedvetenhet? Varför behövs den? Hur manifesterar den sig? Med krismedvetenhet menar vi att mediernas representanter är medvetna om att olika händelser och aktörer kan försvåra, manipulera och förstöra mediernas möjligheter att fullfölja sitt uppdrag, det vill säga medierna inser sin egen sårbarhet och har vidtagit åtgärder för att minimera negativa konsekvenser av extern och intern påverkan.

Ett första kriterium är förstås att medieföretaget är medvetet om sin egen sårbarhet. Denna medvetenhet ska idealt sett omfatta alla anställda, ja även tillfälligt anställda och praktikanter. Detta är hos många organisationer ett försummat kapitel, vardagen tränger sig på och att skapa en hög medvetenhet om en situation som förefaller osannolik har visat sig vara krävande och svårt att genomföra.

Medieföretaget bör ha analyserat sin egen situation, till exempel i form av en risk- och sårbarhetsanalys. Den bör i så fall vara så pass vidsträckt att den fångar upp de speciella former av sårbarhet som kännetecknar medieföretag. Det gäller

inte minst att kunna förutse alla typer av försök till påverkan från externa aktörer. En mycket utförlig och innehållsrik beskrivning av tänkbara försök till påverkan ges av Furustig i denna skrift.

Det bör vidare finnas en insikt om hur det egna agerandet kan komma att uppfattas av omgivningen. Medieföretag är liksom andra organisationer beroende av att agera utifrån en hög trovärdighet. Att en journalist samtidigt med sin journalistiska gärning som politisk kommentator även gjorde kontinuerliga intervjuer med landets statsminister, mot löfte att innehållet inte skulle offentliggöras omedelbart, gav upphov till en livlig debatt där en av infallsvinklarna var just risken för bristande trovärdighet.

Det kan tyckas paradoxalt att samtidigt som svenska befolkningen är storkonsumenter av det medieutbud som finns, så är den generella trovärdigheten för det journalistiska arbetet anmärkningsvärt låg. Detta har visats under en följd av år i SOM-institutets rapporter (se till exempel Holmberg & Weibull 2004).

En god krismedvetenhet innefattar även att medieföretagen skall ha vidtagit mått och steg för att säkerställa en god beredskap mot olika typer av påfrestningar, såväl under normala förhållanden som under kriser. Det innebär dels att man har en aktuell plan för krishantering i vid bemärkelse, dels att denna plan testas regelbundet via olika former av övningar och kontroller.

Det svenska medielandskapet är idag mycket varierande och arbetar under olika förutsättningar. Kommersiella radiostationer som huvudsakligen spelar musik gör sannolikt andra bedömningar om kraven på god krismedvetenhet och beredskap än Sverige Television. Möjligheten att avsätta resurser för krisberedskap varierar säkerligen avsevärt mellan olika medieföretag.

Mediers trovärdighet

Det finns en rad studier som pekar på vilken betydelse medierna har för att hålla allmänheten och grupper inom allmänheten uppdaterade om vad som händer och sker i världen. En av studierna visar att det inte bara är allmänheten utan även politiker och journalister som hämtar sin kunskap från mediernas värld (Nord & Strömbäck 2004).

För såväl samhället som för enskilda medier är det därför av största vikt att medierna har en hög trovärdighet. En låg trovärdighet kan leda till misstro mot budskap som förmedlas via medierna, ökad ryktesspridning, att desinformation bildar underlag för beslut, att allmänheten slutar ta del av nyhetssändningar med mera.

Vad är det då som leder till hög trovärdighet? En faktor som ofta framhålls är mediernas sakkunskap och kompetens inom det område som behandlas. Dessutom framhålls ofta betydelsen av att medierna är objektiva, att de inte är ute efter att manipulera eller att presentera en verklighetsbild som inte är rättvis och ärlig (se Elliot 1997 och Renn, i Warg 2000).

Denna verklighetsförfalskning skulle dels kunna vara en följd av motiv inom medievärlden, men också en följd av externa aktörers försök till avsiktlig vilseledning. Medierna måste således ha sin uppmärksamhet riktad åt två håll: dels att det

egna arbetet bedrivs på ett kompetent och objektivt sätt, dels att genomlysa och analysera externa aktörers aktioner, påståenden och bedömningar.

Det finns en omfattande svensk forskning om allmänhetens förtroende för medier i Sverige. Mätningarna sker ofta på en aggregerad nivå, som mätning av förtroendet för medierna jämfört med andra samhällsinstitutioner (Holmberg & Weibull 2004). Särskilda studier görs även av förtroendet för olika mediers innehåll (Weibull 2004).

Däremot förefaller det vara ont om studier som försöker att *mäta kontinuerligt* i vilken utsträckning som medierna förmår att upprätthålla sin granskande funktion och inte bli manipulerade att helt eller delvis förmedla veklighetsbilder som snedvridits av externa aktörer med egna intressen. De studier som ägnar sig åt liknande frågeställningar har oftast karaktären av fallstudier (se till exempel Nohrstedt, Höijer & Ottosen 2002, Riegert 2002).

Det är också ont om studier som redovisar medieföretagens egna värderingar av sin trovärdighet, samt hur de definierar och mäter densamma.

Mediers förmåga att fånga upp information

Mediernas förmåga att fånga upp information sker inom ramen för de två mer generella faktorer som vi behandlat ovan. Mediernas krismedvetenhet är en faktor som uppmärksammar i vilken utsträckning det finns en medvetenhet om sårbarheten i den egna medieorganisationen. Mediernas trovärdighet handlar dels om i vilken utsträckning omvärlden har förtroende för medierna, dels om medieföretagen är medvetna om omvärldens syn. Nu har vi för avsikt att titta närmare på tre områden som i tur och ordning speglar den journalistiska arbetsprocessen, nämligen mediernas förmåga att fånga in information, att förädla den och att förmedla den. Förmågan att fånga in information kan betraktas utifrån tre frågeställningar:

- Vem väljer ut det som medierna exponeras för?
- Vad är det som gör att medierna uppmärksammar vissa händelser och aktörer?
- Vilka resurser har medierna att fånga in information?

Den första frågan vill lyfta fram det uppenbara, nämligen att det inte bara är medierna som bestämmer dagordningen. I samhället finns en rad aktörer som vill avvakta rätt tidpunkt för att göra rätt utspel, riktat mot viktiga medier i en särskild avsikt. En indikator på detta är att andelen informatörer under ett drygt decennium har tredubblats (Sveriges Informationsförening 2004). En annan indikator är den som journalister gärna ger uttryck för, nämligen att allt fler myndighets- och företagspersoner idag är väl medvetna om hur journalister arbetar och vilka nyhetsvärderingskriterier de tillämpar.

De aktiva försöken att förmå medierna att uppmärksamma en viss företeelse är sannolikt fler nu än någonsin tidigare. Och detta sker samtidigt som det är en tendens inom medievärlden att andelen reportrar inom journalistkåren minskar

samtidigt som reportrarna får ägna en större del av arbetstiden åt redigering och bearbetning av nyhetsmaterial (Nygren & Alström 2002).

En konsekvens av dessa tendenser är rimligtvis att en ökande andel av det som publiceras har tillkommit på initiativ av andra krafter än redaktionens. Det borde i sin tur innebära att risken för manipulation ökar. Fördelningen av innehåll som är initierat utifrån och inifrån borde därför vara en generell indikator på potentiell sårbarhet.

Ett exempel på aktörer som försöker utnyttja medierna för egna syften har beskrivits av Larsåke Larsson (Larsson 1998, s. 22). Enligt Larsson försöker politiker nå publicitet för att:

- Sprida information och påverka medborgare och grupper.
- Göra den egna politiska scenen ständigt synlig.
- Förhandla med utomstående intressen.
- Ge besked till den egna organisationen.
- Få upplysningar om vad som händer i samhället och även internt.
- Få en uppfattning om människors aktuella angelägenheter.

Svaret på frågan om vad det är som gör att medierna väljer att uppmärksamma vissa händelser och inte andra är, liksom flera andra av de frågor som rests tidigare, i sig ett eget forskningsområde. Vi har tidigare beskrivit ett antal kriterier för nyhetsvärdering (se avsnittet om mediernas föreställningsramar ovan). Här avser vi att lista några faktorer som mer anknyter till kommersiella och produktionsmässiga förhållanden:

- Hur väl nyheten passar in i produktionscykeln för respektive medium.
- Hur många andra händelser som inträffat samtidigt.
- Tillgången på journalister med relevant bakgrund.
- Om nyheten kan parallellpubliceras.
- Om nyheten är lättbearbetad i det redaktionella arbetsflödet.
- Ju mer resurser – i form av tid, personal och budget – det kostar att täcka en händelse, desto mindre troligt är det att det kommer att bli en nyhet av händelsen.
- Ju mer journalistiskt en källa har förberett en historia, desto troligare är det att det kommer att bli en nyhet.
- Ju mer selektivt en historia distribueras, gärna så att den kan presenters som journalistens eget arbete, desto troligare är det att det kommer att bli en nyhet.
- Ju mer ett mediums strategi bygger på att berätta om sensationer i något avseende, desto troligare är det att händelser av underhållande slag blir nyheter än att händelser som bygger på relevans, sanning och riktighet blir det.

De fyra sista punkterna är direkt citat från Sigurd Allerns teser om hur ekonomiska omständigheter påverkar arbetssätt och nyhetsurval (i Wadbring 2004).

Vi är därmed redan inne på att besvara den tredje frågan, nämligen vilka resurser som står till mediernas förfogande. Det finns flera bedömningar som pekar på att de som skall bevaka omvärlden för mediernas räkning, det vill säga journalisterna, har en mycket krävande arbetssituation: färre medarbetare skall göra mer, antalet specialreportrar med egna bevakningsområden och eget bevakningsansvar har bantats och tiden för förutsättningslöst arbete förefaller ha minskat.

Samtidigt finns det tekniska möjligheter att söka information som aldrig tidigare. Allt fler organisationer anstränger sig också för att informera via Internet på egna webb-platser, vilket möjliggör sökningar oberoende av tid och rum. Också möjligheterna att bearbeta och visualisera och presentera information har förbättrats väsentligt de senaste decennierna.

Vid akuta kriser i samhället tillkommer ytterligare påfrestningar på medierna. Klarar organisationen att rent fysiskt ta emot och sända all inkommande information? Klarar journalister och fotografer att fullgöra sina arbetsuppgifter under synnerligen påfrestande arbetsförhållande? (SOU 1999:68) Har redaktionen en personalplanering som tillåter att det journalistiska arbetet kan bedrivas på en hög professionell nivå även under en långdragen kris?

Ett tecken på mediers sårbarhet måste vara möjligheten och förmågan att samla in information. Det borde ha framgått av ovanstående presentation att detta är en oerhört komplex frågeställning som rymmer alltifrån tekniska och organisationsmässiga aspekter till kriterier för nyhetsvärdering och kapacitet att analysera olika aktörers avsikter och tillvägagångssätt.

Men att samla in information är bara det första steget i processen. Vi tar oss nu an nästa problem, att förädla informationen.

Att förädla information

Många av dem som agerar för att en viss händelse eller ett visst synsätt skall accepteras och förmedlas av medierna ser gärna att medierna enbart fungerar som kanal och helt enkelt släpper igenom den information som aktören önskar. Om vi studerar mediernas sårbarhet kan detta vara en infallsvinkel. Frågan blir alltså: under vilka förhållanden försvagas eller elimineras mediernas möjlighet att utföra ett traditionellt journalistiskt arbete?

HÄNDELSEN ÄR VÄL PAKETERAD

Om aktören är väl medveten om mediernas verklighetssyn och nyhetsvärdering i allmänhet och den specifike journalistens eller redaktionens värderingar i synnerhet ökar möjligheten att vinkla en händelse eller ett uttalande så att den eller det lättare uppmärksammas av medierna.

BRIST PÅ NYHETSMATERIAL

Tillfälligtvis kan det uppstå ett mindre tillflöde av nyheter än vanligt, till exempel under sommartid eller helger. Men tidningen måste fyllas, sändningarna måste

ske. Det finns en potentiell möjlighet att utnyttja detta förhållande till att presentera nyheter som accepteras i en bristsituation, men som inte skulle blivit publicerade under mer normala förhållanden.

ÖVERFLÖD AV NYHETSMATERIAL

Det motsatta förhållandet är kanske ännu mer lägligt för en aktör som önskar få in material utan alltför närgången journalistisk granskning. Vid stora kriser i samhället ökar informationsflödet mycket kraftigt och den *gate-keeping* funktion som normalt upprätthålls på en redaktion kan under det akuta skedet ersättas av *open-gates*, det vill säga mycket information släpps igenom utan granskning (Flodin 1980).

FÖRÄNDRADE JOURNALISTISKA ARBETSVILLKOR

Om nya villkor råder som innebär att färre skall producera mer, så ökar riskerna för att journalisterna tvingas ta genvägar i sitt arbete: man accepterar andra journalisters beskrivning av en händelse rakt av, man utgår från att en aktörs utspel är relevant och sakligt, man avstår från att kontrollera bakomliggande omständigheter.

I förlängningen av ett sådant arbetssätt finns även ett fåtal journalister som ägnar sig åt rent bedrägligt beteende. I USA skrev journalisten Jayson Blair de mest fantastiska artiklar om händelser runtom i världen som han bevakat för *New York Times* räkning. Det tog mycket lång tid innan redaktionen upptäckte att det hela var ett falsarium (*Dagens Nyheter* 2003-08-14).

OM SNABBHETSKRITERIET TAR ÖVERHAND

I förlängningen av en journalistisk ambition att snabbt förmedla nyheter, ligger ambitionen att vara först med en nyhet. Om denna ambition överskuggar källkritisk granskning ökar givetvis mediernas sårbarhet.

FÖRESTÄLLNINGAR OM PUBLIKEN

Medierna arbetar under föreställningar om vad läsare, tittare och lyssnare har för verklighetsuppfattning och vad de önskar bli informerade om. Ett sätt att öka mediernas sårbarhet är att påverka deras uppfattning om publiken. Om någon aktör till exempel lyckas övertyga medierna om att det är lätt att få allmänheten att råka i panik, så kan det styra nyhetsförmedlingen på ett icke önskvärt sätt.

Aktörer som önskar påverka medierna bör således ha en god föreställning om hur medier överväger publicering beroende på föreställningar om publikens behov och önskemål. Men även frågor om tillgänglighet sett ur mediernas synvinkel är intressant. Medieföretagen måste hela tiden ställa frågor om händelsen är fysiskt, tekniskt och journalistiskt lättillgänglig. Dessutom måste aktörerna känna till hur väl händelsen passar in i olika mediers nyhets- och produktionsförhållanden (Shoemaker 1991).

Att förmedla information

När informationen är insamlad, underlaget bearbetat och förädlat återstår förmedlingen. Den här delen av det journalistiska arbetet borde vara det minst problematiska sett ur ett sårbarhetsperspektiv.

Här är det i allmänhet medierna som avgör vad som skall spridas, i vilken form och med vilka kommentarer. Internt inom varje medium görs dock ständiga avvägningar om namn och bild skall publiceras, om ännu inte helt bekräftade uppgifter kan presenteras, om man skall ta med en intervju som man inte är nöjd med, och så vidare.

Det måste göras ett antal journalistiska överväganden, men dessa kan ibland kollidera med andra typer av överväganden. Om till exempel redaktionen på SVTs Rapport vill bryta ordinarie sändningar med ett extrainsatt nyhetsprogram, så kan ansvarig sändningsledare göra en annan bedömning och insistera på att sändningstablån skall fullföljas.

Likaså kan överväganden om ekonomi och personalbemanning tillåtas övertrumfa journalistiska önskemål.

Det finns därför all anledning att inse att sårbarheten inom medievärlden kan ta sig många uttryck och att olika former av organisatoriska förutsättningar har en direkt och indirekt inverkan på nyhetsförmedlingen.

Organisation och psykosocialt omhändertagande

Vad finns det för inre organisatoriska ramar och förutsättningar som samspelar med det journalistiska arbetet och därigenom kan påverka mediernas förmåga att förädla och förmedla information utifrån vedertagna journalistiska arbetsmetoder och principer?

En viktig dimension som uppmärksammades bland annat i samband med att Estonia förliste och vid brandkatastrofen i Göteborg var hur medieorganisationerna tog hand om den egna personalen (Krisberedskapsmyndigheten 2003b). Vilken insikt råder på redaktionerna om betydelsen av att se till personalens psykosociala hälsa? De studier som vi har läst har mestadels ägnat sig åt journalisters och fotografers arbetssituation vid svårartade kriser. Då är behovet av psykosociala stödinsatser uppenbart. Men även vid normala förhållanden kan personalen bli överbelastad och slutkörd, viket i sig är problematiskt ur sårbarhetssynpunkt.

Vid branden på Hisingen i oktober 1998 gavs flera exempel på god personalvård hos den regionala TV-stationen. Den tillämpade bland annat att alla medarbetare som varit ute på brandplatsen måste infinna sig på redaktionen för samtal och debriefing innan de gick hem. Vidare bestämde ledningen att inte alla journalister fick bege sig till olycksplatsen. Anledningen var att händelsen var så fruktansvärd att personer som varit närvarande, hade mycket svårt att sedan återvända till redaktionen och fungera professionellt (Englund 2000).

Vi har valt att studera de organisatoriska aspekterna dels utifrån krav vid svåra påfrestningar, dels krav vid vardagliga förhållanden. Vid en svår påfrestning hand-

lar det inte enbart om hur medieföretaget agerar under krisen, utan även hur väl förberedd man är. Sårbarheten ökar om medieorganisationen inte har en fastställd plan för krishantering, om det saknas larmrutiner av personal, om det inte finns rutiner för personalbemanning vid en långvarig kris, om det inte finns lösningar för att hantera väldiga informationsflöden, om det saknas rutiner för loggföring av sända meddelanden och så vidare.

Finns denna förberedelse ökar förutsättningarna för att medierna skall kunna fungera tillfredsställande även under svåra påfrestningar. Under själva krisen måste ledningen uppmärksamma tecken på utmattning, psykisk skörhet, överbelastning och andra påfrestningar. Förmåga att strukturera behandlingen av såväl inkommande information som förmedlingen till publiken är också avgörande för rapporteringssäkerheten. I den mån som en medieorganisation har både tryckt tidning och nyhetsförmedling via Internet finns behov av samordning. Den egna omvärldsbevakningen måste vara välstrukturerad.

Ett särskilt problem under detta oerhört arbetsintensiva skede med ett väldigt inflöde av information är att ha förmåga att hinna bevaka och bevara den journalistiska kvaliteten.

Även under vardagliga förhållanden finns anledning att se på vilka organisatoriska omständigheter som kan påverka sårbarheten. En sådan faktor är de enskilda journalisternas utbildning och bakgrund, samt vilka värderingar och åsikter som styr deras journalistiska agerande. En annan faktor som är synnerligen grannlaga och känslig är kontrollen av arbetskamraternas agerande. Nyheter som är påhittade, nyheter som är direkt översatta från utländsk press, intervjuer som aldrig ägt rum är exempel på verksamheter som underminerar mediernas trovärdighet, men hur skall en ledning agera för att dels upptäcka sådana episoder, dels bevara kollegornas förtroende och respekt?

En tredje faktor är att ha ett sådant organisatoriskt minne att man kan relatera sig till en rad olika händelser. Om det uppstår en situation som är helt ny för medierna ökar risken att felaktigheter förmedlas, rykten uppstår och att uppgifter inte kontrolleras. Hur medieorganisationerna hanterar sin rekrytering och personalutveckling är således väsentligt för att minska sårbarheten.

En fjärde faktor är att rekrytera så att den egna organisationen har en god multikulturell kompetens, det vill säga att man inom den egna organisationen har personal med sådan bakgrund att man har förmåga att undvika missförstånd och kulturella stereotyper beroende på egen okunskap.

Att mäta mediers sårbarhet

Forskning som studerar medierna ur ett makroperspektiv finner ett antal stora och komplexa krafter som påverkar och påverkas av medierna: Teknik och ekonomi, juridik och politik, ekonomi och kultur (Nord & Strömbäck 2004).

Flera forskare har försökt att länka dessa makroaspekter till mikronivån, det vill säga till det journalistiska innehållet. Shoemaker och Reese (1996) urskiljer fem nivåer:

- Ideologisk nivå.
- Extra medienivå.
- Organisatorisk nivå.
- Medierutiner.
- Individuell nivå.

Det finns också modeller som lyfter fram att det går att urskilja flera agendor: en offentlig (public) agenda, en medial agenda och en policyagenda (Dearing & Rogers 1996). Inom offentligheten fokuseras intresset på vissa frågor, medierna har ett format och en värderingsstruktur som bildar en medial agenda och politiker och andra beslutsfattare driver frågor på en policy-agenda. Dessa tre agendor samverkar förstås. Det klaraste sambandet förefaller vara att den mediala agendan påverkar utformningen av offentlighetens agenda.

Men låt oss fördjupa Dearings och Rogers resonemang. Mer än undantagsvis finns det inte händelser som så totalt dominerar uppmärksamhet att man kan prata om ”en allmän agenda”. Det är mer relevant att studera samhället uppdelat i olika intressenter och aktörer. Det pågår hela tiden en kraftmätning i samhället om vilka händelser och skeenden som skall uppmärksammas och diskuteras. Under Olympiska spelen i Aten i augusti 2004 spred sig sportjournalistikens ringar ända fram till nyhetssidorna. Så snart spelen och efterdyningarna avklingat krympte sportagendan tillbaka till sportsidorna.

Även inom politik och annat beslutfattande finns det hela tiden krafter som konkurrerar om att sätta dagordningen. Förutom cykliska dagordningar som allmänna val, finns särintressen som vill diskutera alltifrån radon till glesbygdsfrågor.

Men alla försök att sätta dagordning är inte godartade och legitimerade av samhället. I Furustigs bidrag, *Informationsoperationer via medier*, ges en rik provkarta på mer subversiva och illasinnade försök att under vardagliga och normala förhållanden sätta agendan såväl inom medierna som i det offentliga rummet och på policynivå.

Redan denna rapsodiska beskrivning belyser svårigheterna att mäta i vilken utsträckning medierna är sårbara för yttre och inre påverkan. Vi skall ändå göra ett försök att ge förslag på indikatorer som skulle kunna visa sig användbara för att beskriva mediernas sårbarhet. Vi utgår från de sju faktorer vi valt att problematisera i kapitlet ovan.

• Mediernas krismedvetenhet.
• Mediernas trovärdighet.
• Mediernas förmåga att fånga information.
• Mediernas förmåga att förädla information.
• Mediernas förmåga att förmedla information.
• Mediernas förmåga att ge organisatoriskt stöd till det journalistiska arbetet.
• Mediernas förmåga till psykosocialt omhändertagande av de egna medarbetarna.

Vår grundläggande tankegång är att höga värden på de sju faktorerna innebär låg sårbarhet och förstås, att låga värden på de sju faktorerna innebär hög sårbarhet.

Vi har valt att avgränsa oss till den del av mediernas verksamhet som handlar om journalistiska värderingar och journalistiskt arbetssätt. När vi talar om mediernas verksamhet har vi exkluderat många organisatoriska och alla tekniska aspekter. Vi har också valt att tala om ”medierna” som om detta är en homogen skara med likartade värderingar och arbetsmetoder. Så är självklart inte fallet!

Vår ambition är att ge underlag till en diskussion om hur mediernas sårbarhet skall kunna beskrivas och mätas på ett sådant sätt att det ger vägledning inför beslut som innebär att mediernas roll i samhället stärks.

Mediers krismedvetenhet

Vad innebär det att en medieorganisation har hög krismedvetenhet? (1) För det första att medierna är medvetna om sin sårbarhet. (2) För det andra att medierna har planerat för att minska sårbarheten. (3) För det tredje att man har övat och tränat och informerat så att krismedvetenheten är väl förankrad hos alla verksamma i organisationen.

Ett sätt att mäta medvetenheten om sin sårbarhet hos en organisation är att se om det görs regelbundna risk- och sårbarhetsanalyser. Om så är fallet, kan man studera innehållet i dessa och därigenom få en god uppfattning om medvetenheten.

Planerna för att minska sårbarheten bör finnas fastlagda i ett dokument. Planen innehåller uppgifter om organisation, ansvar, rutiner, åtgärder före, under och efter en händelse med mera.

Övning och utbildning måste till för att säkerställa att planens intentioner får en klar verklighetsförankring hos alla medarbetare.

Vår bedömning är att genom att kontrollera förekomsten av och innehållet i risk- och sårbarhetsanalyser, planer för krishantering samt program för utbildning och övningar så får man en god bild av medieföretagens krismedvetenhet.

Ett sätt att hålla medvetenheten uppe är att kontinuerligt ställa frågan: Vad finns det för synsätt och mekanismer inom journalistiken som kan gynna den som vill påverka allmänheten och grupperingar inom offentligheten via medierna?

Mediers trovärdighet

Mediernas trovärdighet har varit föremål för undersökningar under en följd av år. SOM-institutet (Samhälle Opinion Massmedia) vid Göteborgs universitet, som gör årliga undersökningar, ställer till exempel frågan ”Hur stort förtroende har du för det sätt på viket följande samhällsinstitutioner och grupper sköter sitt arbete?”. Bland de 20 samhällsinstitutionerna finns Radio och TV samt Dagspress. De 6 000 slumpvis utvalda personer som svarar på frågorna besvarar även frågan ”Vilket förtroende har du för innehållet i följande massmedier?” Uppräkningen rymmer elva kategorier alltifrån Sveriges Television till lokaltidningar och nyhetstjänster på Internet (Holmberg & Weibull 2004).

Det finns således en mycket god empirisk grund att bygga på när det gäller att bedöma mediernas trovärdighet i allmänhetens ögon. Samtidigt finns det anledning att diskutera nya utvecklingslinjer när det gäller att mäta trovärdighet (Österman 2004).

En möjlig utvecklingslinje är att vidga trovärdighetsproblematiken till att omfatta andra grupper. Hur ser till exempel politiker, företagsledare, generaldirektörer och andra beslutsfattare på mediernas trovärdighet? Om svenska folket kan ses som mottagare av information och nyheter, så kan politiker och andra beslutsfattare ses som givare av information till medierna. Det borde därför vara mycket viktigt att fånga deras bedömning av mediernas trovärdighet. Minskar deras bedömning under en viss nivå kan man tänka sig att beslutsfattarna väljer att kommunicera via andra kanaler.

En andra utvecklingslinje skulle kunna vara att ställa frågor om trovärdigheten i särskilda situationer. En större kris kan vara en sådan situation. En kris är oftast lokal och en intressant frågeställning är om de lokala medierna får en annan ställning och trovärdighet under en kris jämfört med radio och TV på riksnivå (Alström 1997, Arvidson 1998). En annan frågeställning är vart olika grupper vänder sig om något eller några mediesystem slås ut eller blir misskrediterade.

En tredje utvecklingslinje är att studera trovärdigheten när det gäller försök att manipulera medierna. Återfinns de generella mönstren om mediernas trovärdighet också om frågorna riktas specifikt mot olika mediers förmåga att motstå informationsoperationer eller andra försök till manipulering?

Mediers förmåga att fånga upp information

Om medierna skall ha en låg sårbarhet krävs att mediernas representanter vid sina externa kontakter inte bara arbetar utifrån ett nyhetsperspektiv utan även studerar omvärlden ur ett sårbarhetsperspektiv.

En grundprincip är att försöka fånga de tidiga, svaga signalerna och att hitta mekanismer som gör att man kan urskilja de svaga signalerna i allt det brus som sköljer över medierna.

Hur mäter man dessa tidiga svaga signaler till förändring? Patrick Lagadec (1993) har beskrivit olika kännetecken på en potentiell krissituation:

- Det är omöjligt att analysera en fråga inom de befintliga referensramarna.
- Osäkerhet skapar en ovanlig och obekväm känsla.
- Personer som brukar agera håller sig borta.
- Det finns ingen gemensam måttstock mellan händelserna och de värden som styr hur frågan hanteras.
- Motståndet att ta sig an problemet är starkare än vad man kan vänta sig.
- Bisarra uttryck växer fram i säkra kanaler.

Ur ett sådant synsätt kan växa fram ett sätt att mäta sårbarheten i detta sammanhang genom att systematiskt utvärdera om aspekter på sårbarhet uppmärksammas, om det rapporteras inåt inom medieorganisationen samt om det följs upp av ledning och redaktion.

En annan dimension är att intervjua journalister om deras arbetssituation och arbetsvillkor och därigenom komma fram till indikatorer på ökad sårbarhet till följd av minskade möjligheter att söka och samla in information. Här är några förslag till utgångspunkter för en sådan intervju:

- Finns det tid att göra ett gott arbete?
- Är de som lämnar uppgifter duktiga på att få igenom sina budskap?
- Vad har Internet betytt för det journalistiska arbetet?
- Finns det förändringar i det journalistiska arbetet som påverkar möjligheterna att upptäcka försök till manipulation?

Mediers förmåga att förädla information

De punkter som nämns ovan har förstås även relevans när det gäller journalisternas möjligheter att förädla information. Men vi vill också föreslå att man väger in följande aspekter vid bedömningen av sårbarheten:

FINNS DET EN MULTIKULTURELL KOMPETENS INOM MEDIEFÖRETAGET?

Sverige är idag multikulturellt och vår omvärldsbevakning är global. Medier som saknar denna kompetens löper risk för missförstånd, oförstånd och bristande förmåga till djupare analys.

SLINKER VÄL FÖRPACKADE HÄNDELSER IGENOM MEDIERNAS GRANSKNING?

Om en händelse eller nyhet är väl anpassad till mediernas format och värderingar, ökar då sannolikheten att den släpps igenom ograverad?

FINNS PERSONALPLANERING FÖR LÅNGVARIGA KRISER?

Om ett krisförlopp blir utdraget över flera dygn ställs stora krav på att medierna har en personalplanering som ger goda arbetsförutsättningar och hög kvalitet på det journalistiska arbetet även under krisens tredje och fjärde dag.

ÖKAR BEROENDET AV NYHETSBYRÅER OCH ANDRA JOURNALISTER?

Det finns studier som visar att även för journalister är en av de främsta källorna till nyheter andra journalister (Nord & Strömbäck 2004). Detta är en journalistisk rundgång som är positiv i den bemärkelsen att ett nyhetsmedium kan kontrollera att man inte missat något i sin nyhetsbevakning. Men det kan också vara negativt om andra journalisters arbete accepteras rakt av och inte utsätts för samma kritiska granskning som annat material.

TILLGÅNG TILL JOURNALISTER MED SPECIALKOMPETENS

Tillvaron har i många avseenden blivit mer komplex och sammanvävd. I många sammanhang är det önskvärt med en specialkompetens inom den egna redaktionen som kan följa ett område och fortlöpande beskriva och analysera skeenden. Detta är inte minst viktigt för att kunna bevaka de skeenden som har ett långsamt framväxande förlopp och inte kännetecknas av en plötslig händelse.

MÖJLIGHETEN ATT DEFINIERA EN SITUATION

När Monica Lewinsky-affären var som mest aktuell hade Vita husets hemsida flera miljoner träffar per dag. Uppenbarligen var det många som gärna tog del av Vita husets sätt att definiera händelseförloppet.

Man kan diskutera om mediernas sårbarhet ökar i takt med att tillgången på alternativa källor växer på Internet. Regeringen och riksdagen, politiska partier, intresseorganisationer, företag, kommuner och andra aktörer har webbplatser som ständigt uppdateras, tillhandahåller såväl nyheter som bakgrund, förmedlar intervjuer och ger statistik med mera. Medierna får därmed en ny typ av konkurrens om uppmärksamheten.

Mediers förmåga att förmedla information

Om vi fokuserar på det journalistiska perspektivet, vad finns det för faktorer som kan göra medierna mer eller mindre sårbara när det gäller förmedlingen av information?

ÄNDRADE KRITERIER FÖR NYHETSVÄRDERING

Det är fortfarande lätt att identifiera rena nyheter i press, radio och TV. Samtidigt har medieformaten blivit fler och mer svårtolkade. Vi har verklighetsprogram som påminner om fiction och fiction som påminner om verklighet. Det finns dramadokumentärer, underhållningsdokumentärer och så kallad *reality-TV* med stor publik som därmed är potentiella arenor för påverkan.

Om definitionen av vad som är en nyhet och hur den presenterats blir omdefinierad av såväl aktörer som vill påverka medierna, som medierna själva och inte minst konsumenterna av mediernas utbud, så kanske detta skulle kunna definieras som en ökad sårbarhet i medievärlden genom att det blir svårare att förmedla ”verkligheten”.

SAMVERKAN MELLAN TIDSPRESS OCH PRODUKTIONSKRAV

Om färre journalister skall göra mer och kraven på snabbhet ytterligare har accentuerats så torde förutsättningarna för att förmedla information ha ändrats. Om det leder till minskad faktakontroll, minskad användning av externa bedömare, minskad bakgrundsresearch, ökad benägenhet att enbart transportera en uppgift från en extern sändare till lyssnare och läsare, så borde dessa förhållanden kunna tolkas som indikatorer på förändringar i sårbarheten.

KOMPLEXA SKEENDEN SKALL FÅNGAS I ENKLA BESKRIVNINGAR

Sveriges samverkan med omvärlden och vårt intresse för att veta vad som händer överallt i världen innebär bland annat en utmaning hos medierna att kunna beskriva de komplexa förhållanden som de ökade omvärldskontakterna medför. Hur beskriver man EUs jordbrukspolitik i en artikel? Hur långt måste ett nyhetsinslag bli som förklarar bakgrunden till händelser i Afrika?

En aspekt av sårbarhet skulle kunna vara graden av representativitet, utförlighet och relevans vid skildring av komplexa skeenden och händelser.

KONKURRENS OM UPPMÄRKSAMHETEN

Förmågan att förädla informationen beror inte enbart på mediernas inre förhållanden och resurser. Den hänger även samman med konkurrensen om uppmärksamhet från andra medier, men också från andra organisationer som förmedlar nyheter via egna kanaler, till exempel webbplatser på Internet.

Det innebär att bedömningar av om en nyhet tagits upp och hur den tagits upp av andra medier påverkar den enskilda medieorganisationens bedömning av vad som skall förmedlas.

Mediers förmåga att ge organisatoriskt och psykosocialt stöd

Mycket av det som skrivits ovan får sin styrka genom att det förankras inom medieorganisationen i form av planer, riktlinjer, policies och rutiner. Förutom dessa uttalade principer och tankegångar finns även en djup så kallad ”tyst kunskap”, det vill säga sätt att agera och hantera situationer som finns inom den enskilde journalisten och som kommer till uttryck genom de egna arbetsprestationerna. Denna kunskap kan lockas fram genom att nya journalister söker stöd och råd i svåra situationer av mer rutinerade kollegor.

Mediernas sårbarhet när det gäller organisatoriskt stöd bör kunna följas genom att konstatera förekomst av och innehåll i policies, riktlinjer, planer och rutiner. Men även genom att studera förekomsten av arbetssätt som stimulerar utväxling av ”tyst kunskap”, till exempel mentorskap, samarbete i olika projekt, speciella former för informellt kunskapsutbyte och liknande.

En särskild aspekt är hur medieorganisationen löser beredskapen för psykosocialt omhändertagande vid svåra påfrestningar. Finns en särskild plan? Finns ansvaret utlagt på särskilda personer? Finns kontakter med psykosocial expertis och t ex representanter för kyrkliga samfund?

Mediers sårbarhet på nationell nivå

Vi har hittills haft den enskilda medieorganisationen som tankemodell när vi studerat sårbarhet och möjliga sätt att mäta sårbarheten. Det är sårbarheten inom varje organisation som bör vara utgångspunkten. Först och främst för att det är personalen inom varje enskild medieorganisation som har ansvaret för att sårbarheten är låg inom den egna organisationen. Genom detta perspektiv säkerställer vi även att den lokala expertisen tas i anspråk, det vill säga varje medium är bäst på att konstatera den egna sårbarheten.

För SPF finns sedan möjlighet att aggregera de enskilda medieorganisationernas bedömning till en nationell nivå. Det finns dock anledning för SPF att också studera mediernas sårbarhet direkt på den nationella nivån.

Mångfald i medieutbudet anses av de flesta vara ett hälsotecken på vårt samhälle. Utvecklingstendenser som pekar på en minskad mångfald, borde därför vara en indikator värd att uppmärksamma vid bedömning av den generella sårbarheten.

Detta resonemang går även att överföra till enskilda svåra påfrestningar. Vid varje sådant tillfälle finns det anledning att studera mängden tillgängliga medier vid varje given tidpunkt. Om till exempel endast en nyhetsbyrå skildrar ett händelseförlopp kan detta indikera en ökad sårbarhet.

Det skulle också vara intressant att vidga resonemanget om sårbarhet till att inte enbart gälla mediernas arbete utan även ta med vilka som mottar mediernas budskap.

Om medieutbudet fragmentariseras och om konsumtionen fragmentariseras så innebär det att allt färre tar del av ett och samma budskap vid ett visst givet tillfälle.

En möjlig infallsvinkel är även mediernas tendens till att ”följa John”, det vill säga att bevaka samma nyhet på ungefär likartat sätt. Vid ett försök till manipulering av nyhetsbilden skulle det kunna vara utmärkt att utnyttja ett tillfälle när ”drevet går” och i skydd av detta agera för egna intressen. Men mediernas samsyn kan inte bara användas för att undgå uppmärksamhet, utan även till att fånga en stor del av uppmärksamheten för aktörernas egna syften.

Diskussion

Vårt angreppssätt är pragmatiskt. Vi vill undersöka möjligheterna att finna egenskaper och indikatorer på de egenskaper som gör det möjligt att uttala sig om mediernas sårbarhet, eller med andra ord, mediernas rapporteringssäkerhet.

I vår ambition att finna dessa egenskaper och problematisera dem, har vi valt att göra mycket generella beskrivningar av såväl sårbarhetsaspekter som mediestruktur. Avslutningsvis vill vi fördjupa oss något vad gäller sårbarhet och mediestruktur samt även föra in några andra väsentliga aspekter i resonemanget.

Mediernas sårbarhet kan studeras på ett antal nivåer. Vi återknyter här till forskarna Shoemakers och Reeses modell och poängterar vikten av att bestämma på vilken analytisk nivå sårbarheten skall studeras. På den individuella nivån handlar det om utbildning, etik, ansvar, arbetsmodeller, tidigare erfarenheter, samhällssyn med mera.

När vi analyserar medierutiner handlar det i mångt och mycket om de aspekter som vi diskuterat under rubrikerna ”fånga in – förädla – förmedla”, det vill säga de faktorer som styr journalisters och andra medarbetares vardag.

Den organisatoriska nivån omfattar ägarförhållanden, medieföretagets struktur och maktdelning, kommersiell eller public service modell med mera.

Extramedienivån rymmer alla de aspekter som finns utanför medierna själva. I vårt projekt är vi särskilt intresserade av aktörer som begagnar sig av informationsoperationer gentemot medierna.

Inte minst intressant blir de analyser som kombinerar olika nivåer. Vad betyder det för sårbarheten om grundutbildningen av journalister förändras åt ena eller andra hållet? Vad betyder det om antalet specialreportrar minskar samtidigt som antalet områden med högt specialiserad kunskapskärna ökar?

Vi har så gott som hela tiden skrivit om medier i allmänhet. Detta är förstås en oerhörd förenkling. Det finns en mycket stor spännvidd vad gäller resurser, teknik, nyhetsvärdering, rutiner och strukturer mellan de medier som verkar inom Sverige. Även här bör således analysen brytas ned på mer specifika medieformer. Några dimensioner som kan användas är: Är medieföretaget inom public service sektorn eller styrs det huvudsakligen av kommersiella överväganden? Har medierna en mycket avgränsad geografisk räckvidd eller är de mer eller mindre rikstäckande? Publiceras de enbart på Internet eller såväl på Internet som i tryckt form?

De förväntningar som samhället kan ställa på olika mediers rapporteringssäkerhet måste relateras till respektive mediums förutsättningar och inriktning av sin verksamhet. Är det till exempel möjligt att dela in medierna efter grad av förväntan från samhällets sida samt konsekvenser ur samhällssynpunkt om respektive medium misslyckas i sina journalistiska ambitioner?

Det är medierna som står i centrum för vår uppmärksamhet i denna rapport. Det är dock sannolikt så att de som försöker påverka mediernas representanter oftast vill nå en annan målgrupp, nämligen de som tar del av olika mediers utbud. En lyckad påverkan sedd ur en extern aktörs perspektiv kräver således att medierna

uppmärksammar aktörens utspel, återger den på ett sådant sätt att aktören är nöjd, att de tänkta mottagarna uppmärksammar budskapet via medierna, och att de tar det till sig på det sätt som den externa aktören har avsett. Dessutom borde genomslaget vara likartat i alla medier om en stark effekt ska nås. Så även om frågan om mediernas sårbarhet är oerhört viktig, bör den kompletteras med frågor såväl om utbudet, det vill säga aktörernas agerande, som genomslaget hos den tilltänkta publiken.

Till slut vill vi återkomma till kärnfrågan: går det att mäta mediernas sårbarhet? Vårt svar är ja. Hur skall i så fall sådana mätningar kunna ske? I denna rapport har vi visat var man kan börja och vilka faktorer som man skulle kunna väga in. Att utveckla mätinstrument som fångar enskilda medieföretags sårbarhet tror vi är betydligt enklare än att försöka nå ett sammanfattande mått över svenska mediers sårbarhet. Sannolikt är det så att man behöver mäta olika saker på olika nivåer. På en övergripande nivå blir till exempel frågor om mångfald bland medierna viktigt.

Vi anser att frågan om statsmakterna överhuvudtaget ska mäta mediernas sårbarhet är en fråga som i sig handlar om trovärdighet. Om sådana mätningar ska ske måste de utgå från en övertygelse hos mediernas representanter att sådana mätningar inte bara gynnar samhället, utan även enskilda medieföretag samt att mätningarna i sig inte rubbar medarbetarnas eller ägarnas eller allmänhetens förtroende för medierna.

Nästa steg borde därför vara en genomlysning av problemet, sett ur medieföretagens synvinkel. Här är några exempel på frågeställningar: Vilka för- och nackdelar ser medieföretagen med att kontinuerligt mäta sårbarheten? Vilka parametrar är aktuella att väga in i ett mätinstrument som ska studera sårbarhet och rapporteringssäkerhet? Hur ska mätinstrumentet utformas så att det är anpassningsbart efter varje medieföretags särart?

Referenser

Alström, Börje (1997). Morden i Falun. Rapport 171, Styrelsen för psykologiskt försvar

Arvidson, Peter (1998). Åsjäveln biter tillbaka. Lokalbefolkningens upplevelse av händelserna vid tunnelbygget kring Hallandsåsen, Rapport 175:2, Stockholm, Styrelsen för psykologiskt försvar

Dahlgren, Peter, Carlsson, G & Uhlin, L (1998). Mediernas bevakning av händelserna vid Hallandsåsen hösten 1997, Rapport 175:4, Stockholm, Styrelsen för psykologiskt försvar

Dearing, James W & Rogers E (1996). Agenda-Setting, Communication Concepts 6, London, Sage

Granström, Kjell (red, 2002). Göteborgskravallerna, Rapport nr 187, Stockholm, Styrelsen för psykologiskt försvar

Flodin, Bertil (1980). Radio Malmöhus och snöstormen, Rapport nr 98, Stockholm, Styrelsen för psykologiskt försvar

Flodin, Bertil (1999). Planlagd kriskommunikation, Utbildningsserie nr 2, Stockholm, Styrelsen för psykologiskt försvar

Furustig, Hans (2005). Informationsoperationer via medier, i Berggren, K (red) Mediernas beredskap, Stockholm, Styrelsen för psykologiskt försvar

Elliot, Maria (1997). Förtroendet för medierna. TV, radio och dagspress i allmänhetens ögon. Göteborg, Institutionen för journalistik och masskommunikation, Göteborgs Universitet

Englund, Liselotte (2000). Det journalistiska arbetet – erfarenheter av ett svårt uppdrag, i Larsson & Nohrstedt (red) Göteborgsbranden 1998. En studie om kommunikation, rykten och förtroende, Rapport 179, Stockholm, Styrelsen för psykologiskt försvar

Holmberg, Sören & Weibull, L (2004). Samlande institutionsförtroende. I Holmberg, S & Weibull, L. Ju mer vi är tillsammans, SOM-rapport nr 34, Göteborg, Göteborgs Universitet

Hvitfelt, Håkan & Nygren, G (red) (2004). På väg mot medievärlden, andra upplagen, Lund, Studentlitteratur

Jarlbro, Gunilla (2004). Krisjournalistik eller journalistik i kris? En forskningsöversikt om medier, risker och kriser, KBM:s temaserie 2004:1, Stockholm, Krisberedskapsmyndigheten

Johansson, Bengt (2004). Journalistikens nyhetsvärderingar, i Nord, L & Strömbäck, J (red) Medierna och demokratin, Lund, Studentlitteratur

Krisberedskapsmyndigheten (2003). Risk- och sårbarhetsanalyser, KBM rekommenderar 2003:1, Stockholm, Krisberedskapsmyndigheten

Krisberedskapsmyndigheten (2003b). Krisjournalistik. En introduktion för myndigheter, KBM:s utbildningsserie 2003:3, Stockholm, Krisberedskapsmyndigheten

Krisberedskapsmyndigheten (2004). Samhällets informationssäkerhet, Lägesbedömning 2004, Stockholm, Krisberedskapsmyndigheten

Lagadec, Patrick (1993). Preventing Chaos in a Crisis, Strategies for Prevention, Control and Damage Limitation, London, McGraw-Hill Book Company

Larsson, Larsåke (1998). Nyheter i samspel. Studier i kommunjournalistik, Göteborg, Institutionen för journalistik och masskommunikation, Göteborgs Universitet

Leth, Göran & Thurén, T (2000). Källkritik för Internet, Rapport 177, Stockholm, Styrelsen för psykologiskt försvar

Martinsson, Bengt-Göran & Säljö, R (1996). Insändare och debatt i svenska tidningar, Rapport 169-5, Stockholm, Styrelsen för psykologiskt försvar

McQuail, Denis (2002). Mass Communication Theory, 4th edition, London, Sage

Nohrstedt, Stig Arne, Höijer, B & Ottosen, R (2002). Kosovokonflikten, medierna och medlidandet, Rapport 190, Stockholm, Styrelsen för psykologiskt försvar

Nord, Lars & Strömbäck, J (2002). Tio dagar som skakade världen, Rapport 186, Stockholm, Styrelsen för psykologiskt försvar

Nord, Lars, Shehata, A & Strömbäck, J (2003). Från osäker källa. Bevakningen av Irakkriget i svenska medier. KBM:s temaserie 2003:4, Stockholm, Krisberedskapsmyndigheten

Nord, Lars & Strömbäck, J (red) (2004). Medierna och demokratin, Lund, Studentlitteratur

Nordström, Gert Z (2002). Terrorkriget i kvällspressen, Rapport 184, Stockholm, Styrelsen för psykologiskt försvar

Nygren, Gunnar & Alström, B (2004). Från murvel till varumärke och "content provider", i Hvitfelt, H & Nygren, G (red). På väg mot medievärlden 2020. Journalistik, teknik, marknad, andra upplagan, Lund, Studentlitteratur

Petersson, Olof & Carlberg, I (1990). Makten över tanken, Helsingborg, Carlssons

Riegert, Kristina (2002). Kampen om det kommunikativa rummet, Rapport 191, Stockholm, Styrelsen för psykologiskt försvar

Sahlstrand, Anders (2000). De synliga. Nyhetskällor i svensk storstadsmorgonpress, Stockholm, Institutionen för journalistik, medier och kommunikation

SOU 1999: 68 (1999). Brandkatastrofen i Göteborg. Drabbade, medier, myndigheter, Stockholm, Kulturdepartementet

Shoemaker, Pamela (1991). Gatekeeping, Communication Concepts 3, London, Sage

Shoemaker, Pamela & Reese, S D (1996). Mediating the message: theories of influences on mass media content, New York, Longman

Sveriges Informationsförening (2004). Nätverk 2003/2004, Stockholm, Sveriges Informationsförening

Wadbring, Ingela (2004). Nyhetsjournalistikens ekonomiska villkor, i Nord, L & Strömbäck, J (red) Medierna och demokratin, Lund, studentlitteratur

Warg, Lars-Erik (2000). Tillit och trovärdighet i riskkommunikation, i Lidskog, R, Nohrstedt, S A & Warg, L-E (red) Risker, kommunikation och medier, Lund, Studentlitteratur

Weibull, Lennart (2004). Förtroende för mediernas innehåll, i Holmberg, S & Weibull, L (red) Ju mer vi är tillsammans, SOM-rapport nr 34, Göteborg, SOM-Institutet, Göteborgs Universitet

Österman, Torsten (2004). Förtroende under vardag och kriser, Stockholm, Styrelsen för psykologiskt försvar

Tidningsartiklar

Dagens Nyheter 2003-08-14 Relevanta fakta inger förtroende

Dagens Nyheter 2004-08-08 Video med halshuggning av amerikan var ett skämt

Mediers beredskap
Informationsoperationer och mediers sårbarhet

Massmedierna är de viktigaste förmedlarna av olika typer av händelser i samhället. Information och kommunikation är inte bara medel för att bevara medborgarnas förtroende för och tillit till samhället och dess institutioner utan också väsentliga för att kunna rädda liv och egendom i störda situationer. Massmediernas trovärdighet är en förutsättning för detta.

Studien syfte är att fördjupa och bredda kunskapen om medieföretagens sårbarhet inom området informationsoperationer. SPF vill medvetandegöra risken för att medierna i dagens medielandskap utnyttjas för att avsiktligt vilseleda läsare, lyssnare och tittare.

Författare till studien är Bertil Flodin och Anders Sahlstrand vid Gullers Grupp Informationsrådgivare AB, Hans Furustig vid Totalförsvarets forskningsinstitut (FOI) samt Göran Stütz, tidigare forskningschef vid SPF. Redaktör är Katrin Berggren vid SPF.

SPFs skriftserie 2005:3

Styrelsen för
PSYKOLOGISKT FÖRSVAR
Box 2195, 103 15 Stockholm www.psycdef.se