Styrelsen för
PSYKOLOGISKT FÖRSVAR

VILSELEDNING PÅ INTERNET

Gunnar Sjöstedt
Paula Stenström

RAPPORT 183

VILSELEDNING PÅ INTERNET

– en analysansats

Gunnar Sjöstedt och Paula Stenström

Styrelsen för PSYKOLOGISKT FÖRSVAR

Utgiven av Styrelsen för psykologiskt försvar
ISSN 1401-2383
Stockholm 2002
Omslagsbild: Erica Jacobsson

INNEHÅLL

DEL III.

DEL IV.

SPFs FÖRORD

Styrelsen för psykologiskt försvar (SPF) har under senare år ägnat ett betydande forskningsintresse åt frågor som rör samhällets informativa och kommunikativa förmåga främst under störda men också under ostörda, normala, förhållanden. Den snabba utvecklingen på kommunikationsområdet – främst ITs och Internets accelererande betydelse på allt fler områden inom samhället – har av självklara skäl lett till att SPF vidgat sitt forskningsintresse inom dessa nya inslag i samhällsmiljön. Vilka möjligheter kan den nya informationstekniken ge den som önskar påverka människors tankar, attityder, föreställningar och beteenden i en för sändaren önskad, men eventuellt för mottagaren oönskad riktning?

Det är mot den bakgrunden som SPF genomfört ett antal studier, som ur olika aspekter belyser hur IT- och Internetutvecklingen kan påverka samhället och kommunikationen inom detta. Nämnas här kan studierna Hotet från IT (1993), Från löpsedel till webb (1999), Myndigheterna, Internet och integritet (2000) samt Källkritik för Internet (2000). SPF medverkar också sedan länge i årligen återkommande studier rörande medborgarnas bruk av olika medier, bl a Internet.

Utvecklingen i vår omvärld har under senare år medfört att de säkerhetspolitiska hoten förändrats och nu också inrymmer hot av icke-militär art. Till dessa senare hot hör bl a den psykologiska krigföring i form av informationsoperationer som, i termer av avsiktlig vilseledning, skulle kunna riktas mot vårt land. Hur sådana operationer faktiskt skulle gestalta sig är inte lätt att föreställa sig och förutse. Det empiriska materialet är knapphändigt varför en analys av problemområdet i långa stycken blir både teoretisk, hypotetisk och kanske spekulativ. En fråga i det sammanhanget är om Internet skulle kunna användas som vapen i operationer riktade mot vårt land i syfte att försöka påverka opinioner eller vilseföra beslutsfattare ytterst med syftet, att påverka vårt demokratiska samhällsskick eller nationella säkerhet? Hur kan vilseledning gestalta sig i det moderna informationssamhället? Det är om detta denna studie handlar.

Begreppet vilseledning är inte nytt, men formerna och verktygen förändras. Utgångspunkten i den här studien är demokratiska och säkerhetspolitiska sårbarheter i det IT-beroende samhället. Här ges ett helhetsperspektiv där hot, möjliga motmedel och sårbarheter betraktas i ett sammanhang. Jag vill tacka författarna, docent Gunnar Sjöstedt och fil kand Paula Stenström, för en mycket intressant studie, som ökar förståelsen för vilken kraft Internet skulle kunna ha som ett instrument för makt och inflytande och därmed bidrar till diskussionen om ett framtida svenskt agerande avseende IT-relaterade säkerhetsfrågor. Ett tack också till Överstyrelsen för civil beredskap som ekonomiskt bidragit till att projektet kunnat genomföras.

Göran Stütz
Forskningschef, SPF

FÖRFATTARNAS FÖRORD

Vi lever i en omvälvning som vi ännu bara har sett början av. Den informationstekniska utvecklingen är i ständig rörelse och förändrar snabbt perspektiven. Det skapas nya former av samarbete som kan bidra till att stärka det demokratiska samtalet och öka förståelsen mellan människor. Bland mycket annat har Internet öppnat dörren för andra än makteliter att få inblick i och ta del av sådan information som behövs för att kunna påverka samhällsviktiga beslut. Informationsteknologin (IT), som till och med kallas för ”den stora utjämnaren”, skulle kunna utvecklas och användas för fredsbevarande syften och diplomati i en värld som präglas av internationalism och ökad jämlikhet. Men den informationstekniska förvandlingen har även inneburit nya sårbarheter som skulle kunna skapa problem i det demokratiska samhället. Med den här studien vill vi bidra till att förbättra kunskaperna inom ett område som det flaggas om, men utan att svartmåla den nya informationsteknologin eller bli flaggbärare för dess kritiker. Som titeln anger handlar det om vilseledning på Internet.

Hur vi som har genomfört denna studie ser på Internet påverkar förstås inriktningen på studien. Därför vill vi lägga korten på bordet redan nu: Vi är inga tekniska experter utan intresserade av hur Internet skulle kunna brukas och missbrukas för att påverka människor. Självklart är det tekniken som ytterst betingar vad som kan åstadkommas med Internet. Men om, som är fallet i denna studie, syftet är att undersöka hur Internet kan utnyttjas för någon som vill vilseleda, kan analysen inte avgränsas till själva tekniken. Andra faktorer måste föras in i bilden, så som aktörer och intentioner. Utifrån den ambitionen visade sig ”Vilseledning på Internet” vara ett både komplext och relativt outforskat område. Det är inte minst därför vi tycker att ämnet är intressant.

Ett första viktigt steg var att intervjua representanter med stor erfarenhet och kunskap inom området från medier, näringsliv, rättsväsende, försvar och den centrala statsförvaltningen (se referenser). Vi vill tacka Er för att ni ställt upp med både tid och engagemang. Ni har hjälpt oss att hitta fall, ni har låtit oss ta del av er erfarenhet och kunskap och ni har också bekräftat för oss att ämnet för denna studie är angeläget. Vi vill även tacka SPFs forskningschef Göran Stütz och docent Roland Nordlund (tidigare verksam vid SPF), Martin Bennulf (SPF) samt Barbro Malmer (tidigare ÖCB) för det stöd de har givit projektet.

Det mesta som sammanhänger med informationssamhället befinner sig i mycket snabb förändring. Detta gäller också förutsättningarna för vilseledning på Internet. Därför finns självklart en risk för att vissa sakuppgifter och bedömningar som presenteras i denna skrift hunnit bli inaktuella sedan vi inledde projektet. Vi tror dock inte att helheten störs alltför mycket av detta.

Gunnar Sjöstedt och Paula Stenström
Stockholm, februari 2002.

NÅGOT OM SPRÅKET

Internet är det internationella datornät som har den största utbredningen och som bygger på TCP / IP, en standard för datakommunikation. Många av de ord som beskriver Internet saknas i svenska språket. Ibland tas engelska uttryck rakt av, ibland blir det ”svengelska” (t.ex. ’mailen’) och ibland används svenska översättningar. Eftersom området är så pass nytt kan olika uttryck för samma sak skapa missförstånd. Utan att gå efter några speciella regler har vi i denna skrift försökt att hålla oss till samma begrepp för samma sak. I någon mån har vi också följt Svenska Datatermgruppens rekommendationer (www.nada.kth.se / dataterm).

Vissa uttryck är så pass etablerade att risken för missförstånd är förhållandevis liten. Exempelvis använder vi engelskans *mail* eller *e-mail* för elektronisk post vilket kan definieras som ”överföring av meddelande med hjälp av datorer där meddelandet kan läsas vid valfri tidpunkt”. Här rekommenderar Svenska Datatermgruppen tvärtom det svenska ordet ”e-post”, men vi använder det engelska uttrycket eftersom det är det som används i dagligt tal. Verbet ”att maila” är vanligare (och kortare) än svenskans ”att skicka e-post” eller ”att e-posta”. Substantivet ”mail” är också vanligare och lättare än ”e-postmeddelande” tycker vi. Kortformen ”nätet” är egentligen att uppfatta som en kortform av ”det internationella datornätet” e.d. och inte av Internet. Internet kallas här ibland ändå för *nätet*. Då avses hela Internet och inte bara www-delen av Internet. Ett annat begrepp som vi valt att använda är *webbplats* som ersätter annars vanligt förekommande uttryck som engelskans ”webbsite” eller ”site” och de svenska varianterna ”sajt” respektive ”nätplats”. Ordet ”hemsida” har vi undvikit då det allt som oftast används för flera olika betydelser: ingångssida, startsida, webbsida och webbplats. Vi har här följt datatermgruppens råd och använder istället *webbsida* för enskilda sidor (den mängd information på en webbplats som man kan nå utan att behöva gå vidare via en länk, vilket oftast motsvaras av det man kan se på skärmen samtidigt eller genom att rulla bilden) och webbplats när det är fråga om en sådan.

Andra språkligheter handlar om nyckelbegrepp i undersökningen som för en utomstående inte behöver vara självklara. De viktigaste begreppen, t.ex. vad vi avser med *vilseledning* och *Internet* definieras i del I. Andra analytiska begrepp förklaras antingen i första eller andra delen.

DEL I
VAD, VARFÖR, HUR?

Where is all life we lost in living ?
Where is all wisdom we lost in knowledge?
Where is all knowledge we lost in information?
/ T S Eliot

Vad?

Vilseledning har förekommit i alla tider och har återkommande varit ett verkningsfullt politiskt instrument i konflikter där stora värden står på spel. Däremot har formerna och verktygen för vilseledning förändrats under historiens gång. Frågan här är hur vilseledning kan se ut i det moderna informationssamhället?

Syfte och avgränsningar

Vårt syfte är att diskutera på vilket sätt Internet har förändrat förutsättningarna för vilseledning och hur man skulle kunna motverka sådana aktioner. En underliggande fråga gäller samhällets sårbarhet: skulle vilseledning via Internet kunna få negativa konsekvenser för det demokratiska samhället och, ytterst, för den nationella säkerheten?

Vår intention är dock *inte* att göra en bedömning av hur ”farligt” vilseledning på Internet är. Avsiktlig vilseledning behöver inte vara olaglig och behöver inte heller alltid åtgärdas. Vilseledningens ”farlighet” sammanhänger ytterst med dess konsekvenser – och inte med dess metoder. Svenska fall av vilseledning på Internet som haft säkerhetspolitiska konsekvenser saknas dock på det hela taget. Däremot finns en rad uppgifter tillgängliga som visar att individer och organisationer i det normala fredssamhället använder sig av Internet för att med olika motiv, till exempel vinningslystnad eller hämndbegär, försöka lura varandra. En central utgångspunkt för den här studien är att även om det saknas belägg för att det förekommer vilseledning på Internet med relevans för svensk demokrati och säkerhet under normala omständigheter i fredstid, skulle sådan verksamhet kunna förekomma under andra samhällsförhållanden. En annan utgångspunkt är att förbättrad kunskap om harmlös vilseledning som är acceptabel i en demokrati är relevant för förståelsen av vilseledning med mer samhällsfarliga konsekvenser.

Vi är således ute efter att utveckla en ansats som kan användas för att studera problemområdet och därmed öka förståelsen för vilken *potential* vilseledning på Internet skulle kunna ha som ett instrument för makt och inflytande.

Det handlar genomgående om *avsiktlig* vilseledning. Vi berör således inte vilseledning som uppstått på grund av missförstånd eller är självförvållad genom misstag eller okunskap.

Vilseledning

Vilseledning är en form av *inflytande* som en aktör – *sändaren* – genom *kommunikation* uppnår över en annan aktör – *mottagaren*. Vilseledning skulle i och för sig kunna ha ett självändamål men antas i denna undersökning motiveras av ett *bakomliggande syfte* som kan vara av varjehanda slag (t.ex. beröra privata förhållanden, ekonomiska värden, makt eller säkerhet).[2] Skälen till att man vilseleder någon är detsamma som varför man ibland ljuger. Man vill skydda sig själv eller uppnå något, och man tror att det bekvämaste, mest effektiva eller rent av enda sättet att göra det är att ljuga. Men vilseledning är inte alltid detsamma som att ljuga, eftersom det inte krävs en lögn för att luras. Vilseledning kan även vara att avleda uppmärksamheten eller dölja något. Man kan säga att vilseledning innebär en *kalkylerad verklighetsförvanskning*. På så sätt har vilseledning i grunden stora likheter med trollkarlens illusionstrick.

Sändaren kan i princip vara vem som helst: en privatperson, en organisation, ett företag, en nu eller tidigare anställd, en regering, en brottsorganisation eller en terroristgrupp. *Mottagaren* kan på samma sätt vara allt ifrån en enskild individ till en stat. Inflytande uppstår genom att sändaren påverkar mottagarens attityder, tankar, känslor och beteende.

*Framgångsrik vilseledning innebär alltså att mottagaren ges en förvrängd bild av en del av verkligheten och på grund av detta beter sig så som sändaren önska*r. Detta beteende kan ha formen av utåtriktade handlingar. Beteendeförändringar kan också vara helt interna i en aktör och bestå av ett nytt sätt att tänka på eller värdera ett visst fenomen. Sådana interna förändringar kan i sin tur så småningom utlösa utåtriktade handlingar. Den som vilseleds behöver inte alltid ta skada bara för att sändaren uppnått sitt mål. Med den här definitionen skulle vilseledning kunna komma till uttryck som PR, lobbying, reklam eller politisk propaganda; alltså fullt lagliga och vanliga verksamheter i det demokratiska samhället. Men vilseledning *kan* också vara allvarligare: t.ex. att föra en stats beslutsfattare bakom ljuset i en förhandling eller påverka ett annat lands försvarsplanering. Sedan behöver själva mekaniken varken vara särskilt komplicerad eller allvarlig för att få allvarliga konsekvenser.

Vilseledning kan åstadkommas på en rad olika sätt.[3] Variationsrikedomen är stor, men i stort kan vilseledning hänföras till två grundformer: *simulering* respektive *dissimulering*.

Simulering

Genom simulering försöker sändaren *få mottagaren att uppfatta en skenbild som verklig*. Detta kan åstadkommas med hjälp av tre ansatser. En sådan ansats har karaktär av *uppfinning*. Sändaren skapar att nytt, men falskt, fenomen, vilket genom sina egenskaper kan få en effekt på mottagarens föreställningar eller handlande. Ett exempel är den sovjetiska, gigantiska atomladdade missil – domedagsvapnet – som ”uppfanns” i slutet av 1950-talet, men i verkligheten inte existerade. Avsikten med domedagsvapnet var att få bedömare i väst att militärt övervärdera Sovjetunionens kärnvapenresurser (Mitalka, 1982). *Efterapningen* är en nära besläktad simuleringsteknik. Genom att visa falska spår av ett fenomen vill sändaren få mottagaren att dra slutsatsen att det fenomen, som indikatorerna hänför sig till är vid han-

---

[2)] Vilseledning som självändamål ska emellertid inte betraktas som en verklighetsfrämmande teoretisk konstruktion. I ett av de fall, som nedan ska refereras till, lades en falsk webbplats ut i form av en nyhetsbyrå med nyheten att Pol Pot var i Sverige. Skälet till detta uppgavs bl.a. vara att man ville pröva ifall medierna på detta sätt kunde föras bakom ljuset.

[3)] För en grundläggande diskussion om begreppet vilseledning se Sjöstedt, 1988, samt Stenström, 1997.

den. En tredje ansats för simulering är att sändaren låter genomföra avledande *operationer* för att mottagaren inte ska upptäcka en viss företeelse. En bra liknelse är matadorens rörelser med den röda muletan för att dra bort tjurens uppmärksamhet från sin egen kropp. Plojen i detta fall är att få tjuren att uppfatta muletan – och inte matadoren – som ett hot. Ett känt exempel från historien är de avledande aktioner som de västallierade genomförde sommaren 1944 för att dölja förberedelserna för en invasion i Normandie (Haswell, 1979).

Dissimulering

Den andra grundformen för vilseledning är dissimulering, som innebär att sändaren försöker *dölja förekomsten av ett fenomen eller en händelse för mottagaren*. Dissimulering kan i princip åstadkommas med hjälp av tre ansatser, vilka utgör spegelbilden till simuleringens tekniker. En metod är att rent fysiskt *kamouflera* något, till exempel att hålla ett fenomen hemligt med stränga sekretessregler som täckmantel. Fenomenet som ska döljas kan också *förklädas* så att det inte igenkänns eller göras osynligt genom att det fås att smälta in i sin omgivning – ”*omvärldsskuggning*”. När exempelvis en viss signal ska sändas som sändaren inte vill att mottagaren ska uppfatta skapas ” – samtidigt ett sådant brus runt omkring att andra lyssnare än själva mottagaren uppfattar signalen som en del av bruset” (Sjöstedt, 1988).

I praktiken bygger vilseledningen ofta på en kombination av simulering och dissimulering.

Internet

Med Internet avses här de vanligaste tjänster och möjligheter som en uppkoppling till Internet erbjuder idag: sökmotorer, webbplatser, e-mail, filöverföring, diskussionsgrupper, elektroniska anslagstavlor, chat bland många andra.

Varför?

Ännu en bok om Internet alltså. Behövs verkligen det? Det finns hyllmetrar av litteratur som tar upp olika aspekter av Internet; den tekniska utvecklingen[4], handledning för att använda Internet[5], lag och rätt på Internet[6], etik på Internet[7], demokrati och Internet[8], för att nämna några teman.

Tekniska säkerhetsfrågor är ett välbevakat område. Därutöver finns det statliga och andra rapporter och utredningar som särskilt tar upp sårbarheter med hänsyn till IT-utvecklingen.[9] Detta gäller inte minst senare tids totalförsvarsutredningar där IT-relaterade hot givits en betydande plats.[10] Även frågan om miss-

---

4) T.ex. Tor Nørrestranders 1998. Böcker om Internet inleds ofta med en bakgrundsbeskrivning till Internetrevolutionen. Denna handlar vanligtvis om den informationstekniska utvecklingen och expansionen av Internet. Utvecklingen av Internet håller ett högt tempo och böcker av det här slaget blir snabbt inaktuella. Det bästa sättet att hålla sig uppdaterad om vad som händer torde vara att följa med på nätet.

5) T.ex. Häger & Strömblad 1998, Jakobsson 1998. Utöver dessa handböcker finns dessutom ofta interaktiva IT-skolor och nätguider med söktips och instruktioner lättillgängligt på nätet.

6) T.ex. Carlén-Wendels 1998. Dessa böcker tar upp frågor som yttrandefrihet, ansvar för brott, integritet, upphovsrätt, varumärken, marknadsföring, elektronisk handel, skatteregler m.m.

7) T.ex. Engström & Sandgren 1999. Denna litteratur tar exempelvis upp frågor om vad man får och inte får skriva på en webbplats (rashets, religiös extremism, pornografi etc).

8) T.ex. Åkerström 1999, Truedson 1999. Demokratiböckerna tar upp Internets betydelse för demokratin; håller Internet på att skapa förutsättningar för en utveckling med mer direkt demokratiska inslag? Eller kan Internet istället ha en segregerande inverkan genom att det skapar ett 2 / 3-samhälle?

9) T.ex. PTS utredningar om IT-incidenthantering 2000 och 2001, RRV rapport 1997:33, Küchler 2000, SOU 1997:73, Nydén 1995.

10) T.ex. regeringens arbetsgrupp om informationskrigföring (AgIW:s) rapporter om åtgärder och skydd mot informationskrigföring 1997 och 1998. Andra exempel är Eriksson & Fylkner 1999, Mittermaier & Westrin 1999, Fylkner, Grennert & Mittermaier 2000, Lerdell 2000 samt Sundberg 2000.

bruk av Internet har belysts i litteraturen.[11] I den senaste försvarspropositionen betonas att samhällets sårbarhet i förhållande till IT-relaterade hot är av stor säkerhetspolitisk betydelse. Det arbete som sker i Sverige för att öka säkerheten för samhällsviktiga IT-system och för att minska riskerna av såväl IT-incidenter som informationsattacker har fått hög prioritet (prop 1999/2000:30).[12] Tyngdpunkten i de försvarsutredningar som hittills gjorts har legat på det tekniska skyddet av IT-beroende verksamheter och kritisk infrastruktur, liksom på hur IT kan, och i en framtid skulle kunna användas, på det militära slagfältet.[13]

Även rättsväsendet har fått en ny miljö att agera i och man satsar för fullt för att förbättra förutsättningarna föra att bekämpa IT-relaterad brottslighet. Kunskap om IT-incidenter och IT-relaterade brott är efterfrågad, men än så länge begränsad i många hänseenden. När det gäller missbruk av Internet uppskattas mörkertalet som mycket stort. Brottsförebyggande rådet (BRÅ) kom under 2000 ut med en rapport som bl.a. visar att IT-relaterade brott och incidenter mer än fördubblats sedan 1996 (BRÅ-rapport 2000:20). De vanligaste IT-relaterade brotten i Sverige är enligt samma undersökning datavirus, externa och interna dataintrång, stöld och manipulation av information samt bedrägeri via Internet. BRÅ-rapporten visar att den tekniska säkerheten har ökat markant under senare år, men när det gäller manipulation av data är emellertid både säkerhet och medvetenhet om farorna fortfarande bristfällig.

Kampen om våra sinnen är som sagt inget nytt. Det är informationstekniken som har skapat nya möjligheter för att komma åt, hindra och förvanska information. Det är därför inte förvånande att de tekniska aspekterna tenderar att hamna i första rummet oavsett om det handlar om IT-säkerhet, informationskrigföring eller IT-brottslighet. Men frågan är om det räcker med tekniska lösningar för att hantera vissa former av missbruk på Internet – t.ex. avsiktlig vilseledning? Vi tror inte det. För även om det börjar med teknik så är tekniken inte fristående från den information som den lagrar och förmedlar. Den färgar av sig på informationens möjligheter och utseende. Den förändrar inte bara hur vi säger saker till varandra, utan även utformningen av innehållet och hur vi uppfattar det. Som vi skall se har Internet inte bara förändrat, utan kanske också förbättrat möjligheterna till vilseledning. I en studie av vilseledning på Internet måste man därför föra in andra faktorer än själva tekniken; så som aktörer, intentioner, strategier och inte minst vilka effekter vilseledningen kan få. Det behövs nya perspektiv.

---

11) Detta kan vara incidentrapporter och analyser av dessa. Ett bra exempel är John D. Howards avhandling ”An Analysis of Security Incidents on the Internet 1989-1995”.

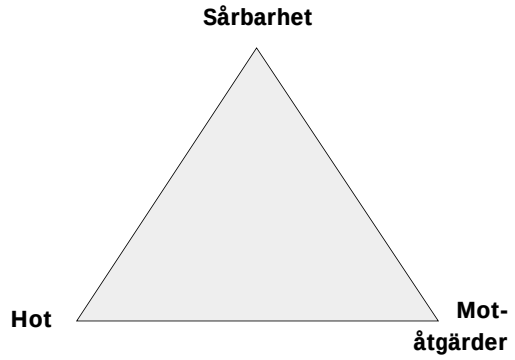
12) Det är fortfarande en öppen fråga om en informationsattack skall betecknas som en IT-incident eller inte. Post- & Telestyrelsen har gjort ett förslag till definition där IT-incidenter står för oönskade och oplanerade händelser som drabbar eller påverkar IT-system, eller utnyttjar IT-system, och kan medföra allvarliga negativa konsekvenser för ägare, användare eller andra. I PTSs översikt över IT-incidenter sorterar informationsattacker under ”civila informationsoperationer” och avser *avsiktlig desinformation som publiceras eller distribueras över Internet* (PTS 2000-03-16).

13) ÖCBs Infrastrukturuppdrag om sårbarheten i den tekniska infrastrukturen (rapporterad till Regeringen 15 mars 2000) är ett exempel på det förra. ”Försvarsmaktens Ledningskrigföringsstudie” (H 21 120:8462) från december 1998 är ett exempel på det senare.

Hur?

Ett holistiskt perspektiv

Till att börja med ville vi utforska vilseledning på Internet ur ett *holistiskt* perspektiv, i den meningen att hot, möjliga motåtgärder och sårbarheter i princip betraktas i ett sammanhang.



Figur 1. Ett holistiskt perspektiv på vilseledning på Internet

Varje sida av den nationella säkerheten kan förstås studeras separat från varandra i särskilda undersökningar. I ensidiga hotanalyser riskerar man emellertid lätt att överdriva enskildheter, medan helhetsbilden förblir otydlig och tvärtom skulle kunna underskattas.[14] Med figur 1 vill vi visa att ingen av den nationella säkerhetens tre sidor kan förstås fullt ut såvida inte vars och ens förhållande till övriga två aspekter beaktas. Sambandet mellan de tre säkerhetsaspekterna kommer till uttryck på olika sätt. Det är hotbilderna som motiverar planering av motåtgärder. Dessas uppläggning och genomförande är betingade av sårbarhetsförhållandena, vilka utgör en utgångspunkt för prioritering mellan olika insatser av motåtgärder. Värderingen av hotbilden påverkas av motsvarande sårbarhetsförhållanden. Ju mindre sårbarheten är desto mindre relevant blir hotbilden för säkerhetspolitiska analyser. Sårbarhetsförhållandena påverkas vidare av tidigare genomförda motåtgärder. Antag till exempel att god träning i att bedöma källor på Internet är ett bra motmedel mot vilseledning. I så fall innebär avsaknaden av sådan träning att sårbarheten mot vilseledning är mycket större än om sådana motåtgärder genomförts.

Metod

IT-hotet i allmänhet, och det som sammanhänger med vilseledning på Internet i synnerhet, är komplext och svårgripbart. Utifrån ovan nämnda ambitioner är ”vilseledning på Internet” därför svåranalyserat. Samtidigt som kunskapsläget är en utmaning innebär det viktiga restriktioner för hur ett projekt kan läggas upp. Enligt vår bedömning är ännu den enda rimliga ambitionsnivån att genomföra en utforskande, *explorativ* undersökning, d.v.s. att upptäcka och utveckla analysen av problemområdet och därmed bereda marken för fortsatta studier.

Underlag

Underlag till studien är hämtad från litteratur, sökande efter information på nätet, föredrag, intervjuer, seminarier och workshops.[15] Mate-

[14] CSIS gör också denna bedömning i: ”Critical Infrastructure Protection and Information Warfare” från 16 juli 2000.

[15] Ibid. Bakgrundsmaterial som inte refereras i texten: Cordsman 2000, ”Europas säkerhet – Sveriges försvar” (Försvarsdepartementet Ds 1999:55), Furustig & Sjöstedt 2000, Haswell 1979, Jakobsson 1998, ”Nationalencyklopedin” 1992, Nydén 2000, Regeringens regleringsbrev för 2000 avseende SPF, prop 1999/2000:86, Rothstein 1995, SOU 2000:55, Stenström 1997,1998, Taylor 2000, material från ”The Presidents Workinggroup on Unlawful Conduct on the Internet”, Thurén 1997, Wik 1999. Artiklar från Aftonbladet, Arbetet Nyheterna, Beredskap, Dagens Nyheter, Internet World, Journal of Strategic Studies, Seybold Seminars Panel samt The Bridge News Forum.

rialets spännvidd från teknik och datasäkerhet till vilseledningens psykologi speglar både det holistiska perspektivet och områdets bredd.

I ett första steg tyckte vi att det var viktigt att komma så nära verkligheten som möjligt. Detta har vi försökt uppnå dels genom *intervjuer* med olika aktörer med stor erfarenhet och kunskap inom relevanta områden (medier, näringsliv, rättsväsende, försvar och den centrala statsförvaltningen)[16], dels genom att samla in konkreta *fall* av vilseledning på Internet. Fallen har hittats genom litteraturstudier, sökande på nätet och genom uppgifter som kommit fram under intervjuerna.

I fantasin kan man lätt föreställa sig många olika sätt att vilseleda med hjälp av Internet. Säkra och fullständiga data om vilseledning på Internet är emellertid mycket begränsade. Framför allt saknas information om enskilda fall, som genomlyser vilseledningens alla faser från planering, över praktiskt genomförande till uppnådda effekter. Tillgängliga uppgifter ger precisa insikter när det gäller vissa enskilda aspekter av vilseledning, särskilt när dessa är teknikrelaterade, men ger i andra hänseenden endast en allmän överblick med stora luckor i (Howard 1997). Det krävdes därför en viss möda att hitta en uppsättning fall.

Kriterier för urval av fall

De utvalda fallen är exempel på när någon avsiktligt vilselett en bestämd mottagare med hjälp av Internet. Samtliga fall i undersökningen har *inträffat i verkligheten*, även om mängden uppgifter såväl som källornas tillförlitlighet varierar. Fallens konsekvenser har inte varit avgörande i urvalet. Fallen har alltså inte valts för att de är särskilt allvarliga ur vare sig säkerhetspolitiskt eller demokratiskt hänseende. Det finn skäl att tro att all form av vilseledning har vissa gemensamheter, t.ex. i form av mekanismer. Därför har istället *vilseledningens mekanik* varit ett viktigt urvalskriterie.

Även om fallen sannolikt inte är heltäckande för en tänkt population av faktiska eller möjliga vilseledningsfall, så är de anpassade för att i *så stor utsträckning som möjligt* spegla variationsrikedomen av möjligheter som Internet ger den som avsiktligt vill vilseleda en mottagare. De sexton fall vi har valt ut är dels exempel på *olika former av vilseledning* (simulering eller dissimulering), dels på olika operationstekniker som Internet erbjuder den som vill vilseleda (blockering, informationsupphämtning, sändning, ”att lägga agn” eller kommunikation genom interaktion – se Del II).

Fallen kan vidare betraktas som exempel på mer generella fall; *typfall*. Utifrån typfallen är det möjligt att utveckla fiktiva fall eller scenarier med säkerhetspolitisk relevans. Sammanlagt presenteras tio typfall med tillhörande scenarier, varav tre hänför sig till *hot mot demokratin* och sju gäller *hot mot den nationella yttre säkerheten* (se Del IV).

Fyra frågor

Syftet är alltså att, utifrån det holistiska perspektivet, *diskutera* hur Internet kan ha förändrat förutsättningarna för den som avsiktligt vill vilseleda en mottagare, vad man skulle kunna göra för att motverka vilseledning på Internet och vilken sårbarhet som finns. *Trots att vi använt oss av empiriskt underlag i form av fall är studien således i första hand teoretisk.* Diskussionen har sin utgångspunkt i följande fyra frågor:

16) Se referenser.

– Hur genomförs vilseledning och hur skulle Internet kunna komma till användning i detta sammanhang? (Del I och II)

– Skulle avsiktlig vilseledning på Internet kunna generera hot, i meningen få negativa konsekvenser för demokratin och den yttre nationella säkerheten? (Del IV)

– Hur skulle man kunna motverka avsiktlig vilseledning på Internet? (Del V)

– Vad återstår det för sårbarheter avseende vilseledning på Internet, när hänsyn tas till möjliga motåtgärder? (Del VI)

Upplägg

Frågorna – precis som undersökningen i sin helhet – följer det holistiska perspektivet. I nästa del sätts vilseledning på Internet in i ett analytiskt sammanhang. Del III innehåller de fall av vilseledning på Internet. Fjärde delen är en analys av fallen utifrån ett hotperspektiv och handlar huvudsakligen om vilka möjligheter Internet ger den som vill vilseleda en bestämd mottagare. I Del V tar vi mottagarens parti: på vilka sätt kan man undvika att bli vilseledd på Internet? I sjätte delen vägs dessa båda sidor mot varandra och sammanfattas i en diskussion om sårbarhet. Sista delen – Del VII – är en utvärderande slutkommentar där frågeställningarna besvaras.

DEL II
VILSELEDNING PÅ INTERNET – EN ANALYSANSATS

Vilseledning på Internet: Några fördelar

På Internet sänds nyheter och annan information i realtid över alla gränser – tankemässiga såväl som geografiska. Utbudet av källor och kanaler har blivit näst intill obegränsat samtidigt som avstånden har krympt. Det ökade utbytet av information har sannolikt ökat omfattningen av olika aktörers försök att påverka människors uppfattningar och beteende genom ord, ljud och bild. Utvecklingen av Internet innehåller i alla fall några inslag som skulle kunna underlätta för den som vill påverka – eller vilseleda – sin omgivning. Det kan vara lämpligt att redan från början göra några allmänna observationer:

- På Internet kan i stort sett vem som helst bli publicist och i jämförelse med andra medier är det väldigt billigt att publicera sig. Förutom att det är billigt blir informationen lättillgänglig och kan snabbt spridas till en stor publik. Därför trängs allt fler på nätet och det är svårt att få överblick.

- En växande mängd individers uppkoppling till nätet skulle kunna ge upphov till negativa effekter. Störningar i ett led kan sprida sig som ringar på vattnet och stora delar av samhället riskerar att påverkas.

- Det finns de som menar att människor är benägna att ta mentala genvägar när pressen blir för stor. ”Information-overload” är sedan länge ett välkänt begrepp. Informationsöverflödet i kombination med ett minskat förtroende för myndigheter och medier,[17] skulle kunna bidra till att allt fler vänder sig till publikfriande informationskanaler och program där de faktiska förhållandena inte alltid sätts i första rummet (”infotainment”).

- En snygg layout och en proffsigt uppbyggd webbsida är förtroendeingivande och skapar en föreställning om innehållets kvalitet som inte behöver vara riktig. Uppdateras webbplatsen kontinuerligt så ökar förmodligen tilltron till innehållet ytterligare. På Internet finns dessutom möjlighet till spårlös uppdatering.

- Samtidigt som klimatet ställer högre krav på källkritik är det kanske inte alltid möjligt för journalister och andra förmedlare av information att bedöma källorna i den mån

[17] Enligt undersökningar finns det tecken som tyder på att den svenska allmänhetens förtroende för olika institutioner i samhället (inklusive medier) har minskat (t.ex. Österman 1999).

det är önskvärt.[18] Den hårdnade konkurrensen och tidspressen skapar visserligen större öppenhet, men kan också leda till felbedömningar och förhastade beslut.

- Att bedöma, jämföra, kontrollera och följa upp information på Internet på ett tillfredsställande sätt är både tidsödande och kräver kännedom om mediet i sig; en kunskap som ännu är ojämnt fördelad i samhället.

- Rutinmässig källkontroll kan visa sig vara opålitlig. Vilseledande information eller rykten som sprids över Internet förs lätt vidare. Detta kan ge upphov till s.k. rundgång i informationsspridningen: en uppgift bedöms som trovärdig för att den publiceras på flera olika ställen, men kan visa sig ha ett och samma (otillförlitliga) ursprung. Det finns även goda förutsättningar för en sändare att dölja eller förfalska sin identitet.

- På Internet sparas all information digitalt på en eller flera servrar, men det går också att genom intrång ersätta information eller få det att se ut som om viss information aldrig funnits. Man kan med enkla medel skyla över gamla misstag eller ändra uppgifter på nätet så att de bättre passar för ens egna syften.

Alla de här förhållandena skapar fördelar för den som är ute efter att vilseleda sin omgivning.

Vilseledningsoperation: Ett nyckelbegrepp

För att åstadkomma ett aktörsperspektiv på undersökningen har vi i analysen valt att se på den avsiktliga vilseledningen som en operation – en *vilseledningsoperation*. Detta begrepp står i centrum för denna studie och är en samlingsbeteckning på de handlingar som sändaren utför för att i något hänseende föra mottagaren ”bakom ljuset”. En plan för en vilseledningsoperation kan vara förhållandevis okomplicerad som t.ex. när en aktör genomför en propagandakampanj med hjälp av falska sakuppgifter på sin egen webbplats på Internet. I detta fall kan själva vilseledningsoperationen enkelt delas upp i två led. I det ena utformas propagandans budskap och i det andra förs denna information in på webbplatsen. I övrigt förlitar sig aktören på att de som ingår i målgruppen för operationen själva ska söka sig fram till dess webbplats och ta del av budskapen på denna.

Men en vilseledningsoperation kan också tänkas ha betydligt större komplexitet och vara betydligt mer resurskrävande. I princip kan en vilseledningsoperation inbegripa en lång räcka ”seriekopplade” element som till exempel förberedelser, konstruktionen av en mekanism för att åstadkomma påverkan (här kallad *ploj*), dennas verkställande, samt uppkomsten av vilseledningseffekter som leder till måluppfyllelse för aktören. Enskilda vilseledningsoperationer kan te sig mycket olikartade beroende på hur, och med vilka syften, som de genomförs. Också det valda sättet att ”föra en aktör bakom ljuset” påverkar hur en vilseled-

[18] Se Del V. Motåtgärder. Läs mer om källkritik på Internet i Leth och Thuréns ”Källkritik för Internet” (2000).

ningsoperation kan läggas upp och genomföras. I undersökningen används ”vilseledningsoperation” således som ett analytiskt begrepp. En vilseledningsoperation är helt enkelt en konstruktion som inkluderar olika element i den avsiktliga vilseledningen. Dessa element är: *sändare, syfte, underrättelser*[19], *meddelande, kommunikation, mottagare, effekt*.

Operationstekniker

Hur skulle Internet rent konkret kunna komma till användning i en vilseledningsoperation? Det är rimligt att anta att risken för att en aktör ska utsättas för framgångsrik vilseledning minskar ju säkrare dennes IT-system är mot intrång. Vilseledning på Internet förutsätter emellertid *inte* olovligt intrång. Ett antagande om att vilseledning förutsätter intrång skulle således kunna utesluta intressanta möjliga fall. Det är exempelvis möjligt för en aktör att manipulera information på en webbplats som denne själv förfogar över och som en tänkt mottagare för vilseledningen besöker helt och hållet på eget initiativ. En analys av vilseledning måste följaktligen läggas upp på ett sådant sätt att intrångsproblemet inte oreflekterat överskuggar andra aspekter. Analysen av fall kräver att vi finner samband mellan vilseledningsoperationens ploj och de ”verktyg” som Internet har för att genomföra dessa.

Framgången med en vilseledningsoperation beror på vad *plojen* (simulering eller dissimulering) kan åstadkomma. Plojen betingas av det konstruerade budskap – falskt eller sant – med vars hjälp sändaren vill påverka mottagarens föreställningar, attityder eller handlande. *Plojen är någonting mer än tillrättalagd eller förvrängd information*. Den bygger på en idé om hur en viss önskad reaktion av den tänkta mottagaren ska kunna tvingas eller lockas fram genom att denne får tillgång till tillrättalagd information.

Budskapet från sändaren utgör emellertid endast *en* del av plojen. Den andra komponenten är dess *presentation* för den tänkta mottagaren, som förutsätter någon slags kommunikation mellan sändare och mottagare. Här antas förstås Internet helt eller delvis kunna utnyttjas för detta ändamål. Kommunikationen mellan sändare och mottagare kan vara upplagd på varjehanda sätt och innebära olika typer av intervention i mottagarens användning av Internet. Sändaren kan exempelvis i vissa fall vilja förhindra att viss information som finns tillgänglig på Internet når fram till mottagaren och på så sätt kommer till dennes kännedom. En variation på detta är att sändaren vill utplåna eller avlägsna information som mottagaren redan förfogar över. Sändaren kan också vilja ge mottagaren tillgång till ny information eller i något hänseende ändra viss för mottagaren redan tillgänglig information.

Vilseledning på Internet bygger på att någon, eller några av följande operationstekniker används:

Blockering

Blockering kan innebära att sändaren gör ett intrång i mottagarens kommunikation med motparter på Internet i syfte att förhindra att viss information som mottagaren efterfrågar når fram till dennes datasystem. Olika tekniker kan användas för att åstadkomma en sådan blockering. Bortkoppling, d.v.s. att koppla bort ett system, ett delnät eller till och med ett helt land från resten av Internet – är kanske det tväraste sättet att blockera någon.

---

[19] Underrättelser är ofta svåra att få information om och bedöma i efterhand, men är sannolikt många gånger avgörande för vilseledningens utgång.

Ett delnät kan även koppla bort ett annat delnät genom att inte acceptera vissa avsändaradresser i den egna accessroutern. En annan möjlig ansats för sändaren är att fånga upp och avleda vissa meddelanden till mottagaren, till exempel e-mail från vissa avsändare. Ytterligare en metod kan vara att genom e-mailbombning under en viss tid begränsa mottagarens förmåga att ta emot information via Internet. DoS, som står för Denial of Service, kan beskrivas som en attack mot tjänst, system eller nät avsedd att hindra tjänstgöring. För att åstadkomma detta finns det olika metoder, däribland överbelastning av systemen genom e-mailbombning eller s.k. SYN Flooding. SYN Flooding är ett verktyg som skickar elektroniska ”paket” upprepade gånger till en mottagare för att fylla dennes ’lyssnartabell’ vilket gör att den inte längre kan ta emot någon ny information utifrån. Andra DoS är överbelastning med hjälp av ”förstärkare”. Genom att skicka för ”stora” brev (ping of death) kan man krascha mottagarens system. För inte så länge sen kom en ny sorts DoS; s.k. distribuerade DoS (DDoS). Syftet med distribuerade DoS är att dölja ursprunget till attacken. Exempelvis kan agenter placeras i hackade datorer (som i sin tur kan styras via styragenter) och initiera en attack (uppgifterna kommer från Rikskriminalpolisens konferens om IT-kriminalitet 22-23 februari 2000).[20]

Informationsupphämtning

En annan operationsteknik är informationsupphämtning. Sändaren går in i mottagarens datasystem i syfte att i hemlighet föra ut viss information från detta. Om sändaren har ett rent underrättelsesyfte kan han förväntas kopiera de eftersökta uppgifterna. Detta kan också göras genom avlyssning av datanät. Otillåten avlyssning sker oftast genom dataintrång i en nätansluten dator. I denna installeras sedan en programvara för nätavlyssning och lagring av data eller så sänds den avlyssnade trafiken vidare. Syftet kan vara att få tag på datoradresser, användaridentiteter eller lösenord för att ta sig vidare. Om emellertid målet är vilseledning är det möjligt att sändaren vill ändra eller radera viss information helt och hållet.

Sändning

Detta är en samlingsbeteckning på åtgärder som innebär att sändaren överför, eller låter överföra, viss tillrättalagd information till mottagaren.[21] Sändningen kan organiseras på olika sätt. Den kan vara öppen eller dold och den kan vara direkt eller indirekt mellan sändare och objekt. Kommunikationen är öppen, och således synlig för alla och envar när sändaren inte har anldning att dölja sin identitet. Ett exempel är när en krigförande part använder vilseledande uppgifter i sin öppna propaganda. Ofta får emellertid framgångsrik vilseledning antas förutsätta dold kommunikation från sändaren till mottagaren. Den indirekta kommunikationen är en teknik som kan användas för att uppnå detta syfte. Sändaren ger då intryck av att den utsända informationen kommer från någon annan än sändaren själv, t.ex. aktören B, vilken frivilligt eller ofrivilligt får fungera som mellanhand. Sändaren kan exempelvis manipulera sändaradressen på utsänd e-mail till mottagaren så att denne

---

20) Hackerattackerna mot Yahoo, eBay och Amazon.com är alla exempel på DoS-attacker. Enligt FBI bedömdes dessa DoS som några av de dittills allvarligaste attackerna mot Internet.

21) Det ska erinras om att vilseledning inte nödvändigtvis förutsätter kommunikation av falsk information, vilket traditionellt men oegentligt betecknas som desinformation. Även i sig korrekta sakuppgifter kan vilseleda genom sättet de presenteras på, genom tidpunkten när detta sker eller på grund av det yttre sammanhanget.

tror att de kommer från aktören B. Ett annat scenario är att sändaren gör intrång i mottagarens datasystem för att åstadkomma att så snart mottagaren söker efter aktören Bs webbplats når den i stället fram till en webbplats som i Bs namn är upprättad av vilseledningssändaren.

”Att lägga agn”

Denna metod kan komma till användning när operationens framgång förutsätter att mottagaren upplever sig själv ha funnit den information som sändarens ploj bygger på. Ett tillvägagångssätt kan vara att lägga in tillrättalagd, vilseledande information på en eller flera webbplatser på Internet, som mottagaren kan förväntas söka sig fram till. Denna metod är emellertid tekniskt krävande och förutsätter att två villkor uppfylls för att vara framgångsrik: (1) Sändaren måste kunna förutsäga vilka webbplatser som mottagaren kommer att uppsöka. En tänkbar metod är att utnyttja spårmaterial som avslöjar vilka webbplatser mottagaren återkommande besöker. Det är också möjligt för sändaren att i viss utsträckning kartlägga vilken slags information som mottagaren hämtar hem från de ofta besökta webbplatserna. En annan metod är att sändaren gör känt, t.ex. genom organiserad ryktesspridning, att information som mottagaren eftersöker finns tillgänglig på en viss angiven webbplats. Ett scenario är att denna ryktesspridning sker i en chatgrupp på Internet, i vilken mottagaren ofta deltar. (2) Sändaren måste kunna förfoga över den webbplats, som ska användas för att ”lägga agn”. Förfogandet kan ta sig flera uttryck; att sändaren särskilt skapar en webbplats för ändamålet; att en allierad aktör med lämplig webbplats utnyttjas; att sändaren genom intrång i hemlighet går in i någons annans webbplats.

Kommunikation genom interaktion

Med hjälp av flertal olika tekniker möjliggör Internet direkt och samtidig interaktion mellan två eller flera parter. Olika metoder representerar något annorlunda blandningar av möjligheter och begränsningar för en sändare som vill överföra tillrättalagd information till en tänkt mottagare i syfte att vilseleda denna.

Kommunikation med hjälp av e-mail liknar i stort konventionell brevväxling: två parter utbyter skriftliga meddelanden mellan sig med hjälp av ett oberoende transportsystem. Samtidigt finns det väsentliga olikheter mellan konventionell postgång och e-mail. Den höga hastigheten i kommunikationen innebär att e-mailinteraktionen kan få karaktär av en dialog, som mer liknar ett telefonsamtal än korrespondens. Två parter kan t.ex. under kort tid tillsammans utreda ett problem eller fatta ett beslut. Emellertid är kommunikation med e-mail i vissa hänseenden annorlunda än telefonsamtal. Det finns ett uttrymme för eftertanke, som är större än i ett telefonsamtal. Samtidigt innebär kravet på skriftliga formuleringar att kommunikationen blir mer arbetskrävande, vilket ökar sannolikheten för att meddelanden med e-mail blir korta. Detta förhållande kan dock kompenseras genom att olika slags dokument liksom bilder kan biläggas ett e-mail (bifogad fil, attachment). I en maildialog finns det goda möjligheter för en sändare att noga utforma ett meddelande som ska generera en vilseledningsploj.

På Internet finns en rad olika former för kommunikation genom interaktion (Häger & Strömblad 1998). Till exempel:

- *E-maillistor* som var och en hänför sig till ett särskilt ämne. De bygger på tekniken att kunna sända samma meddelande till många personer samtidigt. Kommunikation kan enbart ske med andra prenumeranter på en maillista. Varje deltagare har

en identitet. Enskilda deltagare kan med hjälp av filtreringsregler sortera bort sådana identiteter, som de finner vara ointressanta eller som den inte vill ha att göra med.

- *Usenet* fungerar i grunden på samma sätt som e-maillistorna fast med vissa viktiga undantag. Ett vanligt sätt att karaktärisera Usenet är Internets ”dynamiska anslagstavla”. Man måste aktivt titta i Usenet för att se inläggen. Vem som helst kan delta utan att en annan deltagare kan spåra detta. Öppen vildvuxen debatt kännetecknar Usenet. Det går att söka efter innehåll på Usenet, vilket inte går på e-maillistorna. Söktjänster för Usenet tillhandahålls genom sökmotorerna AltaVista och Deja News.

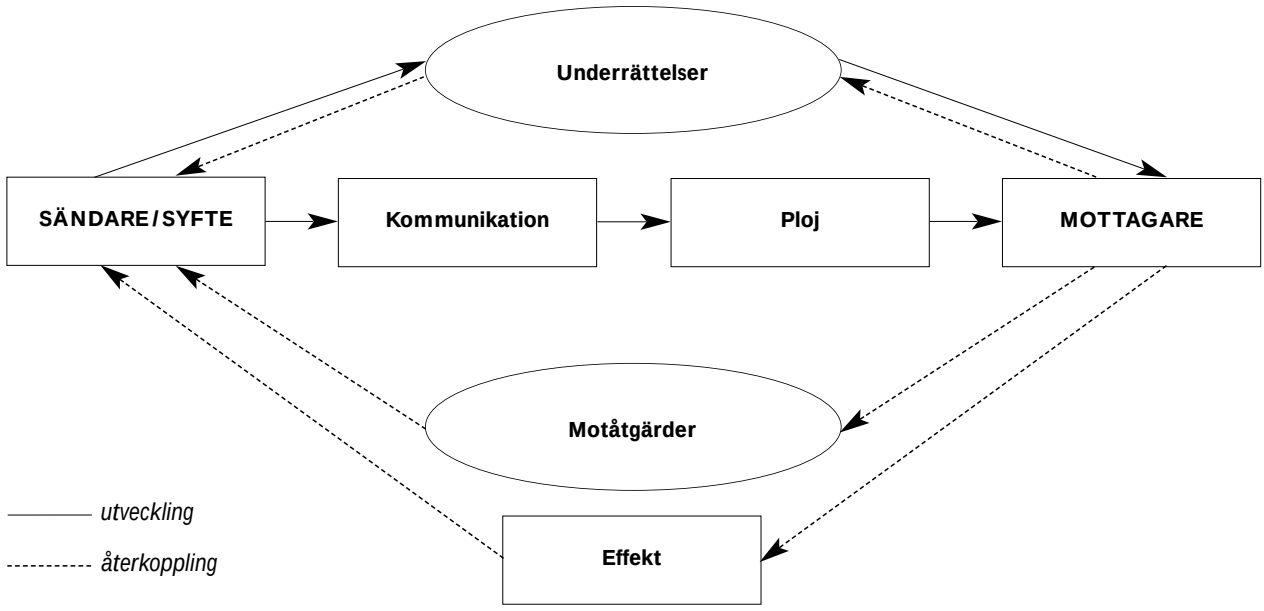
- *Internet Relay* (”chatting”) fungerar ungefär som Usenet. Den stora skillnden är att man under en chat hela tiden ser kommunikatinen rulla fram på sin dataskärm. En chat liknar mer än Usenet ett verkligt samtal. Interaktionen har i mycket karaktär av oreglerat tankeutbyte i en grupp av diskuterande människor.

- *Multi User Domain* (MUD) liknar mycket Internet Relay Chat. Skillnaden är att MUD skapar ett digitalt rum för deltagarna i vilket mycket strukturerad kommunikation kan äga rum. MUD lämpar sig exempelvis för ett informationsutbyte mellan vetenskapsmän/kvinnor.

Analysmodeller

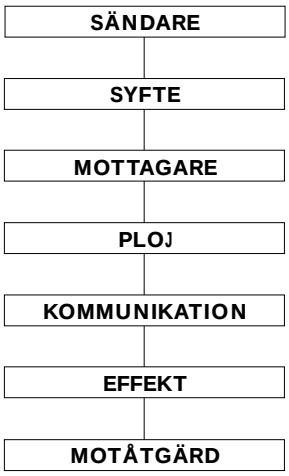
Vilseledning på Internet är som vi tidigare påpekat svårstuderat. I en analys av vilseledning på Internet är det t.ex. nödvändigt att mer systematiskt ta in aktörer och deras intressen och avsikter i analysen, än vad som är vanligt i säkerhetsinriktade analyser med syfte att begränsa risken för intrång. För att få bättre skärpa i bilden krävs således en särskilt anpassad analysmodell, vars konstruktion i sig är ett viktigt element i denna studie.

Begreppet *vilseledningsoperation* utgör här grunden för att systematiskt analysera och jämföra fall av vilseledning med hjälp av Internet. Uttryckt i teoretiska termer kan analysmodellen sammanfattas som i figur 2.



Figur 2. Teoretisk modell avseende vilseledning på Internet

För att denna modell ska kunna fungera som en konkret instruktion för analysen av enskilda fall av vilseledning på Internet behöver den uttryckas i mer operativa termer. En sådan ”översättning” har skett i figur 3, som anger en konkret mall för hur de fall som ingår i undersökningen ska analyseras. Denna analysplan följer vilseledningsoperationens element, med ett undantag: motåtgärder ingår förstås inte i en vilseledningsoperation.



Figur 3. Analysplan för vilseledning på Internet

I enlighet med våra utgångspunkter så tror vi att man genom att analysera verkliga incidenter (godartade fall) och generalisera om dessa kan göra en tentativ bedömning av andra fall (elakartade fall). I Del IV i denna skrift utvecklar vi fallen till mer generella typfall enligt analysmodellen nedan:

Figur 4. Fallanalysens logik

Typfallen utvecklas i sin tur till fiktiva fall av vilseledning på Internet som *skulle kunna* innebära hot för demokrati och säkerhet.

DEL III
FALL

Fallen är exempel på episoder där Internet har utnyttjats för att vilseleda en bestämd mottagare. Ett fall (”SAAB Gripen skyller på dåligt väder”) är exempel på vilseledning där Internet skulle kunna ha använts. Ett annat fall (”Hacktivism – Global Day of Action”) är exempel på hur Internet kan utnyttjas för att skapa opinion och organisera människor. Nedan beskrivs fallen kortfattat och finns ordnade efter vår analysplan för vilseledningsoperationer på Internet.

Under kategorin ”kommunikation” kan man t.ex. se vilken operationsteknik sändaren har använt sig av. Underrättelser finns dock inte med i fallbeskrivningarna eftersom data saknas om detta.

Fallen är identifierade utifrån olika typer av vilseledning: simulering (uppfinning, efterapning, avledande operation) och/eller dissimulering (kamouflering, förklädnad, ”omvärldsskuggning”).

Fall 1.

Pol Pot i Stockholm!

Sista juni 1997 levererade nyhetsbyrån TASS.Net ett hett scoop: Pol Pot befann sig i Sverige: ”Pol Pot was seen arriving to Arlanda airport outside Stockholm, Sweden, Monday, June 30”. På TASS.Net:Newswire fanns även en bildsekvens på hur Pol Pot togs emot på Arlanda av representanter från organisationen Komintern som i hemlighet förhandlat med svenska regeringen för att övertyga om hans flyktingstatus. På webbplatsen fanns även en bakgrundshistoria som beskrev den svenska traditionen att hålla sig neutrala och ge skydd åt politiskt oliktänkande och utstötta. Dagen därpå meddelade nyhetsbyrån att ”Pol Pot Reconfirms Presence in Stockholm, Sweden”. Här fanns inte bara en nyhetsartikel där Pol Pot dementerade ryktet om att hans exil var fejkad, utan också uppgifter om att UD inte kunnat dementera att Pol Pot befann sig i Sverige. På TASS.Net fick man även veta att ryska nyhetsbyrån Itar-TASS genom Reuter förnekat att de hade något med historien om Pol Pot att göra. Än idag finns TASS.Net:Newswire listad bland andra internationella nyhetsbyråer på nätet.

Typ av vilseledning: Simulering genom uppfinning (falsk nyhetsbyrå på nätet med påhittad nyhet). Simulering genom efterapning/dissimulering genom förklädnad (layout, namn och webbadress).

Sändare: Det svenska Internetföretaget Bahnhof.com.

Syfte: Att experimentera och se hur långt man kunde gå genom att lägga ut en påhittad nyhetsbyrå på nätet. Ett annat syfte kan ha varit att dra uppmärksamheten till ett relativt nystartat företag och skapa intresse för dess kommande verksamhet.

Mottagare: Nyhetsredaktioner, regeringar och organisationer världen över.

Ploj: Nyheten om att Pol Pot flytt till Stockholm med hjälp av organisationen Komintern.

Kommunikation: ”Lägga agn”. Falsk nyhetsbyrå på webben: Tass. Net .

Effekt: I stort sett avsedd effekt. Flera internationella medier tog upp nyheten i sin rapportering. Nyheten låg ute på Reuters telegramservice och dementerades först efter några timmar. Förvirring uppstod enligt utsago på Svenska UD och fallet fick efteråt stor uppmärksamhet i svenska medier. Svenska medier rapporterade dock inte händelsen som en nyhet. Istället blev vilseledningsoperationen en varningssignal för svenska journalister och är numera ett skolexempel på hur desinformation kan spridas över Internet.

Åtgärder: Inga direkta åtgärder från vare sig medier eller den svenska regeringen i den akuta fasen.

Kommentar: Hypotetiskt skulle en operation av detta slag kunna ha gjorts i politiskt eller ekonomiskt syfte, t.ex. för att störa förhandlingar mellan Sverige och USA i någon aktuell fråga.

Fall 2.

SAAB Gripen skyller på dåligt väder!

Finland funderade under en tid på att köpa svenska stridsflygplan (SAAB Gripen). Inför den finska provflygningen blev det plötsligt dåligt väder och man tvingades ställa in flygturen. Vid låga moln och dimma, som var fallet här, flyger man inte enligt svenska flygregler. Dessa regler känner alla flygtekniker till. Politiker däremot är mer ovetande om sådana regler, vilket en skandinavienkorrespondent från konkurrentlandet passade på att utnyttja. Snart fick nämligen vederbörandes kontaktnät på hög politisk nivå i Finland uppgifter om att svenskarna hade flygtekniska problem och att det var därför man inte flög. Ryktet spred sig och det tog inte lång tid innan det tjugotal personer som bestämmer i Finland kände till att det var tekniska orsaker och inte vädret, som svenskarna skyllde på, som förhindrat provflygningen. Av en ren händelse råkade en av de personer som korrespondenten kontaktade vara rådgivare till SAAB och på så sätt uppdagades historien. Enligt uppgift lämnad vid intervju var detta medveten vilseledning baserad på tekniska detaljer som sattes in i en krets av omedvetna människor. Kosekvenserna av denna vilseledningsoperation blev bl.a. att höga svenska militärer fick gå ut och noggrant redogöra för omständigheterna kring flygningen för att på bästa sätt försöka övertyga sin numera skeptiska kund om varför man inte hade kunna genomföra provflygningen. Det blev aldrig någon affär med Finland.

Typ av vilseledning: Simulering genom uppfinning; svartmålning av konkurrent i form av falska uppgifter.

Sändare: Utrikeskorrespondent, sannolikt på uppdrag från en konkurrent till SAAB (stat eller företag).

Syfte: Att förhindra finskt köp av svenska stridsflygplan.

Mottagare: Beslutsfattare i Finland.

Ploj: Uppgifter om att provflygning ställdes in p.g.a flygtekniska problem.

Kommunikation: Oviss (förmodligen genom korrespondentens personliga kontakter). Skulle kunna ha skett genom ”att lägga agn” eller genom kommunikation via interaktion (t.ex. e-mail).

Effekt: Det kan inte uteslutas att de finska beslutsfattarna tog intryck av desinformationen. Finland köpte aldrig några svenska stridsflygplan.

Åtgärder: I Sverige gjordes utredningar för att ta reda på vad som hänt och högt uppsatta militärer var tvungna att förklara situationen grundligt för de finska beslutsfattarna.

Kommentar: Fallet är ett intressant exempel på svartmålning med säkerhetspolitiska konsekvenser. När det här utspelade sig (1991-92) var Internet ingen naturlig väg att sprida information. Det finns heller inga säkra belägg för att Internet utnyttjades. Fallet indikerar dock hur Internet skulle kunna användas effektivt som instrument för vilseledning. Här skulle man via e-mail exempelvis ha kunnat framställa avsändaren som någon annan, alternativt skicka meddelandet till några väl utvalda personer som i sin tur sprider det vidare och därmed förstärker trovärdigheten i påståendet.

Fall 3.

"Hacktivism" – Global day of Action

Subject: Re: imf/worldbank spring meeting
Date: Tue, 01 Feb 2000-05-09
From: "Tricky Rudy"
To: "princess keri" /…/no2wto@listbot.com
At 10:43 PM 1/31/00-0800, princesskeri wrote:
No 2 WTO
Anyone know what is being planned for the Spring meeting of the IMF/World Bank in DC? I believe it is the week of April 20-28th...can't find any info regarding this on the net.../.../

Hi, princesskeri@:
IMF & World bank in Washington /April 16, 2000
Stand Again for Economic Justice! Oppose Oppressive Globalization!
A powerful U.S. movement for economic and human rights and fair trade had its coming-out party at the WTO meetings in Seattle. A range of forces to value human and ecological dignity over corporate profits and tickle-down economics came together there. We challenged one of the most insidious tools of unaccountable profit-driven rule, the World Trade Organization, and we scored an important series of victories against some daunting odds. In april the struggle continues in Washington, DC – the very heart of political and institutional control over the global economy: the U.S. Treasury, the International Monetary Fund (IMF) and the World Bank. /.../ Your presence in Washington is needed! /.../ Save the dates! Endorse the Call for Protests and Spread the Word! Start organizing – how many people can you bring to Washington?
Educate yourself and others about the IMF and World Bank! Visit www.50years.org for information!
For more information contact.../…/.

Bakgrund[22]: Vid några tillfällen under 1999 och 2000 skapade aktivister protester via nätet mot några av det kapitalistiska samhällets grundinstitutioner. Ovanstående e-mailutväxling är ett exempel på hur man har använt Internet för att sprida information, skapa opinion och samordna människor kring sitt budskap.

J18 – I juni 1999 varnades det världen över för en "Cyber Warfare Attack" som bland annat gick ut på att störa finansinstitut och multinationella företag genom hackerangrepp. Detta var en del av "J18", en internationell aktionsdag mot marknaden med anledning av G8-mötet i Köln den 18 juni 1999. De elektroniska

[22] Källor: Artiklar om aktionerna bl.a M2 Communications, London 18 juni 1999, Time 13 december 1999 "Rage against the machine" av Richard Lacayo, NIPC Watch 7 december 1999 och 2 februari 2000. (NIPC Watch är US National Infrastructure Protection Centers nyhetsorgan.) Som framgår av källornas datering togs fallet fram långt innan händelserna i Göteborg och Genua hade ägt rum.

attackerna (bl.a. spridandet av en e-mailmask) uppges ha åsamkat skador för hundratals miljoner dollar för de som drabbades.

No30 – Information om The Global Day of Action spreds över Internet, främst via e-maillistor och News Groups, för att samla till demonstration mot WTO-mötet i Seattle den 30 november 1999 (No30). Under WTO-mötet utbröt den då största protestdemonstrationen i USA sedan Vietnamkriget. Genomslaget kan delvis ha berott på den opinionsbildning och organisering som bedrivits på nätet.

A16 – Som en uppföljning av protesterna i Seattle organiserades en demonstration mot IMF och Världsbanken utanför IMFs högkvarter i Washington den 16 april 2000 (A16). E-mailmeddelandet ovan är ett exempel taget från ”NIPC Watch” den 2 februari 2000 vidarebefordrat från en medlem av The Mitre Infrastructure Assurance Support Team. I NIPCs kommentar till brevet nämns att man inte funnit några indikationer på att A16-gruppen planerade att genomföra nätverksattacker för att exempelvis stoppa informationsflödet (denial of service), göra dataintrång eller e-mailflooding. Däremot hade man via aktivisternas diskussionsgrupper vid denna tidpunkt funnit uppmaningar om ”electronic disobedience” (elektronisk olydnad).

Typ av vilseledning: Fallet innehåller ingen dokumenterad vilseledning, men kan användas för att se hur Internet kan utnyttjas för att mobilisera människor och skapa opinion.

Sändare: Organiserade aktivister, ideella organisationer m.fl.

Syfte: Att skapa opinion och protester mot den kapitalistiska världsordningen.

Mottagare: Världsopinionen, potentiella anhängare, medier och makthavare.

Meddelande: Fördjupa kunskapen om vad som styr den kapitalistiska världsordningen, skapa opinion och samla människor till aktiv protest.

Kommunikation: Kommunikation genom interaktion; News Groups och e-mail.

Effekt: Massmedial och politisk uppmärksamhet inernationellt men framförallt i USA. Demonstrationer världen över. Lokala demonstrationer i Seattle skapade förhinder i förhandlingarna som till sist avbröts och förlades på annan plats.

Åtgärder: Okända.

Kommentar: Observera att det här inte är något exempel på vilseledning via Internet, utan illustrerar hur effektiv kommunikation via Internet kan vara och hur nätet på detta sätt skulle kunna utnyttjas för att vilseleda.

Fall 4.

”Ensam, villig och billig!”

Försmådd ung man lade ut en falsk kontaktannons med e-mailadress och telefonnummer till f d flickvännen på nätet. Upp till 30 män hann kontakta kvinnan med snuskiga förslag innan det gick att spärra. Den unge mannen dömdes för grovt förtal.

Typ av vilseledning: Simulering genom uppfinning (falsk kontaktannons på nätet) och efterapning (utformandet och förmedlande av kontaktannons).

Sändare: F.d. pojkvän.

Syfte: Smutskasta och hämnas på f.d. flickvän.

Mottagare: Män som surfar på nätet.

Ploj: ”Ensam, villig och billig – Ung kvinna söker kontakt med män o.s.v.” samt uppgifter om adress, e-mail och telefonnummer.

Kommunikation: Dold, indirekt sändning genom kontaktannons på Internet.

Effekt: Integritetsbrott och förtal. Den berörda kvinnans e-mailadress, telefonnummer och hemadress blev offentliggjorda. Ca 30 män hörde av sig.

Åtgärder: Mannen spårades, åtalades och dömdes för grovt förtal.

Fall 5.

”Hej, det är Olle…”

En student lyckades uppträda som Olof Johansson i ett e-mail till Göran Persson rörande kärnkraftsfrågan.

Typ av vilseledning: Simulering genom uppfinning (innehållet i mailen) och efterapning (formulering). Dissimulering genom förklädnad (utgav sig för att vara Olof Johansson, f.d. centerpartiledare och känd kärnkraftsmotståndare).

Sändare: Student.

Syfte: Påverka politiska makthavare i kärnkraftsfrågan.

Mottagare: Statsminister Göran Persson.

Ploj: Ett, får man förmoda kontroversiellt, uttalande i kärnkraftsfrågan.

Kommunikation: Dold avsändare. Interaktion via e-mail.

Effekt: Missförstånd på Rosenbad.

Åtgärder: Okända.

Kommentar: Ett fejkat meddelande på Inga-Britt Ahlénius telefonsvarare orsakade närapå en regeringskris. Idag finns det möjlighet att skicka e-mail med påhittad avsändare. Fallet ger en idé om vad detta skulle kunna få för effekter.

Fall 6.

Tokyo Joe

En till New York invandrad korean som byggt upp en affärskedja på Manhattan, kallad Tokyo Joe, blev intresserad av aktieaffärer på nätet och gick med i en s.k. ”chatgroup” på Internet. Joe blev så småningom erkänd som en skicklig expert och började konsulteras av andra i sitt ”chatroom”. Detta utnyttjade Joe genom att själv inhandla billiga aktier och tipsa på nätet om att kursen skulle stiga. Han varnade dock för att sälja av för snabbt eftersom de förväntades stiga ytterligare. Tillräckligt många visade sig lyda Joes råd för att aktien verkligen skulle stiga. Men medan en stor del av köparna väntade på ytterliga höjningar, sålde Joe av sina aktier.[23]

Typ av vilseledning: Simulering genom uppfinning (tipset). Dissimulering genom förklädnad (utgav sig för att vara pålitlige ”Tokyo Joe”) och omvärldsskuggning (genom att komma med goda och insatta kommentarer och råd byggde Joe upp förtroende för sin person och smälte på samma gång in i sammanhanget).

Sändare: Tokyo Joe.

---

[23] Dagens Eko onsdagen 5 januari 2000, reporter Cecilia Udén, Washington.

Syfte: Tjäna pengar.

Mottagare: Potentiella aktieköpare som var aktiva på Joes chatgroup.

Ploj: ”Köp dessa aktier nu, de kommer att stiga mycket, så sälj inte för tidigt…”

Kommunikation: Öppen sändning, interaktion i diskussionsgrupp på Internet.

Effekt: Ökade köpet av aktier, kursen gick upp, Joe blev rik.

Åtgärder: Tokyo Joe spårades och åtalades så småningom.

Kommentar: Finans- och bankväsendet är högst IT-beroende och därmed känsligt för informationsstörningar. Med Internet har rykten fått en snabb och obegränsad väg att vandra.

Fall 7.

Säg nej till nazism och MC-gäng och ja till demokratin!

ALLA HAR VÄL LÄST TIDNINGEN IDAG ELLER SETT LÖPSEDLARNA!!!
På detta sätt vill vi visa vårt totala stöd för artiklarna och för de fyra chefredaktörerna; Anders Gerdin, Aftonbladet, Joachim Berner, Dagens Nyheter, Staffan Thorsell, Expressen, Mats Svegfors, Svenska Dagbladet.
När ni tar detta djärva grepp mot nazister och kriminella MC-gäng och publicerar dessa ”människor” med namn och bild, vill vi med detta cirkulationsmail uttala vårt fulla stöd för denna aktion. Tystnaden från vanliga människor är farlig, mycket farlig, men när;
- poliser i Malexander mördas
- poliser i Malmö utsätts för mordförsök, (bilbomben i Malmö)
- journalister utsätts för mordförsök, (bilbomb)
- folkkära artister som Sven Wollter och Mikael Wiehe mordhotas, MÅSTE VI/DU AGERA!
Din uppgift är att vidarebefordra detta mail till hela din privata adressbok och till hela ditt företag, din chef / VD / styrelseordförande lär inte ha något emot det.
Samtidigt med detta skall du sätta;
>> >> – anders.gerdin@aftonbladet.se
mailto:anders.gerdin@aftonbladet.se
>> >> – joachim.berner@dn.se
mailto:joachim.berner@dn.se
>> >> – staffan.thorsell@expressen.se
mailto:staffan.thorsell@expressen.se
>> >> – mats.svegfors@svd.se mailto:mats.svegfors@svd.se
som cc.....
DETTA ÄR MYCKET VIKTIGT för att det hela skall bli så offentligt som möjligt. I Sverige finns det mer än 5 miljoner människor som har tillgång till mail på något sätt. Syftet med detta utskick är att SAMTLIGA dessa 5 miljoner skall i slutet av denna vecka ha läst detta mail, och de fyra chefredaktörerna skall ha fått 5 miljoner mail var i sin mailbox. Målet är högt ställt men MED DIN HJÄLP KAN VI KLARA DET.....
>> >> SÄG NEJ TILL NAZISM OCH MC-GÄNG OCH JA TILL DEMOKRATIN!

Efter mailet följer en lång lista på namn och adresser på vilka som skickat vidare brevet, en del med kommentarer i stil med: ”Vidarebefordra till era vänner så vi skrämmer ner nassarna till de mörka hålen där de varken syns eller hörs”.

Typ av vilseledning: E-mailkedjebrev, sannolikt med syfte att åstadkomma e-mailbombning. Simulering i form av uppfinning. Dissimulering i form av förklädning (falsk avsändare) och omvärldsskuggning (frågan var aktuell och upprörde många).

Sändare: Osäkert eftersom inga seriösa efterforskningar har gjorts. Man anser det dock

belagt att det varit fråga om en planerad e-mailbombning. Man tror att kedjebrevet startades från en mindre grupp som andra sedan gjorde replay på. Tydligen pågick diskussioner på nätet om aktionen och det fanns indikationer på att något var på gång redan dagen innan. Tillgänglig information pekar på att sändaren (individ eller organisation) kan ha haft nynazistiska sympatier.

Syfte: Repressalier för artikelserien där man publicerade bilder och namn på svenska nynazister (förutsatt att den som startade kedjan hade nynazistiska sympatier och inte handlade i god tro).

Mottagare: Alla svenskar med e-mailadress.

Ploj: Upprop för att få människor att skicka e-mail till tidningarnas chefredaktörer.

Kommunikation: Dold sändare. Interaktion via e-mailkedjebrev. En form av ”att lägga agn”.

Effekt: Tidningarnas chefredaktörer blev överösta av e-mail (flera tusen mail i timmen under de första dagarna) och vissa tidningar fick problem med sina servrar. Dock inte tillräckligt stora för att man skulle anse det befogat att göra polisanmälan. Det finns uppgifter om att IT-avdelningen på Göteborgs kommun samt en enhet på Ericsson i Göteborg drabbades av virus i samband med dessa mail. Några uppgifter om virus i samband med e-mailbombningen har man inte förmedlat från tidningarna.

Åtgärder: Man agerade lite olika på de olika tidningarna. En åtgärd var att stänga ner chefredaktörernas e-mailadresser och inkommande e-mail styrdes bort från tidningarnas centrala mailservrar. Man gick även ut och vädjade till läsarna att sluta skicka e-mail. Enligt uppgift har säkerhetsavdelningen för de Bonnierägda tidningarna inte gjort några efterforskningar av ursprunget till kedjebrevet. Material i form av e-mail finns tillgängligt, men detta är såpass omfattande att man antagligen inte kommer försöka spåra ursprunget. Chansen att hitta något uppskattas som minimal. Någon polisanmälan gjordes heller aldrig.

Kommentar: Tidningarna strävar efter öppenhet och publicerar därför medarbetarnas e-mailadresser i artikelbylines etc. En sidoeffekt av detta är ökad sårbarhet i vissa fall. Enligt uppgifter från Bonniers IT-säkerhetsavdelning finns det idag inget man kan göra för att skydda sig mot denna typ av angrepp.

Fall 8.

Adolf Hitler – en av seklets viktigaster personer!

Hej
Har hört att naziorganisationer världen över har gått in för att Hitler ska vinna Times omröstning om århundradets viktigaste person. För närvarande ligger han på plats nummer tre. Jag tycker inte att en man som är ansvarig för miljoner människors död ska få en så ärofull titel som 1900-talets viktigaste person, så jag ber er att gå in på sidan och rösta på en annan person. Om ni trycker på Submit-knappen innan ni röstar så kan ni se den aktuella listan innan ni röstar.

Skicka gärna vidare detta mail!
> >/Catharina W.
www.pathfinder.com/time/time100/poc/century.html

Typ av vilseledning: Simulering genom uppfinning / dissimulering genom förklädnad. E-mailkedjebrev med uppmaning om att gå in på Times webbplats och rösta bort Hitler från

listan över århundradets viktigaste personer. Times omröstning gällde emellertid vem som hade gjort störst inverkan på historiens gång under 1900-talet. E-mailkedjebrevet tros ha varit ett nynazistiskt påhitt för att visa på Hitlers storhet och dra uppmärksamhet till listan.

Sändare: Förutsatt att det varit fråga om vilseledning så finns det två alternativa sändare: Uppgifter om att e-mailkedjebrevet kom från nynazistiskt håll har cirkulerat på nätet. Ett annat alternativ är att det var någon som missuppfattat syftet med Times lista och handlade i god tro för att förhindra att Hitler skulle hamna högst upp på listan. E-mailkedjebrevet skulle förstås kunna ha varit ett PR-knep från Times för att locka besökare till deras nätbilaga. Detta verkar dock inte särskilt troligt.

Syfte:
1)Att uppmärksamma att Hitler låg så långt upp på listan för att sprida föreställningen om att såpass många ansåg att Hitler varit den viktigaste personen under 1900-talet.
2) Att förhindra att Hitler hamnade långt upp på listan.
3) Att dra besökare till Times webbplats.

Mottagare: Så många som möjligt med e-mail.

Ploj: Att omröstningen handlade om 1900-talets viktigaste person och att Hitler av så pass många ansågs vara denna person.

Kommunikation: Interaktion via e-mailkedjebrev. En variant på ”att lägga agn”.

Effekt: Times webbplats fick förmodligen fler besökare.

Åtgärder: Okända.

Fall 9.

eBay saknar skydd mot intrång!

eBay var till för inte så länge sedan världens största webbplats för aktiehandel, när en man som utgav sig för att vara en white hacker[24] meddelade NY Times att han lyckats ta sig in i eBays datasystem där tusentals människors pengar (stora pengar!) cirkulerar varje dag. Detta visade sig i och för sig vara sant: eBay hade inte ens en brandvägg för sin server. Den vilseledande informationen i det här fallet är den goda hackern som troligen var inhyrd av en till eBay konkurrerande webbplats. NY Times publicerade uppgiften och aktierna på eBay gick i botten på en gång. Idag finns det ca fem webbplatser som är i samma storleksordning som eBay på aktiemarknaden.

Typ av vilseledning: Simulering genom uppfinning (skapande av falsk sändare – s.k. vit / god hacker).

Sändare: Hacker, förmodligen på uppdrag av en konkurrent, som utgav sig för att vara en white hacker.

Syfte: Att svartmåla eBay

Mottagare: Massmedier och eBays kunder

Ploj: ”eBay slarvar med kundernas säkerhet”

Kommunikation: Sändning. E-mail till tidning.

Effekt: eBays aktier gick ner och idag finns det ett flertal webbplatser för aktiehandel av samma storlek som eBay. Dessutom blev eBay snart ökända för sin dåliga säkerhet:
May 20, 1999, Thursday
NEWS WATCH; A Consultant Reports a Flaw In eBay's Web Site Security
Nothing lasts for long on eBay, the popular on-line

24) En s.k. ’white hacker’ är en hacker med goda avsikter.

auction house, except, apparently, potential security flaws. Tom Cervenka, a consultant in Edmonton, Alberta, recently found a bug that can redirect personal information –- including passwords – fr… By Tina Kelly

Åtgärder: Okända.

Fall 10.

3:a på Strandvägen lottas ut!

Subject: lycka inte till
Date: Mon, 13 Dec 1999 08:28:23 +0100
Vinn en trea på Strandvägen
Inför millennieskiftet firar Fastighetsbolaget Wihlborgs Fastigheter AB detta genom att lotta ut en trea på Strandvägen i Stockholm. Det enda du behöver göra är att skicka detta mail till tio bekanta samt att skicka ett mail till Wihlborgs Fastighet AB på: info@wihlborgs.se

Typ av vilseledning: Simulering genom uppfinning. I verkligheten hade förstås Wihlborgs Fastigheter AB inte alls några planer på att göra sig av med en våning (värd mer än 2 miljoner kronor) genom utlottning.

Syfte: Om vilseledning var avsiktlig kan syftet ha varit att störa Wihlborg Fastigheter AB:s arbete med e-mail och att ge företaget badwill.

Sändare: Okänd. En missnöjd kund? En f.d. anställd? En konkurrent? Det gick även rykten om att det var en anställd som ville skämta med en kompis.

Mottagare: Så många som möjligt med e-mailadress.

Ploj: Att Wihlborgs fastigheter AB lottar ut en trea på Strandvägen.

Kommunikation: Interaktion via e-mailutskick.

Effekt: Bad-will för företaget. Informationsansvariga fick extra arbete. När det aktuella datumet för utlottningen hade passerat (millennieskiftet) ebbade mail och förfrågningar så småningom ut.

Åtgärder: På Wihlborgs Fastigheter AB uppgav man att man inte visste något om ursprunget och uppmanade allmänhet och anställda att inte skicka mailet vidare. Man stängde ned servern tillfälligt för att undvika haveri, svarade på frågor från allmänheten som ville veta hur det gick med utlottningen och dementerade det falska påståendet. Enligt uppgift gjordes inga efterforskningar för att ta reda på vem som startat kedjan. Någon polisanmälan gjordes aldrig.

Fall 11.

200 Volvobilar lottas ut!

14 december 1999
Ämne: VB: vinn en bil
Prioritet: Hög
Hela denna sida är en marknadsföringsannons från Volvo Personvagnar AB

Hej
Bäste bilförare, vi på Volvo har under 99 lanserat våran hittills mest eftertraktade bil genom tiderna, nämligen Volvo S80. Enligt TEMOs undersökning om antal sålda personbilar i Sverige som publicerades i Motorbörsen i oktober månad har det sålts fler Volvo S80 än BMWs nya 525. Som en del av det nya milleniumet lottar vi på Volvo Personvagnar ut 200 stycken Volvo S80 med fri service i 2 år (värde ca: 350 000 kronor) den 31 december 1999. Det enda du behöver göra för att vara med i utlottningen är att vidarbefodra mejl till adressen: volvo@personvagnar.com. Lycka till önskar Per Lindström, marknadsföringsavdelningen Volvo personvagnar Märsta.

Mail: per_Lindstr mailto:Per_Lindström@volvo.net öm@volvo.net Lycka till!!!

Typ av vilseledning: Simulering genom uppfinning.

Syfte: Att störa arbetet och ge Volvo bad-will?

Sändare: Okänt. En missnöjd kund? En f.d. anställd? En konkurrent?

Mottagare: Så många som möjligt med e-mailadress.

Ploj: Vinn en bil!

Kommunikation: Sändning via e-mailutskick.

Effekt: Bad-will för Volvo?

Åtgärder: Okända.

Fall 12.

– Är det någon som har lite barnporr??

I USA användes vid ett tillfälle en privatpersons namn som avsändare på ett e-mail i vilket barnpornografiska bilder efterfrågades. Brevet spreds vidare och effekten blev omvänd mailbombning: upprörda mottagare skickade hot- och hatmail till avsändaren, vilkens datasystem kraschade.

Typ av vilseledning: Simulering genom uppfinning (försök till smutskastning). Dissimulering genom förklädnad / kamouflage (falsk avsändare).

Sändare: Okänt.

Syfte: Att skandalisera och trakassera.

Mottagare: En privatperson.

Ploj: ”Barnporr önskas”

Kommunikation: e-mail.

Effekt: Den avsedda mottagaren fick dåligt rykte och hans datasystem kraschade.

Åtgärder: Inga kända åtgärder.

Kommentar: När man tänker på e-mailbombning kanske man vanligen tänker på en enskild person eller organisation som skickar (för) stora mängder mail i syfte att protestera mot och störa den tänkta mottagarens verksamhet. Detta kan göras med enkla medel och är heller inget ovanligt. Det finns många kända fall av e-mailbombning.[25] Exemplen ovan visar hur man genom falska e-mailkedjebrev kan åstadkomma mailbombning i stor skala och på så sätt sprida bad-will om den man vill skada. Mailbombning kan vara mer eller mindre allvarligt och säkerheten mot sådana aktioner förbättras hela tiden. Fortfarande kan i princip vem som helst med enkla medel åsamka stor skada genom mailbombning. Mindre företag med mycket kundkontakter via e-mail kan till exempel drabbas hårt.

25) Några kända exempel på e-mailbombning: När fransmännen gjorde kärnvapenprov på Mururoa 1994 skickade hackers världen över tusentals protestmail tills marinbasens server i Toulon gick ner och telefonnätet, som då var integrerat, kopplades bort. 1997 fick en riksdagsman från Centerpartiet 300 likadana e-mail som han satte sig att svara på – bara för att få ännu fler identiska brev. I maj 1998 uppgav de amerikanska myndigheterna att de Tamilska tigrarna hade gett sig på Sri Lankas datasystem. Detta skedde bl.a. genom mailbombning. Mailbomb-attackerna mot Karolinska Institutet och Smittskyddsinstitutet i oktober 1998 fick stor medial uppmärksamhet. Djurens Befrielsefront tog på sig skulden. Detta var det första fallet av mailbombning som ledde till en polisanmälan i Sverige. Efter NATOs bombning av kinesiska ambassaden i Belgrad (maj 1999) angreps amerikanska regeringens datorer från vad man tror var kinesiskt håll. Bland annat så utsattes den amerikanska regeringen för kraftig mailbombning under 48 timmar.

Fall 13.

www.levandehistoria?

Sann historia – Levnadsöden

Mel Mermelstein, Elie Wiesel, Simon Wiesenthal, Rudolf Vrba, och Filip Müller har alla överlevt ”helvetet” på jorden som ”ögonvittnen” till gasningar i nazisternas koncentrationsläger under andra världskriget. Deras öden – som du kan följa på denna hemsida – ger en skakande bild av vad som kan hända när respekten för sanningen upphör och demokratin monteras ner. ”Förintelsen” är ett skrämmande bevis på vad som kan hända om vi inte håller debatten om sanning och lögn vid liv. Genom kunskap och diskussion kan vi motverka att något liknande händer igen.

Därför har vår aningslöse statsminister Göran Persson inte tagit initiativ till en bred informationsinsats om vår version av ”Förintelsen” för svenska skattepengar.

Typ av vilseledning: Simulering genom efterapning. (Plagiat av statsrådsberedningens projekt ”Levande historia” i form av en nästan exakt likadan webbplats, men där innehållet ifrågasätter Förintelsen.)

Sändare: Revisionister, som förnekar förintelsen av judar under andra världskriget, som agerar på nätet på webbplatsen www.levandehistoria.com under rubriken ”Sann historia”. Enligt webbplatsen är de 100% anti-kommunister och 100% anti-nazister. Man kan inte spåra webbplatsen till någon politisk eller annan organisation. Enligt en artikel i Dagens Nyheter (17 november 1998) kallade sig den som registrerat webbplatsen för Karl Svensson. Det fanns även ett telefonnummer angivet som gick till ett taxiföretag i Malmö, som dock dementerade samröre med den plagierade sidan. Det finns länkar på sidan till andra historieförnekare under rubriken ”Proffs”.

Syfte: Syftet med plagiatet är att dra uppmärksamhet till den egna historieskrivningen och undergräva det arbete som görs för att hålla minnet av Förintelsen levande. Detta görs främst i polemik med de fakta som presenteras på Levande Historias webbplats. Man vill på så sätt minska förtroendet för originalet, som för övrigt finns som länk under rubriken ”Bedragare”.

Mottagare: Potentiella besökare på www.levandehistoria.org, surfare på nätet, nynazistiska grupper, andra revisionister, m.fl.

Ploj: På webbplatsen presenteras uppgifter som motbevisar kända fakta om Förintelsen. I gult och blått presenteras en sida som kallas ”Sann historia” där uppgifter om gaskamrar, flygbilder, antal omkomna, vittnesuppgifter från överlevande etc. pekar på att bilden av Förintelsen som presenteras på Levande Historias webbplats inte stämmer med verkligheten.

Kommunikation: Webbplatsen i sig kan betraktas som öppen sändning. Sidans utformning och adress gör att de som söker levande historia lätt kommer till den plagierade webbplatsen, vilket liknar ”att lägga agn”.

Effekt: Det är svårt att säga vilken effekt vilseledningen fått.

Åtgärder: Plagiatet inleds numera med en förklarande text som skiljer plagiatet från originalet. Inga andra kända åtgärder.

Kommentar: Detta är ett exempel på hur man kan utnyttja en välkänd eller välrenommerad webbadress för att dra uppmärksamhet till sig själv och samtidigt svartmåla motståndaren.

Fall 14.

Hackers kapar webbplats!

Hackers Hit Nasdaq, Amex Web Sites
The Wall Street Journal 9-16-99
Washington – A group of computer hackers breached security and vandalized the Web sites of the Nasdaq Stock Market and the American Stock Exchange early yesterday, but officials of the markets said their extensive computerized trading networks were untouched. The hackers hijacked the Web sites early yesterday morning, writing a taunting message in the Nasdaq site's news section. Nasdaq technicians spent the morning reviewing the break-in. /…/ The hackers , who refer to themselves as the "United Loan Gunmen" have claimed responsibility for several high-profile Web-site defacements. /…/ The hackers' message on the Nasdaq site said their aim "was to attempt to make the stocks rise drastically, thus making all investors happy, hopefully ending with investors putting bumper stickers on their Mercedez' that say 'Thanks ULG!' Meanwhile, ULG members go back to flipping burgers at McDonald's.

Nasdaq is the world's second largest – and most automated – stock market. Its computer system allows stock dealers to execute instantaneous trades around the globe. But its Web site is a separate system, although millions of investors and market dealers use it to obtain news, stock quotes and to track investment portfolios. /…/ It is likely that the hackers are not out to cause serious damage, said Andy Meldrum, chief operating officer of Infrastructure Defense, "but the impact can be damaging , even if it's just a loss of public confidence." (END)

Typ av vilseledning: Simulering genom uppfinning; (intrång på webbplats och lämnat meddelande).

Sändare: Hackers som kallar sig "United Loan Gunmen".

Syfte: Maktuppvisning. Uttalat syfte: att få kursen att stiga och på så sätt göra investerarna lyckliga och få dem att sätta tack-ULG-klistermärken på sina Mercedes. Troligt syfte: att störa börsen genom att demonstrera intrånget.

Mottagare: Besökare på Nasdaq's och American Stock Exchanges webbplatser, samt media och allmänheten.

Ploj: Meddelande på Nasdaq's nyhetssida på nätet som säger att de är ansvariga för en massa intrång relaterade till aktiehandeln på nätet, samt att deras syfte är att göra aktieköparna rika…

Kommunikation: Dold sändning genom intrång och lämnat meddelande på Nasdaq's nyhetssida.

Effekt: Sannolikt tillfälligt minskat förtroende för Nasdaq's Internettjänster.

Åtgärder: Okända.

Kommentar: Det här är ett exempel på dataintrång där man manipulerat innehållet på en webbplats. I detta fall var det förmodligen tydligt för besökarna på Nasdaq's webbplats att det var fråga om ett intrång (en hack). Eftersom hackergruppen kapade webbplatsen – d.v.s. gjorde den otillgänglig för andra under den tid de opererade – kom det inlagda meddelandet förmodligen inte som någon överraskning. Nasdaq's säkerhetsansvariga sa sig inte heller bedöma hacken som speciellt allvarlig eftersom webbplatsen inte var relaterad till företagets nätverkshandel. Liknande operationer skulle dock kunna genomföras mer subtilt, i det fördolda, och ge upphov till verkliga problem.

Fall 15.

NATO ljuger!

www.serbia-info.com/news/1999-04/15/10898.html

Kosovo & Metohia
Unstoppable line of lies
April 15, 1999

Belgrade, April 14 (Tanjug) – As soon as they think that some, in a line of lies they are launching since they started their criminal aggression on Yugoslavia is beginning to get over-used, monsters from NATO invent a new one, with the intention to convince the world in the necessity of their action they – what an ironi – justify with humanitarian reasons.

The latest lie from "NATO kitchen" in Brussels, shot from the pens of dedicated western journalists, is that the Serbian security forces on Tuesday entered on Albanian territory, i.e. made aggression on a neighboring country. The news, of course, went around the world with the aim of amplifying vilification of Serbs, launching for several years, for accomplishing of their strategic goals in the Balkans. Those who have in the last three weeks been closely watching behaviour of the western aggressors could have expected such a "bomb", because NATO leadership needed a highly disturbing news for pushing from the focus terrible crimes they commited the day before. Precisely: the news about the alleged Serb aggression should have "deleated" the information about the list of civilian targets the aircraft of the alliance hit the day in witch they launched a journalist lie about forces entry into the "country of eagels". /…/ The mentioned list is long and shocking. NATO Bombs and missiles hit targets in the vicinity of teo big hospitals in Belgrade /…/, a factory in Krusevac, hotel on Kopaonik (!), bridge on the Rasina river, refinery in Pancevo (again), residental block in Novi Sad, several civilian facilities and residental buildnings all over Serbia. /…/When once, and that moment must come, made is a balance of media lies launched in the West on the occasion of aggression on Yugoslavia for its justification, it will be a big file of documents dishonor. /…/ Everything that happens still has some sense: dirty war needs dirty propaganda.

Typ av vilseledning: Simulering i form av efterapning (propaganda förklätt till nyheter).

Sändare: Serbiska informationsministeriet.

Syfte: Att svartmåla NATO och stärka den egna trovärdigheten.

Mottagare: Troligen så många som möjligt: serbiska befolkningen, inhemska opinionsbildare, nationell press, exiljugoslaver, världspressen, beslutsfattare och opinionsbildare i grannländer och resten av omvärlden.

Ploj: NATO ljuger och svartmålar serberna för att dölja sina egna illgärningar i syfte att nå sina strategiska mål på Balkan.

Kommunikation: Öppen sändning – Serbiska informationsministeriets webbplats (Serbian Information Ministry www.serbia-info.com.)

Effekt: Okänd.

Åtgärder: Okända.

Kommentar: Exemplet visar hur Internet kan användas, och används, för opinionspåverkan och propaganda. Propaganda kan förstås vara mer eller mindre vilseledande. Vi har inte gjort några efterforskningar för att bevisa eller motbevisa fakta i artikeln utan fallet får illustrera hur Internet skulle kunna användas i vilseledande syfte. Med Internets expansion ökar även medvetenheten om mediet. Det

serbiska informationsministeriets webbplats inger ett trovärdigt intryck och ser ut som en vanlig webbplats för nyheter: den har en snygg design, klassiska typsnitt och innehåller en huvudnyhet, notiser samt länkar till artiklar och andra webbplatser. I konflikter har nätet kommit att bli ett allt viktigare propagandainstrument. I Kosovokonflikten utnyttjades och uppmärksammades Internets genomslagskraft för första gången på allvar. Kriget har också kallats ”the first war on-line”.

Fall 16.

Internetbluff fick börskurs att rasa!

Klipp från Uppsnappat nr 370 – 29 augusti 2000.

Ett falskt pressmeddelande fick på fredagen det amerikanska fiberoptikbolaget Emulex börskurs att dyka med nära 20 miljarder kronor, motsvarande mer än 60%. I meddelandet, som publicerades av bland annat nyhetsbyrån Bloomberg News, fanns uppgifter om att bolagets VD hade avgått, att tidigare resultatrapporter varit felaktiga samt att den amerikanska börsmyndigheten inlett en granskning av bolaget. Detta fick börskursen att rasa från 103 till 45 dollar på 15 minuter. Den extrema kursnedgången gjorde marknaden nervös och också andra aktier inom samma bransch påverkades. Syftet med bedrägeriet kan ha varit att tjäna pengar på kursrörelsen. FBI och andra organ undersöker nu vilka som handlat med aktien. De falska uppgifterna verkar först ha publicerats av Internet Wire, en tjänst för att distribuera pressmeddelanden till nyhetsbyråer och webbplatser. [PW] http://www.emulex.com/

Typ av vileledning: Simulering genom uppfinning av falska uppgifter. Desinformation om företaget Emulex spreds som ett rykte på nätet.

Syfte: Att få aktierna i företaget Emulex att sjunka.

Sändare: Okänt. Skulle kunna vara aktieklippare, konkurrent eller en f.d. anställd som vill hämnas.

Mottagare: Aktieägare, aktiespekulanter, kunder m.fl.

Ploj: Falskt pressmeddelande som svartmålar Emulex.

Kommunikation: Eventuellt kommunikation genom interaktion. Dold sändning. Det är oklart var ryktet startat. Man tror att det först publicerades av Internet Wire, ett företag som förmedlar nyheter på nätet.

Effekt: Emulex börskurs dök med mer än 60 % inom loppet av en kvart.

Åtgärder: FBI granskning.

DEL IV
HOT

Finns det hotfulla höjder,
vatten med vass,
beväxta håligheter
eller dungar med kraftig undervegetation
/.../ måste dessa undersökas.
/Sun Zi

Vad är ett hot?

Den nationella säkerhetens ”hårda kärna” uppfattas alltjämt vara nationens fysiska överlevnad (*suveräniteten*). En annan dimension rör inskränkningar i förmågan att uppfylla särskilt viktiga nationella målsättningar, vilka kan hänföra sig till skilda områden som till exempel kulturen, skyddandet av miljön eller folkförsörjningen (*beslutsautonomi*).[26] Ovanför ett tröskelvärde, som knappast kan anges objektivt, innebär begränsningar i förmågan att fatta autonoma beslut i princip hot mot den nationella säkerheten. I praktiken växlar allvaret i hotbilden med frågornas vikt såsom dessa bedöms av ansvariga beslutsfattare. En grundläggande aspekt av den nationella autonomin är därför tryggandet av ett demokratiskt styrelseskick och dess förmåga att fungera normalt utan störning av illegala eller oetiska aktioner. *Det är framför allt genom att hota beslutsautonomin avseende för nationen viktiga frågor, som vilseledning på Internet kan antas kunna generera hot mot Sveriges nationella säkerhet*.

Hoten sammanhänger således med risken att någon aktör i Sverige ska utsättas för vilseledning, vilken får till konsekvens att svenska säkerhetsintressen åsidosätts. Häri ingår risken för störningar i den demokratiska processen.

Vi är väl medvetna om att det vi här betecknar som hot, förstås utgör möjligheter för den som vill påverka eller vilseleda. Detta förhållningssätt är säkert vanligt förekommande i t.ex. näringslivet. Detta påpekades också vid ett flertal tillfällen under intervjuerna.

Två ståndpunkter

Den jämförelse som gjorts av fallen har haft en renodlad explorativ inriktning, att ställa snarare än att empiriskt pröva hypoteser. Två grundläggande ståndpunkter utgör utgångspunkten för denna ansats.

---

[26] Försvagandet av nationens autonomi – och ytterst dess suveränitet – är en säkerhetsfråga endast så länge som denna utveckling sker i strid med de ansvariga beslutfattarnas vilja. Möjligheten av en militärt åstadkommen annektering till Nazityskland under 2:a Världskriget kunde i vida kretsar uppfattas som ett hot mot den nationella säkerheten. Denna situation ska jämföras med den troliga utvecklingen att Sverige allt mer kommer att integreras i den Europeiska Unionen. Detta scenario kan inte rimligen ses som en säkerhetspolitisk hotbild eftersom Sveriges medverkan i EUs integration bygger på beslut fattade av regering och riksdag.

Den ena är att vilseledningens förmåga att ge upphov till säkerhetspolitiska hot (dess ”farlighet”) i stor utsträckning sammanhänger med dess syfte, vem eller vad den riktar sig mot samt den faktiska effekten på mottagaren. I princip kan en enkel operation som sker med helt legala medel vara farligare ur nationell säkerhetssynpunkt än en stort upplagd operation som bygger på ett brottsligt och avancerat intrång i någons datasystem.

Den andra grundläggande observationen är att samma typ av operation – kombination av kommunikationsmönster och ploj – kan användas mot olika mottagare, i varjehanda situationer och för många olika syften. Detta betyder att vilseledningsoperationer är ”lömska” för såväl den som drabbas av dem som för analytikern som vill studera dem, eftersom de är svåra att upptäcka och att utvärdera. Denna ”lömskhet” förstärks av att en vilseledningsoperation i egenskap av instrument för påverkan är lätt att anpassa till olika yttre betingelser.

Fallen: En summering

Den analysplan som illustreras i figur 3 har använts för att göra en sammanställning av de studerade fallen.

Sändare

I de sexton fall av vilseledning som ovan beskrivits har sändaren inte alltid kunnat identifieras. Detta gäller bland annat i fallet om svartmålning av stridsflygplan (”SAAB Gripen skyller på dåligt väder!”), fallet rörande mobiliseringen av en stor opinionsrörelse (”Hacktivism – Global Day of Action”) liksom de fall där kedjebrev kommit till användning (t.ex. ”Säg nej till nazism och mc-gäng och ja till demokratin!”). Det kan dock konstateras att en rad olika typer av aktörer har uppträtt som sändare i de studerade fallen. I ett fall är sändaren en enskild person. Andra sändare kan identifieras som utrikeskorrespondent, ”hacker”- grupp, IT-företag, intresseorganisation och statlig myndighet.

Syfte

Vilseledningen i de 16 fallen har tjänat olika slag av syften. I ett fall (”Pol Pot i Stockholm!”) har sändaren troligen velat fästa uppmärksamheten på sig själv, *PR*. I ett annat fall har det varit fråga om ren *maktuppvisning* (”Hackers kapar webbplats!”). Också *propaganda/opinionsbildning* förekommer (”Hacktivism – Global Day of Action”, ”NATO ljuger!”). I andra fall är syftet att svartmåla (”eBay saknar skydd mot intrång”) eller att *skönmåla* (”Adolf Hitler – en av seklets viktigaste personer!”). Andra syften är *beslutspåverkan*; att förhindra ett visst beslut eller påverka beslutsfattare i en viss fråga (”SAAB Gripen skyller på dåligt väder!”, ”Hackers kapar webbplats!”), *vinning*; att tjäna pengar (”Tokyo Joe”) att *åstadkomma skandal/trakasser*a (”3:a på Strandvägen lottas ut!” samt ”Är det någon som har lite barnporr?”).

Mottagare

Även de aktörer som varit utsatta för vilseledningsoperation är av olika slag: enskild individ, en specifik grupp av människor (chatgrupp), viss del av befolkningen (de med e-mail), allmänna opinionen / allmänheten, redaktioner / massmedier; ett visst företags kunder, statliga tjänstemän samt i ett av fallen en representant för en regering. En iakttagelse är att i flera av fallen (t.ex. ”Säg nej till nazism och mc-gäng och ja till demokratin!” och ”ebay saknar skydd mot intrång!”) inriktar man sig på ett större antal aktörer exempelvis tidningsläsare eller kunder till ett speciellt företag. Förhoppningen är att dessa aktörers beteende i sin tur ska åstadkomma den avsedda effekten på den verkliga mottagaren för operationen. Exempelvis smutskastades en

viss produkt – ett flygplan – respektive ett företag genom information till kunder eller potentiella kunder. Kedjebrev genom e-mail och annons på Internet användes för att med hjälp av vilseledning störa och trakassera en individ eller ett företag.

Underrättelser

Källmaterialet rörande de sexton fallen saknar på det hela taget uppgifter om hur de olika vilseledningsoperationerna planerats och förberetts. Några observationer kan dock göras. I ett av fallen, det rörande manipulering av aktiekurser på Internet (”Tokyo Joe”), var den kommunikation som vilseledningen krävde interaktiv och innebar därför en löpande information till sändaren om mottagaren för operationen. Detta torde också ha gällt Seattle-fallet rörande storskalig mobilisering av opinionsrörelse (”Hacktivism – Global Day of Action”).

Vissa av fallen har en sådan uppläggning att de förutsätter tillgång till vissa slag av kvalificerad information. I ett fall (”SAAB Gripen skyller på dåligt väder!”) krävdes initierad information dels om förhandlingsläget i flygplansfrågan dels om vilka finska beslutsfattare som var inblandade i denna. Också i flera andra fall krävdes kvalificerad kunskap / information om mottagaren och dennes verksamheter (t.ex. ”eBay saknar skydd mot intrång!”). I detta fall, liksom flera andra, hade sannolikt vilseledningsoperationen till en del betingats av att sändaren från början var väl bekant med mottagaren (t.ex. ”Ensam, villig och billig!”). I åtminstone ett par fall krävdes ingen särskild informationsinhämtning därför att den genomförda operationen visserligen var en direkt reaktion på någon annan aktörs handling, till exempel publiceringen av en tidningsartikel, men i första ledet riktade sig till den breda allmänheten (t.ex. ”Säg nej till nazism och mc-gäng och ja till demokratin”, ”Adolf Hitler – en av seklets viktigaste personer!”). ”Pol Pot i Stockholm!” kräver kvalificerat vetande på IT-området. Däremot fordras det inte någon särskild information om någon mottagare eftersom den aktionen också vänder sig till allmänheten i sitt första led och i sitt andra avser att fästa uppmärksamheten på sändaren själv.

Ploj

Inget av fallen ger någon information om hur sändaren har planerat plojen eller tänkt hur denna ska fungera i den specifika vilseledningsoperationen. Fallen innehåller i allmänhet endast förhållandevis allmänna uppgifter om ett händelseförlopp, som endast indirekt visar vilken typ av ploj som använts. Trots detta har en del allmänna jämförelser kunnat göras mellan fallen med avseende på hur plojen konstruerats och fungerat.

Den använda plojen är genomgående förhållandevis okomplicerad även om den i de flesta fall bygger på en kombination av vilseledningens två grundtyper, simulering och dissimulering. I flera av fallen utnyttjas *dissimulering* för att på olika sätt hålla sändarens verkliga identitet hemlig. En metod är exempelvis att använda sig av ombud, vilket verkar ha skett i ”eBay saknar skydd mot intrång!”. Ett annat tillvägagångssätt är att ta någon annans identitet (”Ensam, villig och billig!”, ”Hej, det är Olle…” och ”Är det någon som har lite barnporr?”). En liknande ansats av dissimulering var något mer komplicerad och tekniskt krävande, nämligen att konstruera en falsk webbplats (”Pol Pot i Stockholm!”). Den vanligaste formen av dissimulering är emellertid att sändaren helt enkelt undvek att uppge sin identitet (t.ex. ”Säg nej till nazism och mc-gäng och ja till demokratin!”) eller presenterade sig med ett kodat namn (”Hackers kapar webbplats!”). Dold identitet genom dissimulering var i de

flesta fall ett nödvändigt men inte tillräckligt villkor för att uppnå en vilseledningseffekt på mottagaren.

I många fall skapades själva vilseledningseffekten genom *simulering*, varvid den vanligaste formen är kategorin *uppfinning* (fall 2, 6, 8, 9, 10, 11 och 12) eller en kombination av *uppfinning* och *efterapning* (fall 1, 4, 13 och 14). I ett par av fallen kombineras dissimulering och simulering så till vida att den falska identitet, vilken gavs åt sändaren utgjorde ett element i en uppfinning / efterapning (t.ex. ”Pol Pot i Stockholm!”).

Kommunikation och effekt

I jämförelsen mellan undersökningens 16 fall framstår kommunikationsmönstret mellan en operations sändare och mottagare som mycket varierat. Såväl direkt som indirekt kommunikation förekommer liksom både dataintrång och att ”lägga agn”. Den vanligaste kommunikationen kan beskrivas som direkt informationsöverföring till en eller flera utvalda mottagare, i de flesta fall med hjälp av e-mail (fall 2, 3, 5, 9, 10, 11 och 12). Kedjebrev med hjälp av e-mail representerar en teknik att överföra en viss information till ett så stort antal mottagare som möjligt (”Säg nej till nazism och MC-gägn och ja till demokratin” och ”Adolf Hitler – en av seklets viktigaste personer!”). Att lägga ut information på sin egen korrekta webbplats har en liknande målsättning och effekt (”NATO ljuger!”). I flera fall fördes falsk information ut på Internet genom simulerat medium (falsk webbplats respektive annons) för att där ”läggas som agn” (fall 1, 4 och 13). Övriga kommunikationsformer är interaktiv kommunikation på Internet (”Tokyo Joe”) och intrång i mottagarens datasystem (”Hackers kapar webbplats”).

I fallet ”Hej, det är Olle…” har syftet med vilseledningsoperationen med stor sannolikhet inte uppnåtts. I fyra fall (fall 2, 8, 11, 13 och 15) saknas möjligheter att bedöma effekten av vilseledningen utom på så sätt att uppnått syfte inte kan uteslutas. Avsedd effekt kan konstateras i övriga fall.

Alla analyserade fall representerar måttliga satsningar när det gäller förberedelser, omkostnader och risker för sändaren. Ändå verkar avsedd effekt ha uppnåtts i merparten av fallen. Operationerna har involverat ett flertal typer av aktörer i egenskap av såväl sändare som mottagare och har styrts av olika syften som PR, svart- och skönmålning olika slag av beslutspåverkan och trakasserier. Vilseledningseffekter har uppnåtts med ganska enkla medel. En rad olika kommunikationsformer har kommit till användning: direkt riktad information, att ”lägga agn” på Internet, kedjebrev med hjälp av e-mail, interaktiv kommunikation på Internet respektive intrång i datasystem för att ”injicera” tillrättalagd information. Fallen pekar i sig inte på att vilseledning på Internet skulle vara ett nationellt problem av säkerhetspolitisk dignitet. Men analysen utesluter samtidigt inte att de typer av vilseledning som förekommit i fallen skulle kunna få säkerhetspolitiska effekter med *andra aktörer, målsättningar och yttre kontexter*.

Typfall och scenarier

Genom att närmare studera de metoder för vilseledning som används i de sexton redovisade fallen har ett antal typfall med säkerhetspolitisk relevans kunnat konstrueras. Dessa har i vissa fall utvecklats till scenarier, vilka mer i detalj demonstrerar hur det *skulle kunna* gå till när vilseledningsoperationer får säkerhetspolitiska konsekvenser för Sverige. Detaljerna i scenarierna är *fiktiva* men mekaniken i de vilseledningsoperationer, som illustreras är härledda – dvs generaliserade – från de studerade fallen (se figur 4).

Sammanlagt presenteras tio typfall med tillhörande scenarier med säkerhetspolitisk relevans. Tre hänför sig till hot mot demokratin medan sju gäller hot mot den nationella yttre säkerheten.

Hot mot demokratin

Typfall 1.
Manipulering av opinion

Det första typfallet hänför sig till sådana situationer där hela, eller en viss del, av befolkningen i Sverige ska göra ett ställningstagande vars utfall får politiska konsekvenser. Typfallet innebär att denna process manipuleras med hjälp av en vilseledningsoperation. Typsituationen kan illustreras med hjälp av ett scenario.

Sakfrågan i scenariot är långtidslagring av radioaktivt avfall från svenska kärnkraftsanläggningar i Strålinge kommun. Den tekniska expertisen har föreslagit ett visst område som lämpligt för djupborrningar. Berggrunden och de allmänna förhållandena där anses vara gynnsamma för långtidslagring av kärnavfall. Opinionen i Strålinge är kluven. Vissa grupper stöder förslaget att kommunen ska upplåta mark för att ta hand om det farliga kärnavfallet medan andra argumenterar mot att så sker. De förstnämnda pekar på att lagringen är en avancerad affärsverksamhet, vilken kommer att skapa arbetstillfällen och dra investeringar och inkomster till kommunen. Motståndarna är emot allting som har med kärnkraft att göra. Många är rädda för att lagringen inte ska vara helt säker så att farlig strålning på något sätt ska släppas ut från lagren.

Motsättningen mellan de bägge lägren återspeglas inom flera av de politiska partierna, varför det fattas beslut att hålla en kommunal folkomröstning i frågan. Debatten i kommunen inför denna hålls till att börja med på ett mycket sakligt plan. Ja- och Nej-sidan kämpar mot varandra huvudsakligen med hjälp av korrekt sakinformation. Bägge sidor utnyttjar i stor utsträckning Internet för att sprida sitt budskap. Organisationer i respektive block uppmanar befolkningen i kommunen att studera deras webbplatser. Två dagar före folkomröstningen uppmärksammas en webbplats upprättad av en ny miljöorganisation, vilken bl.a. innehåller ett hemligstämplat dokument från Kärnkraftsinspektionen. Detta uppger att grundvattnet i den typ av berggrund, i vilken slutförvaringen av kärnavfall föreslås ske, för upp radioaktiva partiklar till jordytan i mycket större omfattning än vad tidigare varit känt. Dessa nya sakuppgifter sprids snabbt i kommunen. Spontana demonstrationer äger rum, i vilka myndigheterna anklagas för ”mörkning” av obekväma fakta. I omröstningen vinner nej-sidan. Det visar sig så småningom att dokumentet från Kärnkraftsinspektionen var förfalskat och att detta förts in på en privat internationell organisations (NGOs) webbplats av okända hackers.

Teknikerna för vilseledningsoperationen i detta scenario återfinns i åtminstone tre av de sexton studerade verkliga fallen. Ett element i operationens genomförande är således det tillfälliga skapandet, eller övertagandet, av webbplats, vilken uppfattas vara trovärdig (t.ex. ”Pol Pot i Stockholm!”). Ett annat inslag var tillhandahållandet av falsk information som mottagarna var mycket lyhörda för (”SAAB Gripen skyller på dåligt väder!”). Slutligen förekommer i scenariot också tekniker för att med hjälp av Internet påverka många människor samtidigt (”Hacktivism – Global Day of Action”).

Typfall 2.
Svartmålning

Ett avgörande element i den demokratiska processen är val av personer som ska fatta beslut ”på folkets vägnar”. Om valet av representanter på något sätt avsiktligt och på ett

långtgående sätt manipuleras utgör detta ett beaktansvärt hot mot hela den demokratiska processen. Detta typfall representerar en sådan hotbild.

Scenario: Ett riksdagsval i Sverige närmar sig. De större och etablerade politiska partierna arbetar med att få fram sina kandidatlistor genom t.ex. provval eller andra konsultationer inom det egna partiet. Vid denna tidpunkt uppmärksammas inom X-partiet en webbplats, som hänför sig till en nybildad internationell organisation för jämställdhet. På webbplatsen listas namnen på ett stort antal personer från olika länder, vilka i Thailand avslöjats som pedofiler utan att nödvändigtvis ha dömts i domstol. Ett förhållandevis ovanligt namn återfinns på listan vilket är det samma som namnet på en av riksdagskandidaterna i X-partiet. Denne är känd för sina många resor till Sydostasien. Namnet förs inte upp på X-partiets kandidatlista.

Detta typfall är förhållandevis starkt förankrat i fallstudierna. Flera av dessa handlar om hur en person eller organisation på litet olika sätt svartmålas (”Ensam, villig och billig!”, ”eBay saknar skydd mot intrång!”, ”3:a på Strandvägen lottas ut!”, ”200 Volvobilar lottas ut!”, ”Är det någon som har lite barnporr?”). Dessa fall ger en indikation på den stora variation, med vilken svartmålning kan genomföras.

Typfall 3.
Begränsning av opinionsbildningen

”Det fria ordet” utgör en av grundförutsättningarna för att den demokratiska processen ska kunna fungera på ett tillfredsställande sätt. Ett typfall av hot mot demokratin, som nedan ska illustreras med ett scenario, är någon form av intervention i opinionsbildningen som leder till att det fria ordet på något sätt blir begränsat.

Scenario: En offentlig debatt pågår internationellt liksom i Sverige om i vilken utsträckning genforskning behöver regleras och kontrolleras av statsmakterna. Diskussionen gäller särskilt vad som är etiskt försvarbart beträffande forskning rörande stamceller från människor. Frågan är naturligtvis mycket kontroversiell. Speciellt vissa religiösa grupper har uttryckt starka invändningar mot genforskning överhuvudtaget. Debatten har delvis ägt rum i massmedierna. Flera inlägg i frågan har gjorts på de större morgontidningrnas debattsida, men framför allt har Internet kommit till användning för att framföra åsikter och för att presentera fakta.

En av huvudpersonerna i debatten är professor NN som är ordförande i Universitetssjukhusets etiska nämnd och som försvarar forskning med användande av stamceller. Professor NN har blivit en huvudperson i debatten inte bara på grund av sin faktakunskap om det komplicerade problemområdet utan också därför att han kan formulera sina ståndpunkter på ett enkelt och tydligt sätt. Emellertid får professor NN plötsligt svårigheter att fortsätta delta i debatten. Dels utsätts han för en omfattande ”mailbombning” som hindrar användning av e-mailen som kommunikationsmedel. Dels förekommer plötsligt en rad extrema synpunkter på den webbplats där Universitetssjukhuset informerar om sin forskning om stamceller. Dessa uppgifter tas bort från webbplatsen med en förklaring om att ingen vet hur de hamnat där. Men skadan är skedd: professor NN har förlorat sin trovärdighet i debatten.

De tekniker som används i typfallet för att åstadkomma vilseledning återfinns i de studerade verkliga fallen. Hit hör skapandet av en webbplats, eller det tillfälliga övertagandet av en sådan (”Pol Pot i Stockholm!”). Också andra viktiga åtgärder är belysta i de studerade fallen, till exempel användningen av

”mail-bombing” (”Säg nej till nazism och mc-gäng och ja till demokratin!” och ”Adolf Hitler – en av seklets viktigaste personer!”).

Hot mot den nationella yttre säkerheten

Yttre hot mot den nationella säkerheten innebär i denna analys huvudsakligen att beslutsfattare i Sverige, vilka arbetar med säkerhetspolitiska frågor, möter restriktioner av olika slag när de vill göra sådana val som de egentligen föredrar. Dessa inskränkningar uppstår genom avsiktlig vilseledning med hjälp av Internet. Antingen luras beslutsfattaren att avstå från att försöka uppnå ett visst handlingsalternativ eller så skapar vilseledaren yttre hinder som blockerar detta, exempelvis i form av en opinionsstorm.

Typfall 4.
Manipulering av demonstrationer och andra opinionsyttringar

Flera av de sexton fall som analyserats visar hur Internet nyttjats som ett instrument för opinionsbildning i såväl liten som stor skala. Internet användes exempelvis för att mobilisera deltagare till demonstrationerna mot Världshandelsorganisationens (World Trade Organization, WTO) möte i Seattle i december 1999 (”Hacktivism” – Global day of Action”). Det finns dock inga belägg för att vilseledning användes just i det sammanhanget. Seattle-fallet pekar emellertid på en möjlig hotbild där en grupp välorganiserade aktivister systematiskt använder Internet i syfte att åstadkomma en opinion för att motverka – eller stödja – en viss organisation eller ett särskilt politiskt program.

De studerade fallen pekar på en rad möjligheter som en vilseledningsoperatör skulle kunna använda sig av för att driva den internationella opinionsbildningen i önskad riktning till exempel med hjälp av ”chatgrupper” (”Tokyo Joe”). Vilseledningen skulle exempelvis kunna bestå av små inslag av svårupptäckt desinformation (svart- eller skönmålning av t.ex. en institution eller en handlingsplan) i ett omfattande informationsmaterial, som sänds ut till en mängd adressater. Internet möjliggör att sanna såväl som falska uppgifter, vinklade eller missvisande kommentarer etc, kan differentieras mellan olika målgrupper. I en opinionsrörelse riktad mot WTO skulle till exempel personer med kända intressen eller ståndpunkter (kanske indikerade genom medverkan i någon NGO) för en viss sakfråga som miljöproblem eller mänskliga rättigheter få delvis annorlunda informationsmaterial. En sådan differentiering av den tillrättalagda, utsända informationen skulle kunna multiplicera effektiviteten i en vilseledningsoperation, vilken åsyftar en omfattande mobilisering av intressegrupper på nationell eller internationell nivå.

En bedömning är att Internet bidrar till att stärka den demokratiska processen när det används för att underlätta opinionsbildning (”Hacktivism’ – Global day of Action”). En hotbild kan emellertid också uppstå när Internet bidrar till att driva fram en opinionsbildning på falska premisser, t.ex. felaktiga sakuppgifter som avsiktligt förs ut i en krets människor, säg, i en ideell förening. Det eventuella hotet skulle kunna sammanhänga med själva karaktären på en demonstration som organiserats med bl.a. hjälp av Internet. Ett syfte med en stor politisk demonstration kan således vara att orsaka spänningar och instabilitet i samhället snarare än att bidraga konstruktivt till opinionsbildningen genom synpunkter eller fakta. Ett sätt att orsaka instabilitet kan vara att med hjälp av vilseledning provocera fram våldsamheter i en stor demonstration. I så fall utgör vilseledningen inte bara ett störande inslag i den demokratiska processen utan kan också bidra till att ge

upphov till yttre hot i en mer traditionell mening.

Typfall 5.
Manipulering av opinionsbildning utanför massmedierna

Internet kan användas för att under kort tid påverka en stor mängd människor att med konkret handling visa en attityd, eller hävda en uppfattning, i en konkret fråga, vid ett givet tillfälle eller i en viss situation. Några av de sexton fallen visar hur ett betydande antal personer förmåtts att medverka till att ”mailbomba” en viss organisation, t.ex. en tidning, för att på detta sätt genomföra någon slags individuell demonstration (t.ex. ”Säg nej till nazism och mc-gäng och ja till demokratin!”). Detta pekar på möjligheten för en sändare att på kort tid åstadkomma en omfattande opinionsbildning i en viss fråga, bl.a. i form av aktioner på Internet. Med andra ord kan Internet fungera som en hel kontext för vilseledande opinionsbildning. Säkerhetshot kommer att uppstå om vilseledningsoperationen framgångsrikt tjänar ett omstörtande syfte.

Typfall 6.
Påverkan av debatten i massmedierna

Internet har blivit en viktig informationskälla inom journalistiken. Fallet ”Pol Pot i Stockholm!” visar att det är möjligt att på ett enkelt sätt få falska sakuppgifter accepterade i massmediernas nyhetsrapportering om de bara framstår som tillräckligt intressanta. Pol Pot-fallet fungerar som en varningssignal. Den missbedömning som gjordes i medierna var inte ett banalt olycksfall i arbetet. Det var resultatet av en avsiktlig, om än förhållandevis enkel, men ändå framgångsrik vilseledningsoperation. Denna hade ett klart syfte, nämligen att skapa den falska bilden av Pol Pot på svensk jord, kanske på väg mot en överenskommelse med svenska myndigheter om politisk asyl. Detta sätt att föra ut falsk information i massmedia hade mycket väl kunnat vara inriktat på att uppnå effekter med säkerhetspolitisk innebörd, t.ex. att förhindra svensk vapenexport eller att undanröja möjligheten att en viss politiker med stor erfarenhet av säkerhetspolitik blir utnämnd till försvarsminister. Internet skulle även kunna bidraga till att i betydande grad effektivisera spridningen av tillrättalagd information motsvarande de falska uppgifterna om Pol Pot.

Typfall 7.
Missledande propaganda på webben

I ett krig söker de inblandade parterna föra ut sin syn på konflikten till omvärlden så mycket som möjligt. Därvidlag används olika medel som t.ex. regeringsstyrda tidningar eller radio- och tv-sändningar. På senare tid har webbplatser på Internet blivit ytterligare ett sådant möjligt propagandainstrument, med vars hjälp en part i en konflikt kan prisa sina egna goda motiv eller peka ut motpartens oacceptabla egenskaper och handlingar (”NATO ljuger!”). Den information som torgförs på detta sätt i en regerings propaganda innehåller inte sällan falska eller missvisande uppgifter. Webbplatser är lätt hanterbara redskap för denna typ av vilseledning (”Pol Pot i Stockholm!”). När den ifrågavarande konflikten äger rum i ett isolerat område med flera parter inblandade och samtidigt är betingad av komplicerade och svårkontrollerade sakfrågor skapas ett särskilt stort utrymme för falska uppgifter. De mångåriga krigen och icke-militära konflikterna på Balkan tillhandahåller goda exempel på detta. Flera av de fall som studerats i denna undersökning handlar om vilseledning, som bygger på svartmålning med hjälp av Internet (”Ensam, villig och billig!”, ”eBay saknar skydd mot intrång!” och ”3:a på Strandvägen lottas ut!”).

Typfall 8.
"Den förvanskade identitetens propaganda"

I vad som skulle kunna kallas en öppen propagandaoperation med hjälp av Internet argumenterar en sändare ofta på sin egen webbplats. Detta skulle kunna ske med hjälp av helt eller delvis felaktiga sakuppgifter. Det finns också indikationer på att en aktör i t.ex. en allvarlig konflikt kan försöka öka genomslagskraften i en propagandaoperation genom att låtsas att den framförda argumentationen härrör från någon annan ("Pol Pot i Stockholm!"). En teknik kan vara att konstruera hela webbplatser som ger intryck av att hänföra sig till en viss aktör, t.ex. en regering eller en viss organisation.

En annan metod är att genom ett dolt "hacker-angrepp" tillfälligt deponera viss information på en annan, respekterad aktörs webbplats. Aktioner av detta slag kan få säkerhetspolitisk innebörd och dignitet om de t.ex. är inriktade på att påverka ett säkerhetspolitiskt beslut eller dess genomförande, t.ex. vissa omstruktureringar av det militära försvaret eller visst försvarssamarbete med andra länder ("SAAB Gripen skyller på dåligt väder!").

Typfall 9.
Maskering av förberedd terror- eller sabotageverksamhet

För att mobilisera och leda en global opinionsrörelse liknande den i Seattle 1999 krävs en omfattande kommunikation. För att kunna realisera sina intentioner behöver denna kommunikation organiseras så ändamålsenligt som möjligt, vilket kan komma att fordra tidiga förberedelser långt innan en aktion genomförs. I en, som i det här fallet, normal och fullständigt legitim operation är det oproblematiskt, rent av fördelaktigt, om dess inledande förberedelser är fullt synliga och till exempel uppmärksammas i medierna. Förberedelsearbetet i sig kan ju ha en positiv effekt på den opinion som ska påverkas. Internet kan utnyttjas för att sprida information om hur en kampanj mot, säg, WTO, håller på att byggas upp. Det kan exempelvis göras allmänt känt (bl.a. med hjälp av e-mail) att information om kampanjen och dess syften finns tillgänglig på vissa webbplatser. På så sätt kan förberedelserna bidraga till att öka deltagandet i en kampanj, som håller på att inledas. I sådana fall där en opinionskampanj med många tänkta deltagare innehåller olagliga inslag har dock ledarna för operationen anledning att försöka dölja förberedelsearbetet. Detta gäller naturligtvis särskilt terror- eller sabotageaktioner. För att dessa ska kunna genomföras på ett avsett sätt, vilket empelvis kan innebära samordning mellan verksamheter, som pågår samtidigt i flera länder, kan ett effektivt kommunikations- och informationssystem behöva konstrueras i förväg. Internet inrymmer för det första möjligheten att göra detta på ett tekniskt tillfredsställande sätt. För det andra möjliggör Internettekniken att dessa förberedelser vid behov kan döljas. Det går att skapa helt osynliga webbplatser, som "normala" surfare på nätet aldrig kan ta sig fram till men som invigda omedelbart kan nå.

Typfall 10.
Påverkan genom interaktiv kommunikation

I fallet med "Tokyo Joe" vilsefördes många individer genom att de blev invecklade i en diskussion om aktieplaceringar i en "chatgrupp" på Internet. I chatgruppen fick de vilsefördа personerna inte bara allmän information om hur olika aktiekurser utvecklade sig. Genom de bedömningar som gjordes av andra kompetenta personer i gruppen, vilka betraktades som tillförlitliga, (t.ex. Tokyo Joe själv) tillförsäkrade sig åtminstone vissa deltagare i chatgruppen råd avseende köp av

aktier. Uppenbarligen var själva interaktionen inom chatgruppen av stor betydelse för att vilseledningen skulle lyckas. Informationsutbytet mellan deltagarna skapade en kontext av fri diskussion som verkar ha bidragit till att ge Tokyo Joes roll som rådgivare tillräcklig auktoritet och legitimitet för att ha inflytande på andra medlemmar av chatgruppen.

En av de hotbilder som fallet med Tokyo Joe indikerar är möjligheten för en aktör att inom ramen för en återkommande interaktion på Internet definiera en roll, för att i en framtida situation missbruka andras tilltro till denna. Ett exempel kunde vara en ”inflytandeagent” för en främmande makt som agerar på detta sätt i en diskussionsklubb för säkerhetspolitiska experter med inflytande på sitt lands politik.

Sammanfattning

De sexton verkliga fall som studerats i denna undersökning illustrerar vilken potential vilseledning via Internet skulle kunna ha som politiskt instrument. Jämförelserna mellan fallen påvisar variationsrikedom med avseende på såväl mål som tekniker. Möjligheten måste därför beaktas att vilseledning med hjälp av Internet skulle kunna utnyttjas av någon aktör på ett sådant sätt att hot uppstår mot den svenska nationella säkerheten. De tio generaliserade typfall som skisserats avser att illustrera några av dessa möjligheter. De enskilda detaljerna i scenarierna är förstås fiktiva. Men de operationstekniker som använts har stark verklighetsanknytning eftersom de identifierats i något av de sexton verkliga fallen.

DEL V
MÖJLIGA MOTÅTGÄRDER

The Greatest Challenge for the Information Age Manager
is to Create an Organisation that can Share Knowledge
/Thomas Steward, Intellectual Capital: The New Wealth of Organizations.

Att mota Olle i grind

Om vilseledning på Internet skulle kunna innebära ett problem eller, i allvarliga fall, till och med utgöra ett hot mot demokrati och säkerhet så måste man förstås fråga vad man skall göra för att minska dessa risker. Men det allra första man kanske borde fråga är vad man *kan* göra. Vi har yttrandefrihet och opinionsfrihet och det är inte förbjudet att vare sig ljuga eller luras i Sverige. Press- och etermedierna är fortfarande de huvudsakliga kanalerna för information till allmänheten. Förutom public-serviceuppdraget så finns pressetiska regler som är till för att motverka publicering av alltför vidlyftiga uppgifter. Med Internet har det emellertid blivit möjligt för vem som helst att snabbt sprida sina idéer och budskap till en bred publik. I totalitära stater kämpar man ständigt med att styra innehållet på Internet.[27] I en demokrati som Sverige kan man självklart inte förbjuda eller censurera propagandaspäckade webbplatser bara för att de innehåller vinklade eller felaktiga uppgifter. Syftet med motåtgärder kan istället beskrivas som att ”mota Olle i grind”. Det handlar om att föregripa och minska mottagarens känslighet för vilseledning.

Olika perspektiv

IT-säkerhet och skydd mot riktade informationsattacker kan indelas i följande fyra kategorier: långsiktiga och kortsiktiga respektive allmänna och riktade åtgärder. Man kan också diskutera åtgärder utifrån olika Internetanvändares perspektiv; lösningarna ser inte likadana ut för alla tänkbara mottagare. Man kan se två motsatta trender som IT-utvecklingen satt igång: ett ökat oberoende för den enskilde och samtidigt ett ökat beroende mellan olika sektorer i samhället; till exempel mellan privat och offentligt. Därför finns det en poäng med att inte göra någon strikt uppdelning mellan tänkta mottagare när man skall studera motåtgärder. För att bedöma behov och lämplighet av motåtgärder behövs ett tillförlitligt underlag, och här finns det brister i egentligen alla led av en analys: från svårigheter med att identifiera och samla in statistik över incidenter (”threat assessment”), värdera dessa för att skapa en samlad, nyanserad hotbild – till lagar

[27] I Kina har exempelvis flera åtgärder vidtagits för att skärpa kontrollen. Senast var det Folkets Dagblad som ertappades: alla webbsidor som de publicerar måste numera genomgå säkerhetskontroller för att ”hindra läckor av statshemligheter”. (Med statshemligheter avses i Kina all information som inte godkänts för publicering.)

och ansvarsförhållanden. Incidentrapporter innehåller sällan information om, och i så fall vilka, åtgärder som vidtagits efter det att vilseledningen upptäckts. Även i beskrivningen av enskilda fall saknas information om hur man har agerat för att förebygga vilseledning. Det saknas alltså ett gott underlag för att bedöma vilka motmedel som är lämpligast eller mest effektiva i olika specifika situationer. Det är knappast heller värdefullt att försöka sätta upp generella formler eller detaljerade rekommendationer för skydd. Däremot kan man diskutera *olika former* av motåtgärder.

I debatten kring skydd av infrastruktur och viktiga informationssystem kan man identifiera tre återkommande teman: *informationssäkerhet, ansvar och samarbete samt kunskapsuppbyggnad*. Dessa teman är relevanta även i diskussionen om hur man bäst skyddar sig mot vilseledning på Internet.

Informationssäkerhet

Informationssäkerhet avser generellt att säkra information och informationssystem från olovliga intrång. Detta är förstås en viktig åtgärd för att stå emot den typ av vilseledning som bygger på att vilseledaren olovligen tar sig in i mottagarens system. Kryptering, signering och brandväggar är vanliga former av IT-skydd. Anti-virusprogram, att tillfälligt stänga viss trafik i brandväggar eller bortkoppling är andra metoder. I förebyggande syfte kan man göra auktoriserade intrångsförsök för att blottlägga brister i den egna IT-säkerheten (Howard 1997). Det är inte ovanligt att de tekniker som används av en angripare även kan användas för att skydda sig mot intrång. Man kan söka svagheter genom s.k. Port Scanning (”dörrknackning”), som innebär att man gör försök till uppkoppling mot utvalda portar på nätanslutna datorer. (Port Scanning är för övrigt den metod som hackers ofta använder sig av för att förbereda ett intrång.) Ytterligare ett exempel på detta är s.k. webb-trojaner, som använts för att göra motangrepp.[28] Motattacker kan dock medföra att oskyldiga drabbas. Om exempelvis en användare (t.ex. en systemadministratör, operatör eller nätägare) som utsätts för e-mailbombning med falsk avsändare, svarar på attacken genom att skicka klagobrev, kan den oskyldiga avsädarens e-mail i sin tur överbelastas (PTS 200-03-16).

Tekniska försvarsåtgärder bör emellertid kompletteras med andra metoder. Till att börja med kan man konstatera att vi (ännu) inte kunnat skapa ett helt säkert dataskydd. Ett sådant skulle sannolikt bli väldigt kostsamt. Enbart den snabba tekniska utvecklingen skapar osäkerhet i detta hänseende. Det kan också uppstå andra problem när Internettekniken springer fortare än människan, som sammanhänger med t.ex. inlärning, användning, upptäckt av brister, undersökning eller lagstiftning. Det krävs en teknisk kompetens, som många saknar, för att överhuvudtaget uppfatta och förstå problem med datasäkerhet. Det spelar ingen roll hur höga säkerhetsmurar vi än bygger, så länge det finns möjlighet att på kort tid ta sig under, över och runt dem. Det är sedan länge ett axiom i IT-säkerhetskretsar att det enda egentliga skyddet mot intrång är tidsfördröjning, s.k. Time Based Security (TBS). TBS går ut på att skapa tid för att upptäcka och reagera på intrång (Schwartau 1999).[29]

---

[28] Med webb-trojan avses här en webb-sida som angriper Internetanvändarens dator, d.v.s. den som laddar ner webbsidan drabbas. Webb-trojaner skall exempelvis ha använts för att göra motangrepp på aktivister som genom samordnad överbelastning lamslagit en webbplats (PTS 2000-03-16).

[29] Winn Schwartau höll under InfoWarCon i London 1999 föredraget ”Time Based Security for the Network and the Infrastructure”.

Ansvar och samarbete

I diskussionen om motåtgärder mot skadliga operationer på Internet, och vem i samhället som bör ta på sig ansvaret för att genomföra dessa, går meningarna ofta isär. Denna diskussion är sammansatt och föränderlig och knappt möjlig att ringa in inom ramen för denna studie. Preciseringarna av vilka IT-incidenter som skall anses vara kriminella handlingar och vilka som skulle kunna utgöra ett hot mot den nationella säkerheten, är inte helt klara. Detta försvårar ansvarsfördelningen avseende motåtgärder mellan myndighetger och andra institutioner. Denna oklarhet gäller inte bara för Sverige, utan är ett problem internationellt. I USA förs exempelvis diskussioner om ansvarsförhållanden mellan FBI och den amerikanska regeringen.

Grovt förenklat kan två, eller möjligen tre, trender urskiljas i argumentationen om ansvarsförhållanden: (1) synsättet att det främst är rättsväsendets uppgift, (2) att försvarsmakten har det yttersta ansvaret och (3) de som anger att vare sig rättsväsendet eller försvaret är kapabla att hantera IT-incidenter på ett tillfredsställande sätt. Denna sista kategori förespråkar inte sällan en större roll för privata organisationer.

Polis

Om vilseledningen är ett brott i sig, eller ingår i brottslig verksamhet, har polisen skyldighet att undersöka brottet. Olovligt införskaffande av information och otillbörlig manipulation av information är exempel på vilseledning som kan klassas som IT-relaterade brott. Hur vilseledning på Internet skall hanteras och åtgärdas beror delvis på vem som har genomfört operationen. Om det är uppenbart kriminella som ligger bakom vilseledningsoperationen, är det klart en polisiär angelägenhet. För att komma åt brottslingar på nätet krävs förstås att polisen dels har tillräcklig IT-kompetens, dels att de ges de befogenheter som krävs. Lagen släpar dessvärre fortfarande efter, trots att man arbetat på att förnya lagarna i snart tio år[30]. Vilseledning på nätet sker mycket ofta med hjälp av kommunikation som övergränser de nationella gränserna (t.ex. genom att en server i ett annat land används). Även den internationella rätten måste anpassas till den nya brottsmiljön för att polisen ska kunna arbeta effektivt. Anonymiteten på nätet är ett problem för polisen: brottslingar gömmer sig, parasiterar på andras identitet och sopar igen spåren.

Utvecklingen på IT-området ställer allt större krav på polisen som inte bara skall spana och spåra i en ny miljö (utan att själva synas), utan också måste kunna säkerställa elektroniska bevis och lägga fram dem till prövning. Polisen måste hålla hög hastighet och kunna röra sig i ”cybervärlden” dygnet runt. Med Internet suddas gränserna ut och internt, regionalt, nationellt såväl som internationellt samarbete blir allt viktigare för att motverka IT-relaterade brott.[31]

Stat och försvar

Det krävs en nationell policy för hanteringen av IT-hot. Ur försvarssynpunkt handlar det om att skydda och upprätthålla nationell

---

30) Exempel på utredningar som har gjorts för att anpassa lagarna till informationssamhället är: ”Datastraffs-utredningen” (SOU 1992:110) och ”Polisrättsutredningen” (SOU 1995:47).

31) Rikskriminalchef Lars Nylén framförde några av dessa krav på polisen vid en konferens om IT-brottslighet i februari 2000: mer kunskap om IT och IT-brott, ökade insikter om denna typ av brott, en ökad förmåga att känna till och upptäcka IT-brottens ’modus operandi’, säkerhetstänkande i alla led: i utbildningen, i den brottsförebyggande verksamheten såväl som i utredningsarbete och hantering av brott.

suveränitet och säkerhet. Om en främmande stat eller terroristorganisation skulle utföra en informationsattack där centrala delar av landets information och/eller informationssystem hotas skulle detta bli en fråga för försvarsmakten. En av underrättelsetjänstens uppgifter är att upptäcka informationsspridning som skulle kunna beröra Sveriges säkerhet. Inom det militära försvaret har man börjat utveckla kunskaperna inom områden som psykologiska operationer, informationsoperationer och informationskrigföring. Bland annat har man kunnat konstatera att det för dessa områden egentligen inte går att dra någon skarp gräns mellan fred och krig, och inte heller mellan civilt och militärt försvar. En informationsattack kan börja i princip var som helst och riktas mot i princip vem eller vad som helst. Man eftersträvar därför ett helhetstänkande och letar efter gränsöverskridande lösningar. Ett speciellt problem är oviljan hos såväl privata företag som statliga myndigheter, att rapportera IT-incidenter. En anledning tros vara rädslan att blotta sina säkerhetsbrister eftersom detta skulle kunna leda till minskad trovärdighet (bad-will). Som ett första led i sökandet efter en lösning har Post- & Telestyrelsen (PTS) fått i uppdrag av regeringen att upprätta en nationell IT-incidentrapporteringsstation.[32] Detta är en viktig länk i arbetet med att få en tydligare bild av IT-hotet. Men bättre rapportering löser inte frågan om vem som har ansvaret när det verkligen händer någonting.

CERT

Kritiska röster menar att varken polis eller försvar är organiserade för att hantera IT-incidenter på ett ändamålsenligt sätt; de militära lösningarna passar inte problemen och polisen är tekniskt och lagligt begränsad att agera mot IT-brott på ett tillfredsställande sätt. Lösningen menar man finns i s.k. CERTs (Computer Emergency Response Teams). Fördelarna med CERTs är att de är fokuserade på incidentproblemet och kan erbjuda anonymitet för den som blivit utsatt för någon form av IT-attack. CERTs kan utnyttjas av både den offentliga och den privata sektorn och har kompetens att övervaka internationella informationsflöden. På uppdrag av regeringen utreder Post- & Telestyrelsen förutsättningar för en central funktion för IT-incidenthantering (ibland kallad ”StatsCERT”).[33] Informationsförmedling, informationsinsamling, mottagning av incidentinformation, aktiva åtgärder vid IT-incidenter, statistisk rapportering och analys är exempel på uppgifter som en sådan funktion skulle kunna ha.

Den enskildes ansvar

Dilemmat med ansvarsförhållanden avseende IT-relaterade incidenter kommer troligtvis att vara bestående så länge problemen med att bedöma elektroniska attackers *ursprung*, *uppsåt* och *motiv* kvarstår. Och så länge arbetsfördelningen är oklar hamnar förmodligen ansvaret i praktiken på den organisation, den myndighet eller det företag inom vilken den som drabbas verkar. En viktig fråga är därför

---

32) Från PTS poängterar man dock att de till att börja med kommer att genomföra en försöksverksamhet, som skall ligga till grund för den ”riktiga” stationen.

33) Frågan om en statsCERT har behandlats av Statskontoret och Arbetsgruppen för skydd mot informationskrigföring (AgIW, Fö 1997:A). I AgIWs rapport från maj 1999 och i Statskontorets rapport 1998:18 finns förslag på området. I propositionen *Förändrad omvärld – omdanat försvar* (prop. 1998/99:74) uppger regeringen att möjligheterna för att införa en StatsCERT kommer att övervägas (Regeringsbeslut 1999-11-25 N1999/11654/ITFoU).

vart t.ex. frilansande journalister, enskilda företagare och privatpersoner ska vända sig när de blir utsatta för vilseledning på Internet? *Det största ansvaret när det gäller att förebygga såväl som upptäcka och anmäla vilseledning på nätet vilar slutligen på den enskilde.* Det börjar alltid med en enskild incident och då är det upp till den enskilde att upptäcka och reagera. Hur man värderar information på nätet skiljer sig förmodligen från person till person. Generellt kan nog hävdas att kunskapen om IT och Internet fortfarande är bristfällig i samhället i stort. Den skeva kunskapsfördelningen utgör fortfarande grund för en uppdelning mellan de som kan och de som inte kan, där de som kan har ett övertag. Spridandet av kunskap, både om Internet och om vilseledning, är också den viktigaste typen av långsiktiga allmänna åtgärder.

Källkritik

Insikter i hur Internet fungerar, ett kritiskt förhållningssätt till källor på nätet och kunskaper om hur man kan bedöma dessa, är grundläggande för att undvika att bli vilseledd (t.ex. Leth & Thurén, 2000). Därför har vi här inriktat oss på de kunskapsmässiga aspekterna på källkritik för nätet.

Var och en sin egen gate-keeper

Bakom den interaktiva cyberkatalogen som är Internet, döljer sig ett storförlag som publicerar tusentals skribenter, författare och journalister varje dag. Alla som har tillgång till en dator och ett modem kan publicera sig, lägga ut sin musik, spela in program och säga sin åsikt. Alla dessa röster vill förstås vinna sin tilltänkta publiks uppmärksamhet och helst också deras hjärtan. Internetanvändaren är inte bara sin egen informationsuppköpare och publicist, han eller hon är – mer eller mindre framgångsrikt – också sin egen grävande journalist och gate-keeper. För att inte drunkna i informationsfloden gäller det att sålla information. Man måste leta fram de kanaler som erbjuder intressant och tillförlitlig information. Med Internet kan den som har teknisk kompetens undersöka ursprungskällan och kanske till och med kommunicera med denna. Det är viktigt att det finns en förståelse för dynamiken kring information och en insikt i vad som krävs för att bedöma en källas trovärdighet på Internet.

Källkritik innebär att ”kritiskt granska till buds stående källor”.[34] Syftet med källkritiken är att finna källor som ger den ”bästa kunskapen” om verkligheten inom ett visst område. Idealet är när en källa är oberoende, opåverkad av andra källor och inte själv har något att vinna på att sprida falsk eller tillrättalagd information. Om källans information rör en viss händelse så bör berättelsen om denna ligga nära i tid till denna. Sedan skall förstås källan till informationen vara den som den utger sig för att vara. Man skiljer mellan primär- och sekundärkällor och källor som kommer med uppgifter i tredje hand.[35] Man bör eftersträva att använda sig av förstahandsinformation så långt det är möjligt, men källkritik handlar inte om att sortera bort alla andra källor. På Internet finns en mängd källor som kan vara värdefulla fastän de inte är primärkällor. De källkritiska principerna gäller för all form av kunskapsinhämtning och självklart även när man skaffar sig kunskap på Internet. Behövs det då en särskild källkritik för nätet? Nej, sva-

---

34) ”Svensk Ordbok” 1998

35) Läs mer om källkritiska principer i ”Källkritik” (1997) av Torsten Thurén. Se också Leth & Thuréns ”Källkritik för Internet” (2000).

rar många. Denna inställning hänger inte sällan ihop med attityden till Internet som en ny informationskanal i raden bland många andra. (Som någon uttryckte det under en intervju: ”Förut åkte vi häst och vagn – nu åker vi bil”.) De som har studerat frågan (t.ex. Leth och Thurén) svarar både ja och nej. För samtidigt som det interaktiva inslaget gör det möjligt för var och en att ta direkt kontakt med en källa, så är källkritik på nätet något av en paradox.

Källkritik för nätet – en paradox?

Källkritik i sin ursprungliga mening har med Internets intåg blivit en absurditet, eftersom antalet källor inom i princip vilket område som helst är oändligt. Att kritiskt granska alla de källor man har tillgång till är därför många gånger omöjligt. Kanske behövs en särskild sorts källkritik just för Internet. Internets betydelse för informationssökaren går inte att överskatta. Internet underlättar på många sätt arbetet för informationssökaren. Men samtidigt ställs det högre krav på den som söker information. Med avancerade program (”elektroniska motorvägar”) kan stora mängder data behandlas och analyseras. Den rätta länken kan öppna en ny värld. Med ett klick kan ett scoop göras, ett annat bekräftar en uppgift och ytterligare ett klick kan rasera en tes. Möjligheten finns alltid att använda fler källor, att ta reda på fler, bättre och intressantare uppgifter. Den enda begränsningen är egentligen sökarens uthållighet och tid. Även vana informationssökare, t.ex. journalisten, forskaren och underrättelsemannen, är på ett annat sätt än tidigare utlämnade till sig själva i bedömningen av uppgifter. Internet är ingen källa. Internet är ett verktyg för att finna källor, och för att kunna bedöma dessa måste man vara väl förtrogen med detta verktyg.

Sanning sökes!

Internet, säger man, erbjuder en värld utan gränser. Detta är i en mening korrekt, men samtidigt inte. Det oändliga utbudet av källor är i själva verket inte tillgängligt för de flesta. När man exempelvis söker ett ämne igenom en sökmotor tror man kanske att man då söker igenom större delen av Internet. Men databaserna, även de största, är små i förhållande till den totala mängden information som finns på nätet. Den synliga delen, t.ex. den del av Internet som man kommer åt genom en av de stora öppna sökmotorerna, utgör mindre än en femtedel av den verkliga verksamheten på Internet.[36] Varje sökmotor är uppkopplad mot en konstruerad databas, som inte på långt när uppdateras i samma takt som det tillkommer webbplatser. Man räknar med att det tillkommer en webbplats var fjärde sekund, dygnet runt. Internet understryker på många sätt osäkerheten i all kunskap. Kunskapen ter sig alltmer tillfällig och bristfällig. Den här synen på kunskap, som vunnit allt större respekt inom vetenskapen, är förmodligen ett bra förhållningssätt när man söker efter ”sanningen” på Internet.

Det finns två fällor man kan gå i när man söker efter information på Internet. Den ena är att bli misstänksam mot alla källor (total relativism) eller att man sätter en överdriven tilltro till vissa utvalda källor på Internet. Hur skall man då bära sig åt för att på bästa sätt bedöma källors trovärdighet på nätet? Leth och Thurén (2000) föreslår tre tillägg till de tra-

---

[36] I en undersökning av användningen av Internet som presenterades i Nature i juli 1999, kom man fram till att man genom att söka genom Alta Vista kommer åt ca 16% av den totala mängden information som finns på Internet.

ditionella källkritiska reglerna: ta reda på källans världsbild och kunskapssyn, förutsättningar och egenskaper samt bedöm källans trovärdighet. Källkritik för nätet innehåller således sju principer: tidsaspekten, oberoende, äkthet, tendens, världsbild, kunskapssyn och trovärdighet. De nya aspekterna har, liksom de gamla, en speciell tillämpning på nätet.

Källkritik för nätet – några tips

Tid

När det gäller tidsaspekten kan det till exempel handla om att kontrollera om en websida uppdateras regelbundet, när den uppdaterats, och i så fall vad som har uppdaterats (allt behöver inte uppdateras bara för att sidan är uppdaterad).

Oberoende

Det kan vara svårt att avgöra om en källa på Internet är oberoende eftersom tradering är vanligt förekommande på nätet. En regel kan vara att försöka kontrollera uppgifter med primärkällan om det är möjligt. Annars skall uppgiften uppges av minst två av varandra oberoende källor, d.v.s. de skall inte utgå från samma primärkälla. För att bedöma om två källor är oberoende av varandra kan man till exempel jämföra formuleringar och titta efter likheter i detaljuppgifter.

Äkthet

Hur skall man avgöra om en källa på nätet är den den utger sig för att vara? På Internet har det blivit betydligt svårare att skilja mellan vad som är äkta och falskt. Det kan handla om falska avsändare, plagiat eller helt enkelt om att utge sig för något som man inte är. En vilseledare kan även göra ändringar utan att lämna några spår efter sig. Ett tips är att vara misstänksam mot vaga presentationer av personer och institutioner.

Tendens

Det är viktigt att en källa inte själv är part i målet eller på annat sätt kan ha intressen av att vinkla uppgifter, överdriva eller underdriva, framhålla visst och undanhålla annat. Om så är fallet är en källa tendentiös. Varje källa som kan förväntas ha intresse av att ljuga eller förvränga måste på nätet nästan misstänkas för att göra det. Här kan man kontrollera kommersiella intressen, nationalitet, partitillhörighet o.s.v. Kärnan i problemet med att bedöma tendens på nätet är svårigheten att med säkerhet avgöra källans identitet.

Världsbild och kunskapssyn

Men finns det egentligen några källor som saknar tendens? Den här frågan är kanske särskilt viktig att ställa på nätet, där den som söker efter information stöter ihop med källor från hela världen. Alla källor kommer ur en kultur och är färgade av sin syn på kunskap, religiösa föreställningar, traditioner, värderingar, historia, språk, seder o.s.v. På nätet, där många sidor till utseende påminner om varandra och är anpassade till en internationell publik, kan det vara lätt att glömma bort detta.

Trovärdighet

Att bedöma en källas trovärdighet på nätet handlar alltså till stor del om att leta efter ledtrådar: Verkar källan vara opartisk? Objektiv? Kan den ha några dolda motiv? Är den kvalitativ i sin information? Man kan ta reda på så mycket som möjligt om avsändaren och kanske till och med kontakta källan själv. Man kan även ta reda på så mycket information som möjligt om informationen (metainformationen); finns det t.ex. kommentarer och värderingar om källans uppgifter på någon annan webbplats? Vilken adress har källan? Toppdomänen är den sista delen i en Internetadress (domänadress, e-mailadress eller

webbadress); .gov står exempelvis för statliga sidor, .mil för militära sidor, .edu för universitet och dylikt, .org för ideella organisaitoner, .com som kan vara vad som helst och .net som oftast är sökmaskiner av olika slag. Ofta kan ett välrenommerat toppdomännamn indikera trovärdighet, vilket som vi sett kan missbrukas (t.ex. i fallen ”Pol Pot i Stockholm” och ”www.levandehistoria.?”). Toppdomännamnet skvallrar snarast om källans tendens. Man kan också försöka kontrollera vem som står bakom ett domännamn, men detta är inte alltid möjligt. Ett annat sätt är att se hur informationen framställs: är det rimligt, är det noggrant eller slarvigt genomfört, hur går argumentationen o.s.v. Internet är den perfekta floran för rykten; det figurerar ett otal myter, vandringssägner, legender och s.k. hoaxes[37] på nätet. För att undvika de värsta grodorna kan det vara värt att kolla att källan eller uppgiften inte tillhör någon av de redan kända ”nätblufarna”. På nätet finns det förstås sidor där man samlar på just sådant.[38]

Sammanfattning

Utifrån diskussionen ovan kan några enkla slutsatser dras om hur man kan minska sin sårbarhet för vilseledning på Internet:

1. Det är viktigt att ansvarsförhållandena blir tydligare när det händer något.

2. Tekniska åtgärder är viktiga, t.ex. för att skydda sig mot olovliga intrång, men bör kompletteras med andra åtgärder. Skyddet står t.ex. alltid i relation till upptäckt och reaktion.

3. IT-utvecklingen ställer krav på den enskilde som är en potentiell mottagare av vilseledning på Internet. Motåtgärder i fråga om vilseledning på Internet borde därför väsentligen handla om spridandet av kunskap i samhället om detta fenomen och vad den nya informationstekniken erbjuder för möjligheter. Kunskap, kritiskt sinnelag och en viss beredskap är grundläggande förutsättningar för att minska den enskildes, och därmed samhällets, känslighet för vilseledning på Internet.

4. För att bedöma en källas trovärdighet måste man tillämpa en utvidgad och skärpt källkritik.

5. Området är dynamiskt och kunskapsutveckligen är snabb och komplex. Man kan därför inte bli färdiglärd och inte heller räkna med att lösa problemen en gång för alla.

---

37) En hoax är ett varningsmeddelande om datavirus som har till syfte att störa datanättrafiken. Genom att oroa och skrämma får man folk att skicka en uppsjö av varningar kors och tvärs över nätet. Dessa hoax är alltså inte några virus.

37) På www.snopes.com finns t.ex ett arkiv med hoaxes och länkar till dementier.

DEL VI
SÅRBARHET

På vem regnar det?

Med sårbarhet menas i allmänhet någons (t.ex. en persons, organisations eller stats) relativa utsatthet för ett hot.[39] Om en lastbil kolliderar med en personbil är föraren i personbilen normalt mer sårbar än föraren i lastbilen. Uppskattningar av sårbarhet avseende vilseledning med hjälp av Internet är till viss del problematiska. En svårighet är att avgöra vad sårbarheten egentligen innebär. Vems sårbarhet talar vi egentligen om? Vid en analys av sårbarhet vad gäller militära hot är det självklart att hänföra denna problematik till hela nationen. Ett väpnat angrepp på Sverige skulle ske över den internationella gränsen till en suverän stat, som därför av nödvändighet blir inbegripet i sin helhet i en väpnad konflikt. Ett liknande resonemang kan föras om vissa ickemilitära hot, till exempel ekonomiska sanktioner som skulle kunna riktas mot nationen Sverige.[40] Ett analogt resonemang är emellertid svårare att föra om sårbarhet avseende vilseledning med hjälp av Internet, eftersom en analys av detta problemområde måste utgå från den enskilda aktören i högre grad än vad som gäller för den militära säkerheten. Det är individer, organisationer och myndigheter som blir utsatta för vilseledning och som måste försvaras – inte nationen som helhet. Förhållanden i samhället kan påverka hur sårbara dessa aktörer är. Men aktörernas egna särdrag och speciella relationer till sin omvärld måste också antas utgöra förhållanden som i grunden påverkar deras sårbarhet gentemot vilseledning.

Betingelser för sårbarheten

Delvis annorlunda sårbarhetsfaktorer kan härledas till tre av vilseledningens faser: *underrättelser*, *ploj* och *kommunikation*. Mottagaren kan vara olika sårbar under de olika operationsfaserna. Vid en jämförelse mellan två aktörer som är objekt för samma vilseledningsoperation kan den ene ha större beredskap än den andre att, t.ex., hantera tekniska

---

39) Det kan finnas skäl att göra en distinktion mellan känslighet och sårbarhet (Keohane & Nye 1989). Känsligheten är ett uttryck för någons grad av utsatthet i det ögonblick ett hot uppträder. Sårbarheten uttrycker den grad av utsatthet som är vid handen efter det att motåtgärder har vidtagits för att hantera ett givet hot. En person på promenad kan exempelvis minska sin känslighet i förhållande till en plötslig regnskur genom att fälla upp sitt medhavda paraply. Risken att trots denna åtgärd bli blöt motsvarar sårbarheten i förhållande till regnet. Bedömningar om skillnaden mellan känslighet och sårbarhet, och analyser av orsaker till diskrepansen, kan ge stöd åt utformningen av en försvarsstrategi. I det följande kommer emellertid sårbarhet att användas som ett begrepp som täcker såväl känslighet som sårbarhet i mer precis mening. Detta kan göras för att diskussionen hänför sig till de grundläggande beskrivningsfaktorerna som på det hela taget är de samma för känslighet respektive sårbarhet.

40) Situationen som ska bedömas är dock inte glasklar. Det kan t.ex. diskuteras om risken för att företaget Ericsson ska utsättas för en bojkott också ska ses som en risk för Sverige.

problem som påverkar sårbarheten avseende själva kommunikationen. Medan den andre är mindre lättlurad när det t.ex. gäller tolkningen av tillrättalagd information, och således mindre sårbar när det gäller vilseledningens ploj. Dessa förhållanden är viktiga att ha i åtanke när generella åtgärder övervägs mot vilseledning via Internet.

Underrättelser

I nästan samtliga empiriska fall som ingår i denna studie är operationen – inte minst dess ploj – skäligen okomplicerad. I inget fall finns uppgifter om att sändaren skulle ha inhämtat speciella underrättelser som ett led i förberedelserna till vilseledningsoperationen. Dock indikeras i flera fall behovet av relevant information som stöd för vilseledningsoperationen.

Sett ur ett sårbarhetsperspektiv har underrättelser om mottagaren egenskaper som på ett betydelsefullt sätt särskiljer den från de två andra kategorierna. Såvida sändaren inte redan har den nödvändiga informationen innan vilseledningsoperationen genomförs (t.ex. ”Hackers kapar webbplats!”, ”Hej det är Olle...” och ”Tokyo Joe”), kan han eller hon samla in information om tekniker och andra förhållanden runt mottagaren oberoende av denne.

När det gäller kunskap / information om mottagaren själv är betingelserna annorlunda. Sändaren kan visserligen inhämta en del relevanta underrättelser om mottagaren från andra källor än denne själv. Om mottagaren t.ex. är en ”känd person” finns det ofta mycket pressklipp och liknande källmaterial som kan användas. Men sannolikheten är stor att vilseledningsoperatören kommer att behöva information om mottagaren som måste inhämtas från denne själv eller från dennes närmaste omgivning.[41]

De sårbarhetsförhållanden som sammanhänger med underrättelser om mottagaren är speciella därför att de i åtminstone viss omfattning låter sig påverkas av mottagaren själv. Ett exempel är vidtagna säkerhetsåtgärder som förhindrar eller försvårar för andra att komma åt information om mottagarens datautrustning och rutiner på dataområdet inklusive Internetvanor. Andra villkor för att sändaren ska kunna genomföra en sofistikerad och framgångsrik vilseledningsoperation låter sig inte påverkas på samma sätt av mottagaren för aktionen, till exempel sändarens tillgång till ny teknisk information om hur spärrar mot intrång i datasystem ska kunna kringgås.[42]

Förhållandet mellan sändare och mottagare spelar alltså stor roll för mottagarens sårbarhet. Antag exempelvis att plojen som i fallet ”Hackers kapar webbplats!” förutsätter att sändaren gör ett intrång i mottagarens datasystem. Antag vidare att sändaren har denna nödvändiga förmåga men att *samtidigt* mottagaren är minst lika kompetent vad gäller att skydda sig mot intrång. Under de betingelserna är mottagaren mindre sårbar än om det råder en ojämn fördelning av kunskap där mottagaren är den underlägsne.

Sammanfattningsvis kan fyra kritiska aspekter på underrättelser urskiljas betraktat

---

41) Detta behov av information / kunskap om mottagaren blir, såsom gäller för flera av de studerade fallen, reducerat om sändaren från början är bekant med mottagaren för vilseledningen. En sådan förkunskap kan vara en förutsättning för att sändaren överhuvudtaget kommer på idén att utsätta mottagaren för vilseledning.

42) Naturligtvis kan man föreställa sig undantag mot denna allmänna regel, t.ex. att den aktör som blir objektet för en vilseledningskampanj har förutsett detta och därför har reducerat sändarens tekniska kapacitet att genomföra en sådan operation genom sabotage.

med mottagarens ögon: (1) underrättelser om mottagaren till exempel rörande egenskaper, vanor eller relationer till andra, (2) underrättelser om sakfrågor eller den yttre kontexten som vilsledningen hänför sig till, (3) underrättelser om de tekniker som skall användas i plojen och / eller kommunikationen av denna och (4) underrättelser om plojens effekter när vilseledningsoperationen börjar genomföras.

Ploj

Plojen är nyckeln till vilseledningsoperationens framgång. Det är det framgångsrika genomförandet av plojen som faktiskt vilseleder mottagaren. Övriga åtgärder som sändaren vidtar skall skapa förutsättningar för denna vilseledningseffekt. Kommunikationen kan exempelvis bära fram tillrättalagd information inför mottagarens ögon" men vilseledningseffekten beror på hur kommunikationen arrangerats och hur informationen presenterats, d.v.s. hur plojen konstruerats och verkställts.

Eftersom de plojer som redovisats i de sexton vilseledningsfallen är förhållandevis okomplicerade utgör de ett relativt dåligt underlag för en sårbarhetsanalys. Många tänkbara, mer eller mindre sofistikerade varianter på plojer, har därför fallit utanför analysen. Några övergripande observationer skall dock göras.

Det är tankeväckande att ett Internetföretag med hjälp av en förfalskad webbplats och en påhittad nyhetsbyrå lyckades få ett flertal nyhetsbyråer – inklusive Reuters – att publicera uppgiften att Pol Pot skulle ha kommit till Sverige. En förklaring till att plojen i denna operation fick effekt var, att den genomfördes av professionella experter på Internet och datakommunikation. Samtidigt riktade sig vilsledningsoperationen till andra "proffs", nyhetsvärderare och analytiker på nyhetsbyråer, tidningar och synbarligen också utrikesdepartement. När man i efterhand granskar denna episod måste man göra bedömningen, att om vedertagna regler för källkritik hade följts så skulle uppgifterna om Pol Pot i Stockholm inte förts vidare av något nyhetsmedium. Hänvisningen till namnet Komintern borde till exempel ha uppfattats som en larmsignal. Den refererade nyhetsbyrån (TASS.NET:NEWSWIRE) hade ett sådant namn och dess webbplats en sådan konstruktion att denna trots sändarens yrkesskicklighet borde ha avslöjats ganska omgående av varje professionell nyhetsvärderare. En trolig sårbarhetsfaktor som underlättade plojens genomslag var det *sensationella* i de uppgifter som fördes fram av TASS.NET:NEWSWIRE. Detta skärpte konkurrensen mellan de olika medierna om att kunna sälja eller publicera denna nyhet först, vilket troligen bidragit till bristande kontroll. Detta hör ihop med det *överraskningsmoment* som operationen utnyttjade. En annan sårbarhetsfaktor skulle kunna vara att nyhetsbyråer ofta har hög trovärdighet i förhållande till andra medier.[43] En tentativ slutsats är att de faktiska rutiner som utvecklats för inhämtning av information från Internet skulle kunna representera en sårbarhetsfaktor av vikt.

I flera av de sexton fallen bygger plojen på en kombination av vilseledningens båda dimensioner – simulering och dissimulering – såtillvida att simuleringens ofta enkla trick har getts trovärdighet genom att sändarens identitet har förfalskats (t.ex. "Ensam, villig och billig!"). En möjlig sårbarhetsfaktor kan därför vara benägenheten att utan närmare kontroll

[43] En uppfattning som dels kom till uttryck i intervjuerna för den här studien, dels i intervjuer med journalister med erfarenhet från Bosnien för studien "Med sanningen som insats" (Stenström 1997).

acceptera den angivna identiteten på sändaren till ett mottaget meddelande. En typ av ploj som återkommer i flera av fallen innebär att sändaren vänder sig till en viss mottagare för att åstadkomma en reaktion hos denna, som i sin tur åstadkommer en avsedd effekt på en helt annan aktör, vilken är operationens egentliga objekt. Ett sådant syfte är att svartmåla en mottagare (”SAAB Gripen skyller på dåligt väder!”, ”Ensam, villig och billig!”, ”eBay saknar skydd mot intrång!”). Sett ur ett sårbarhetsperspektiv är innebörden av denna typ av indirekt vilseledning att mottagaren inte kan vidta åtgärder mot den ploj som orsakar den negativa effekten för denne. Fallet ”eBay saknar skydd mot intrång!” illustrerar detta dilemma mycket tydligt. Operationen syftar till att svartmåla ett företag med verksamhet på IT-området genom att med ett mail locka en tidning att publicera misskrediterande information om detta företags kompetens. De negativa effekterna för det drabbade företaget och dess verksamhet har ingenting med själva vilseledningen att göra utan uppstår genom att företagets försäljning minskar. Orsaken till denna skada är emellertid en vilseledningsoperation, som företaget haft få eller inga möjligheter att påverka genom motåtgärder. Ett skäl till detta är att vilseledningen i sitt första led inriktats mot andra mottagare än företaget. I detta fall är således företaget – det verkliga objektet för vilseledningen – mycket sårbart. Det finns inga uppenbara åtgärder som mottagaren kan vidta för att minska riskerna för att i framtiden drabbas av en liknande operation.

Fallet ”Tokyo Joe” visar att en vilseledningsoperation kan bli framgångsrik trots att mottagaren inte presenteras falsk information. Om medlemmarna i chatgruppen tror på Joes förutsägelse att kursen på en viss aktie ska stiga och därefter följer Joes råd att köpa, kommer ju faktiskt förutsägelsen att infrias, åtminstone under en kort tid. En del av sårbarheten sammanhänger uppenbarligen med att medlemmarna i chatgruppen inte hade tillgång till fullständig information om de aktier som Joe spelade med, vilket försvårade eller rent av omöjliggjorde en korrekt bedömning av Joes analys och råd. Medlemmarna i chatgruppen hade gjort sig beroende av Joes råd, vilket representerade sårbarhet för dem eftersom detta beroende kunde utnyttjas av Tokyo Joe. Sådana generellt positiva faktorer som tillit och förtroende kan således under vissa förhållanden komma att utgöra faktorer som ökar mottagarens sårbarhet när det gäller vilseledning.

En aktörs sårbarhet avseende vilseledning med hjälp av Internet sammanhänger till sist med dennes egenskaper, särskilt psykologiska och kognitiva. Eftersom en vilseledningsploj underlättas av om den kan kombineras med en överraskningseffekt, har kunskap och medvetenhet om förekomsten av vilseledning och desinformation förmodligen stor betydelse. Ett svagt medvetande om dessa förhållanden utgör tillika en sårbarhetsfaktor.

Kommunikation

Sårbarheten avseende vilseledningsoperationsfasen ”kommunikation” sammanhänger i allmänhet med datasäkerheten. Ju sämre datasäkerhet en aktör har desto större är sårbarheten avseende vilseledning med hjälp av Internet.

I åtminstone två av de analyserade fallen (”Pol Pot i Stockholm” och ”Hackers kapar webbplats!”), är manipulerad kommunikation avgörande för vilseledningsoperationens framgång. Även i andra fall (t.ex. ”Ensam, villig och billig!”, ”Hej, det är Olle...”) har manipulation av kommunikationen, i form av falsk identitet, varit ett bärande inslag i vilseledningen. Bristen på datasäkerhet var här en avgörande sårbarhetsfaktor. Det ska dock betonas att datasäkerhet i meningen ”skydd

mot intrång" endast i ett fall hade undanröjt det hot som vilsledningen utgjorde ("Hackers kapar webbplats!").

Syntes

Analysen av fallen indikerar att det är viktigt att skilja mellan några av vilseledningsprocessens olika faser när sårbarhetsfaktorer avseende vilseledning med hjälp av Internet skall bedömas. Delvis helt olika typer av åtgärder är effektiva för att minska mottagarens sårbarhet.

Med avseende på *underrättelser* verkar sårbarheten delvis sammanhänga med datasäkerhet i konventionell mening, till exempel mottagarens förmåga att förhindra eller åtminstone upptäcka dataintrång. Sårbarheten kan också ha att göra med upprätthållandet av sekretess när detta är motiverat och tillåtet (t.ex. sekretessbelagda handlingar i regeringskansliet eller hos förvarsmyndigheterna). En viktig sårbarhetsfaktor är att den information sändaren behöver för att framgångsrikt genomföra en vilseledningsoperation inte nödvändigtvis är förvarad i mottagarens dator eller skyddad av sekretesregler. De sakuppgifter som sändaren exempelvis behöver om mottagaren kan vara tillgängliga på flera ställen (t.ex. i databaser eller tidningsarkiv) eller möjliga att samla in utan att mottagaren är medveten om eller får kännedom om detta.

Sårbarheten när det gäller *plojen* sammanhänger också i viss utsträckning med datasäkerheten. Utbildning och riktigt utformade rutiner borde minska risken för att en person eller organisation ska bli lurad av säg en falsk webbplats eller en falsk e-mailidentitet. Huvudsakligen sammanhänger emellertid sårbarheten avseende plojen troligen med psykologiska och kognitiva faktorer, d.v.s. egenskaper hos mottagaren själv och dennes relation till sin omgivning.

Inte heller sårbarheten avseende vilseledningens *kommunikation* är helt och hållet en fråga om datasäkerhet i vanlig mening, t.ex. skydd mot intrång i datautrustning eller i kommunikation mellan datorer. Det finns anledning att tro att kommunikationen mellan sändaren och mottagaren ofta kan ske på ett normalt och till synes helt legalt sätt eller så att mottagaren lockas att själv söka den tillrättalagda information som är avsedd att åstadkomma en ploj.

Av resonemanget ovan kan man dra slutsatsen att utbildning och medvetandegörande är viktiga metoder för att minska sårbarhet avseende såväl ploj som kommunikation. Utbildningsåtgärderna får emellertid inte allt för mycket koncentreras på rena frågor om datasäkerhet. Det är angeläget att utbildningen även inbegriper kunskap om vilseledningens förutsättningar, mekanismer och möjliga effekter.

Problemet att generalisera

En framkomlig väg att identifiera och utvärdera sårbarhet avseende vilseledning med hjälp av Internet borde vara att beskriva, analysera och jämföra verkliga fall av vilseledning. Ett problem är hur den kunskap som samlas in ska kunna generaliseras och relateras till samhället i dess helhet. En lista med generella sårbarhetsfaktorer skulle kunna se ut på följande sätt:

- mindre Internetvana,
- beroende av datasystem med mindre utvecklade mekanismer och rutiner avseende datasäkerhet,
- lägre grad av medvetenhet och kunskap rörande datasäkerhet,
- sämre medvetenhet och kunskap rörande vilseledning, samt
- mindre utbildning och träning i att värdera Internetkällor.

Alla dessa faktorer kännetecknas av att de genom utbildning och träning kan omvandlas

till mer hanterbar eller acceptabel sårbarhet.

En annan ansats för att specificera generella sårbarhetsfaktorer är att identifiera sårbarhet som hänför sig till olika sammanhang som bedöms vara viktiga att fånga in i en undersökning.[44] En speciell kontext är landet i dess helhet. Sårbarhetsfaktorer på nationell nivå är emellertid i flera hänseenden problematiska. För det första är de så generella att de ur analyssynpunkt tenderar att vara triviala. För det andra är de ur policysynpunkt alltför diffusa för att ge tydlig vägledning för utformningen av en försvarsstrategi. För det tredje är kunskaperna osäkra om känslighet och sårbarhet avseende vilseledning med hjälp av Internet eftersom deras empiriska grundval är svag.

Nationella sårbarhetsfaktorer kan emellertid särskiljas från sårbarhetsfaktorer som hänför sig till *avgränsade kontexter*.

Sårbarhetsfaktorer i avgränsade kontexer

Med avgränsad kontext menas här ett bestämt sammanhang där fler än en individ kan utsättas för vilseledning med hjälp av Internet. Ett exempel på en sådan kontext är en viss organisation eller företag eller en hel bransch som omfattar en viss typ av företag som dagstidningar, elektronikföretag eller departement i regeringskansliet. Vid en utvärdering av sårbarhet avseende vilseledning med hjälp av Internet, kan det vara meningsfullt att bedöma sårbarheten i den aktuella organisationen eftersom dessa riskerar att vara strukturella och därför av bestående natur.

Avgränsade kontexter kan också definieras utifrån andra kriterier än det organisatoriska. Två exempel är *yrkesområden* och *beslutssituationer*.

Yrkeskontext

Professionell verksamhet utgör en typ av yrkesrelaterad kontext som kan vara relevant i en sårbarhetsbedömning avseende vilseledning med hjälp av Internet. Exempel på representanter för professioner är soldater, diplomater, journalister och underrättelsekonsulter. De som tillhör en speciell profession har i väsentliga delar en gemensam referensram, vilken inkluderar såväl kunskap som attityder, värderingar och beteenden.

Utnyttjandet av Internet är ett exempel på ett sådant beteende, som betingas mycket annorlunda i olika professioner. Datakonsulter till exempel kan självfallet förväntas vara mer förtrogna med Internet än till exempel domstolsjurister. Generellt kan sårbarhetsförhållanden förväntas variera mellan yrkesområden. Intervjuer gjorda med representanter för olika professioner visar att olika professioner bedömer trovärdigheten hos Internet olika. Skillnaderna mellan *journalister* och *underrättelsekonsulter* är intressant. Intervjuerna med journalister pekar nämligen på att ett vanligt och respekterat förhållningssätt är att upprätta ett urval av informationskällor på Internet som man efter prövning uppfattat som trovärdiga. När man en gång värderat en viss informationskälla som trovärdig kan man sedan använda denna i nyhetsvärderingen utan att behöva göra särskilda undersökningar och bedömningar. Förhållningssättet till informationskällorna på Internet verkar vara ett annat inom professionen *underrättelsekon-*

[44] Vad som är en viktig kontext bestäms av vad sårbarhetsanalysen vill åstadkomma. En sårbarhetsanalys som avser statsförvaltningen kan t.ex. tänkas fokusera på andra kontexter än en studie som vill undersöka ett privat företags sårbarhet avseende vilseledning.

sulter. Här fanns en större skepsis till den information som finns tillgänglig via Internet. Exempelvis är en norm att nyhetsbyråer är andra- eller tredjehandskällor, vilka i största möjliga utsträckning ska undvikas i en analys.[45] Journalistens respektive underrättelsekonsultens olika förhållningssätt till informationsinsamling på Internet medför förstås skilda sårbarhetsförhållanden.

Beslutskontext

För en aktör som överväger att genomföra en vilseledningsoperation är det av stor betydelse vilken slags beslutssituation som ska påverkas. Det finns anledning att särskilt beakta tre slag av beslutssituationer: *rutinbeslut*, *krishantering* och *planering*.

De förhållanden i beslutssituationen som kan förmodas utgöra villkor för vilseledning genom Internet sammanhänger med hur de påverkar aktörernas inhämtning och användning av information som kommer att ingå i deras beslutsunderlag. Exempel på sådana omständigheter är beslutssituationens komplexitet, dess grad av struktur liksom tidsbetingelserna. Faktorer som exempelvis knapphet på relevant kunskap och information eller antalet aktörer som medverkar i beslutsprocessen spelar in här. Graden av komplexitet i beslutssituationen kan förväntas sammanhänga med hur beslutsfattaren sköter informationshanteringen. Informationshanteringen i en beslutssituation betingas av i hur stor utsträckning beslutsfattaren är tränad och van att hantera denna. Det har också betydelse i vilken grad beslutsfattarens informationshantering styrs av precisa regler och procedurer. En beslutsprocess sårbarhet avseende vilseledning kan ju t.ex. påverkas av den tid som beslutsfattaren har till sitt förfogande. Möjligheterna att såväl söka som källvärdera information riskerar att begränsas om tidspressen på beslutsfattaren ökar.

Rutinbeslut

Begränsad komplexitet, relativt stora tidsbegränsningar och en höggradigt strukturerad beslutssituation kan förväntas prägla rutinbesluten. I denna typ av situation sker informationsbehandlingen i beslutsprocessen normalt på ett inlärt och beprövat sätt. Detta gäller även utnyttjandet av informationskällor. Rutinbeslut har klara implikationer avseende sårbarhet för vilseledning. En rimlig hypotes är å ena sidan, att beslutsfattaren har mycket begränsad benägenhet att söka efter ny information till exempel på Internet. Å andra sidan är en annan hypotes att beslutsfattaren också har en liten benägenhet att kontrollera trovärdigheten hos beprövade informationskällor, vilka utnyttjas i beslutsfattandet. Detta förhållande tenderar att höja sårbarheten avseende vilseledning.

Krishantering

Tidsbegränsningarna är mycket stora, beslutssituationen är ostrukturerad, inte minst informationshanteringen. Ofta är komplexiteten betydande. Beslutsfattarna har behov av att snabbt få fram sakuppgifter och bedömningar som kan underlätta olika ställningstaganden. Man har inte tid att rationellt väga olika handlingsalternativ mot varandra utan är benägen att välja den acceptabla problemlösning som man först får ögonen på. Sannolikt har beslutsfattarna inte tid för vare sig en omfattande sökning efter information eller noggrann informationsprövning. Hypotesen kan ställas att beslutsfattarna är sårbara gentemot manipulering av beslutsunderlag genom

---

45) Intervjuer med Anders Lignell (TT) respektive Ulf Petersson (konsult).

dataintrång. Beslutsfattaren / krishanteraren kan också antas ha en förhållandevis stark benägenhet att utnyttja information som vid en första bedömning framstår som relevant och trovärdig och som finns tillgänglig när den behövs.

Planering

Beslutssituationen kännetecknas av förhållandevis små restriktioner för informationshanteringen, stor komplexitet bl.a. genom långsiktighet och osäkerhet liksom av en förhållandevis låggradig struktur. Planeringen brukar vara tydligt organiserad och förstrukturerad på ett övergripande plan men inte när det gäller detaljarbete i exempelvis informationshanteringen. Tidsbegränsningarna är förhållandevis små, särskilt vad beträffar beslutsprocessens sökfas.[46] Beslutsfattarna kan därför agera förhållandevis rationellt och har exempelvis möjligheter att följa reglerna för källvärdering utan att detta inkräktar på beslutsfattandet. En hypotes är att dessa förhållanden försvårar vilseledningsoperationer. Tekniskt komplicerade frågor och osäkerhetsproblem i framtidsbedömningar skapar behov efter ny kunskap / information, vilket kan antas underlätta för vilseledningsoperationer i vilka plojen exempelvis består av manipulation av vetenskaplig kunskap / information.

Sammanfattning

- För att bestämma ett långsiktigt förhållningssätt till de risker som sammanhänger med vilseledning med hjälp av Internet, är det viktigt att känna till den troliga sårbarhet som kvarstår efter det att möjliga motåtgärder vidtagits. En uppsättning ”rimliga” sårbarhetsfaktorer utgör karaktäristika på aktörer (individer, företag eller andra slag av organisationer) eller på stora grupper och klasser av aktörer (t.ex. en genomsnittlig förhållandevis låg kunskap om källkritik). En annan kategori sårbarhet hänför sig till samhället i dess helhet, eller delar av samhället, vilka tenderar att förstärka aktörers, eller aktörsklassers, utsatthet avseende vilseledning med hjälp av Internet (t.ex. den allmänna utbildningsnivån i landet).

- Ett antal faktorer kan urskiljas vilka sannolikt påverkar den allmänna benägenheten i det svenska samhället till sårbarhet avseende vilseledning med hjälp av Internet. En uppsättning sådana omständigheter sammanhänger med infrastrukturen på Internet och dess sätt att fungera, t.ex. detta systems storlek mätt i faktorer som antalet användare, intensiteten i användningen, antalet webbplatser, på vilka information finns att söka liksom variationen i att kommunicera.

- Andra generella sårbarhetsfaktorer hänför sig till tekniska och andra rutiner som används för att försvåra / förhindra missbruk av Internet. Den allmänna sårbarheten avseende vilseledning torde reduceras med en förhöjd genomsnittlig skyddsnivå i datasystem och rutinerna för normal användning av Internet.

- Den allmänna kunskapsnivån och erfarenheten i samhället avseende användningen av Internet torde också kunna ha inverkan på den allmänna sårbarheten avseende vilseledning. Ju högre kunskapsnivå, ju mer erfarenhet – desto mindre allmän sårbahet.

---

46) I detta hänseende råder dock stora variationer mellan planeringsprocessens olika faser. Inför avgöranden, särskilt formella beslut, upprättas tidsgränser, vilka kan sätta press på beslutsfattarna.

DEL VII
FINNS DET SOM INTE SYNS?

Internet har, minst sagt, haft stor inverkan på att samhället ser ut som det gör idag i skilda avseenden och kommer med säkerhet att fortsätta påverka människornas villkor. Förenklat kan man se två motsatta trender: å ena sidan har den informationstekniska revolutionen givit oss ett större informationsutbud, fler valmöjligheter, ökad jämlikhet och spirande möjligheter till en mer levande och ”direkt demokrati”. Den har medfört ökad individualisering, fragmentering, frihet och ett större oberoende för individen. Å andra sidan har IT och Internet inneburit en internationalisering som bidragit till ett ökat ömsesidigt beroende mellan individer, företag, organisationer och stater. Ett uttryck för detta är att många organisationer – liksom individer – har ett växande behov av löpande information från omvärlden. Den ekonomiska, sociala och strategiska miljön är utvidgad och till viss del känsligare för informationsstörningar än tidigare. Detta innebär risker av ett nytt och annorlunda slag – däribland vilseledning på Internet.

I den här studien har vi diskuterat hur Internet har förändrat, eller skulle kunna förbättra, förutsättningarna för den som avsiktligt vill vilseleda en eller flera mottagare i det nya globaliserade samhället. Vi har också diskuterat om, och i så fall hur, man skulle kunna motverka den typ av vilseledning på Internet som skulle kunna generera oacceptabla konsekvenser. Den underliggande frågan har gällt informationssamhällets sårbarhet utifrån ett demokratiskt och säkerhetspolitiskt perspektiv. Vi har önskat belysa detta problemområde utan att svartmåla Internet, eftersom vi tror på dess enorma positiva möjligheter för såväl enskilda människor som för samhällsutvecklingen i stort.

Inledningsvis ställdes fyra övergripande frågor om vilseledning på Internet. Dessa frågor har varit utgångspunkter för resonemangen i studien. Vi skall nu försöka sammanfatta svaren på dem.

Fyra frågor besvaras

Hur genomförs vilseledning och hur skulle Internet kunna komma till användning i detta sammanhang?

Vilseledning är en form av inflytande som en aktör – sändaren – genom kommunikation uppnår över en annan aktör – mottagaren. Inflytande uppstår genom att sändaren påverkar mottagarens attityder, tankar, känslor och beteende. Framgångsrik vilseledning innebär att mottagaren bibringas en förvanskad bild av en del av verkligheten och på grund av detta beter sig så som sändaren önskar. Vilseledning kan åstadkommas på en rad olika sätt, men kan i stort hänföras till två grundformer: simulering respektive dissimulering. Man kan se på den avsiktliga vilseledningen som en vilseledningsoperation. En vilseledningsoperation är en konstruktion som inkluderar olika element i den avsiktliga vilseledningen. Dessa element är: sändare, syfte, underrättel-

ser, meddelande, kommunikation, mottagare, effekt. Framgången med en vilseledningsoperation beror på vad den s.k. plojen kan åstadkomma.

Plojen betingas av det konstruerade budskap – falskt eller sant – med vars hjälp sändaren vill påverka mottagaren. Budskapet från sändaren utgör emellertid endast en del av plojen. Den andra komponenten är dess presentation för den tänkta mottagaren, som förutsätter någon slags kommunikation. Internet kan användas för detta ändamål.

Interaktionen på Internet har egenskaper vilka skulle kunna underlätta iscensättandet av en vilseledningsoperation. Några exempel:

- Vilseledande information kan publiceras billigt och snabbt nå en stor publik.
- På Internet kan man med enkla medel skapa förtroende för sin person utan att behöva visa upp sig helt och hållet.
- Man kan göra intrång på Internet och ersätta eller ändra information eller få det att se ut som om viss information aldrig funnits.
- Det uppstår lätt rundgång i informationen på Internet och ogrundade rykten eller felaktig information sprids snabbt vidare samtidigt som det är svårt att kontrollera källan.
- Det finns goda förutsättningar för en sändare att dölja sin identitet eller att förfalska den.
- Den hårdnade konkurrensen och tidspressen skapar visserligen större öppenhet, men kan också leda till felbedömningar och förhastade beslut.
- Det finns möjlighet att manipulera inflödet av information till en mottagare.

Kommunikationen mellan sändare och mottagare kan vara upplagd på flera sätt och innebära olika typer av intervention i mottagarens användning av Internet. Vilseledning på Internet bygger på att någon, eller några av följande operationstekniker används: blockering (t.ex. bortkoppling, e-mailbombning, Denial of Service, SYN Flooding), informationsupphämtning (t.ex. kopiering av uppgifter eller avlyssning av datanät), sändning (kan vara öppen eller dold), ”att lägga agn” (t.ex. genom att lägga in tillrättalagd information på en eller flera webbplatser på Internet), kommunikation genom interaktion (t.ex. e-mail, e-maillistor, Usenet, ”chatting”).

De sexton verkliga fall som undersökts i denna studie bekräftar att avsiktlig vilseledning med hjälp av Internet som fenomen förekommer. Däremot vet vi inget om omfattningen av sådana aktioner. Den modell som används i undersökningen för att analysera fallen visar att dessa vilseledningsoperationer är ganska enkla till sin konstruktion och sitt sätt att fungera. Trots detta har i de flesta studerade fallen den taktik för vilseledning som prövats varit framgångsrik.

Skulle avsiktlig vilseledning på Internet kunna generera hot, i meningen få negativa konsekvenser för demokratin och den yttre nationella säkerheten?

De granskade vilseledningsoperationerna skiljer sig åt i flera viktiga hänseenden: (1) med avseende på *yttre omständigheter*; vilseledningen har t.ex. ägt rum inom ramen för enskilda individers privatliv eller i opinionsbildningskampanjer, i affärs- eller medievärlden, liksom att den också kommit till användning i propagandakrig mellan stater; (2) med avseende på *slaget av aktör* som uppträder som sändare respektive mottagare av vilseledning, t.ex. enskilda personer, företag, organisationer eller statliga institutioner; (3) med avseende på vilka *syften* som eftersträvas; t.ex. svart- respektive skönmålning av person eller objekt, kontroll / övertagande av resurser, störning av verksamheter i en organisation samt dold direkt beslutspåverkan; (4) med

avseende på vilka medel som används i såväl den slags *kommunikation* som operationen kräver som för att genom denna åstadkomma en vilseledningsploj, t.ex. falska e-post meddelanden, falska hemsidor eller interaktiv kommunikation i en grupp; (5) och med avseende på konstruktionen av den *ploj*, som användes i vilseledningsoperationen, ofta en kombination av simulering och dissimulering. Flertalet fall som analyserats inom ramen för den här studien har inte i sig själva någon säkerhetspolitisk innebörd. Samtidigt har bedömningen gjorts att många – dock inte alla – generaliserade mönster av vilseledningsoperationer som de sexton studerade fallen representerar (t.ex. beslutspåverkan, svartmålning eller störning av beslutsfattande), skulle kunna ha använts för säkerhetspolitiskt relevanta syften.

Studien pekar alltså på att avsiktlig vilseledning med hjälp av Internet har en stor användbarhet under varierande omständigheter. Ur ett säkerhetspolitiskt perspektiv måste denna variationsrikedom uppfattas som en varningssignal. Man kan befara att vilseledningsoperationer av den typ som undersökts i denna studie vid behov förhållandevis lätt skulle kunna anpassas till att tjäna syften av säkerhetspolitisk dignitet och riktas mot mycket säkerhetsmedvetna mottagare.

Ser man på hur vilseledning använts på det säkerhetspolitiska området tidigare i historien finns anledning att beakta risken med vilseledning med hjälp av Internet, även om det med säkerhet inte kan konstateras att sådan verksamhet förekommer idag. Läxan från de historiska exemplen (några nämndes i Del I) är att typer av vilseledning som av politiska och andra skäl inte skulle övervägas i en normal situation kan bli aktuella i en krissituation eller i en destabiliserad värld. Särskilt då vilseledningens eventuella politiska kostnader kommer att överskuggas av andra och mycket större risker för en potentiell sändare. Vid säkerhetspolitiska bedömningar (”worst case”) finns det skäl att misstänka att försök att vilseleda med hjälp av Internet skulle kunna tillta under sådana omständigheter.

Hur skulle man kunna motverka avsiktlig vilseledning på Internet?

Den ovan rapporterade analysen av motmedel visar att det inte finns någon enkel patentlösning för att hantera problemen med vilseledning på Internet. Detta beror i huvudsak på två förhållanden. För det första är många typer av motåtgärder förknippade med kraftfulla restriktioner. Ett exempel är polisiära åtgärder. Sådana kan genomföras endast avseende metoder för vilseledning som på något sätt är kriminella. Samtidigt skulle en vilseledningsoperation kunna få stor genomslagskraft i Sverige utan att sändaren behöver bryta mot lagen.

För det andra kan en mottagares känslighet för vilseledning i stor utsträckning sammanhänga med förhållanden som är situationsspecifika. En genomtänkt strategi måste därför vara en kombination av allmänna och riktade åtgärder.

En rad åtgärder har diskuterats som möjliga ”motmedel” mot avsiktlig vilseledning på Internet. Många av dessa försvarsansatser hänför sig till två områden; informationssäkerhet respektive kunskapsuppbyggnad. Rent tekniska säkerhetsåtgärder på IT-området, t.ex. skydd mot intrång, hänför sig i första hand till vilseledningens kommunikationsaspekt. Detta är en viktig åtgärd för att stå emot den typ av vilseledning som bygger på att vilseledaren olovligen tar sig in i mottagarens system. Det är inte heller ovanligt att de tekniker som används av en angripare även kan användas som skyddsåtgärd. Men tekniska försvarsåtgärder måste ofta kompletteras med andra metoder, bland annat för att den snabba tekniska utvecklingen skapar osäker-

het i detta hänseende. Ett annat skäl är att det tekniska skyddet alltid står i relation till upptäckt och reaktion.

Beredskap mot vilseledningens ploj handlar i stor utsträckning om att hantera perceptioner, kunskap, referensramar och andra psykologiska förhållanden, vilka inte alltid har något med IT eller Internet att göra. I slutänden bygger säkerheten därför mycket på att den enskilde mottagaren förbereds och ges förutsättningar för att förebygga och upptäcka vilseledning på Internet, samt att agera på ett så adekvat sätt som möjligt om han eller hon utsätts för vilseledning. Samhällets viktigaste beredskapsuppgift borde vara att sprida information och kunskap om Internet och om hur vilseledningsoperationer är uppbyggda, hur de fungerar och vilka slags effekter de kan åstadkomma. Det vill säga verka för en ökad insikt i och en kritiskt värderande hållning till den nya mediemiljön, inklusive Internet.

Vad återstår det för sårbarheter avseende vilseledning på Internet, när hänsyn tas till möjliga motåtgärder?

Sannolikt kan känsligheten i samhället för vilseledning på Internet begränsas till en lägre grad av sårbarhet genom ett väl genomtänkt program för motåtgärder. Emellertid måste man ta hänsyn till att kraften hos vissa motåtgärder i sin tur kan komma att begränsas genom samhällsutvecklingen. I det avseendet ska två aspekter särskilt beaktas: Den första synpunkten är att resursrika och / eller kunniga aktörer har möjlighet att med hjälp av Internet göra vilseledningsplojen mer raffinerad och effektiv än i de studerade fallen. Exempelvis var de falska webbplatser som förekom i ett par av de studerade fallen förhållandevis grova förfalskningar. Med litet större arbetsinsatser vore det enkelt att åstadkomma betydligt mer sofistikerade förvrängningar och falsarier.

Den andra synpunkten är att vissa aktörer också kan få motiv att göra stora satsningar på vilseledningsoperationer när säkerhetspolitiska eller andra stora värden står på spel. När motiven ökar, och de politiska kostnaderna för vilseledning minskar, kan således de motåtgärder, vilka hittills framstått som tillräckligt effektiva, börja förlora sin verkan.

Att undersöka det som inte syns

IT-hotet i allmänhet, och vilseledning på Internet i synnerhet, är som vi sett komplext och svårgripbart. När vi började med den här studien trodde vi att det skulle vara lätt att finna verkliga fall av vilseledning på Internet. Denna föreställning var även dominerande bland de personer vi intervjuade. Det visade sig dock ganska snart att det var lättare sagt än gjort. Framförallt saknades information om enskilda fall med tydliga säkerhetspolitiska förtecken. Dessutom var det svårt att finna exempel som genomlyste en vilseledningsoperations alla faser. Det fanns förvisso gott om exempel på att inkorrekt information presenterats på en webbplats. Emellertid var det brist på uppgifter om vilseledningens bevekelsegrunder, syften och effekter samt hur man åstadkommer dessa effekter (vilseledningens ploj). Den hotbild som växte fram byggde till stor del på osäkra uppgifter och enskildheter riskerade att uppförstoras och kanske övervärderas, medan helhetsbilden förblev otydlig. Därtill saknades en ändamålsenlig metod för att anlysera vilseledning på Internet.

Likt osynlig skrift?

Man kan då fråga sig: Tyder inte bristen på konkreta uppgifter att vilseledning på Internet av säkerhetspolitisk dignitet är ett skenproblem? Detta är naturligtvis en rimlig ståndpunkt, vilken emellertid måste prövas noga innan den fastslås.

Givet att vilseledning av säkerhetspolitisk betydelse faktiskt förekommer, kan den förväntas vara mycket svår att upptäcka. Detta är en verksamhet som för att vara framgångsrik för det mesta måste bedrivas i det fördolda. Lyckad vilseledning är normalt osynlig för alla utom för den som utövar den. Denne sändare har heller ingenting att vinna på att i efterhand skryta om sin framgång med en genomförd vilseledningsoperation. Tvärtom skulle de negativa konsekvenserna av en sådan öppenhjärtighet kunna bli betydande. Resultatet av operationen skulle kunna äventyras och sändaren skulle riskera att dra på sig politiska eller andra kostnader för att ha använt illegitima politiska metoder. Dessutom försämrar ett avslöjande förutsättningarna att använda samma vilseledningstrick vid ytterligare något tillfälle. Skulle mottagaren för vilseledningen upptäcka operationen har denne part också skäl att hålla tyst om detta för att inte vålla oro i omvärlden, exempelvis bland en regerings samarbetspartner eller ett företags aktieägare och kunder. Avsaknaden av upptäckta empiriska fall av vilseledning med säkerhetspolitisk relevans kan inte utan vidare tas till intäkt för att detta fenomen har försumbar betydelse. Detta gäller särskilt vid en säkerhetspolitisk bedömning, som måste ta hänsyn till att det värsta tänkbara skulle kunna hända. Möjligheten måste beaktas att vilseledning med säkerhetspolitisk relevans kan jämföras med osynlig skrift som finns men inte syns, men som kan göras synlig om den utsätts för en riktig behandling, till exempel några droppar saft från en citron. Med andra ord: Kan det vara så att det som inte syns ändå finns, och kan påvisas om bara den rätta analysansatsen används? För att ta reda på om det kunde vara så, utvecklade vi en särskild ansats för att studera vilseledning på Internet.

Några droppar citron

Undersökningen är explorativ och i första hand till för att bereda marken för kommande studier. Vi har använt olika slag av empiriskt material: litteratur, intervjuer och fall. Utifrån detta material har vi sedan utvecklat en ansats för att analysera området. Grundidén med den här ansatsen har varit att genom analys av harmlösa fall bygga upp en kunskap som ökar förståelsen för hur vilseledning med allvarligare konsekvenser skulle kunna se ut. Den stora variationsrikedomen avseende såväl aktörer, syften, kommunikationssätt, liksom i viss utsträckning plojens utformning i de studerade (relativt få) fallen – leder till bedömningen att vilseledning lätt skulle kunna användas av sådana aktörer, drivas av sådana syften och få sådana effekter att de skulle kunna generera hot mot den nationella säkerheten såsom detta begrepp uppfattas i denna rapport. För att få fram en nyanserad och komplett bild har vi utgått ifrån ett holistiskt analysperspektiv där hot, sårbarhet och möjliga motåtgärder kan analyseras med hänsyn till inbördes beroendeförhållanden. Ett annat skäl till det valda perspektivet har varit att diskussionen skall vara så relevant för området vilseledning på Internet som möjligt, och inte hamna i allmänna teknikfokuserade hotanalyser.

Mot denna bakgrund anser vi att det kanske viktigaste resultatet är den analysmodell som med framgång har prövats i undersökningen. Som några droppar citron på den osynliga skriften…

DECEPTION ON THE INTERNET A SUMMARY

by Gunnar Sjöstedt & Paula Stenström*

That individuals, groups, organisations, nations, companies, etc., attempt, in various ways, to deceive one another is, of course, not a new phenomenon, but has occurred throughout history and has recurrently been an effective political instrument in conflicts in which great areas of land are at stake. The forms and tools of deception, however, have changed during the course of history. This study addresses the question of the forms deception takes in our modern information society.

The Internet has had a great influence in making society what it is today and it will certainly continue to affect the human condition. The economic, social and strategic environment has been expanded and is in certain respects more sensitive to informational disturbance than it was previously. This implies risks of a new sort – among them deception on the Internet.

The study examines how the Internet has changed, or could improve, the prerequisites for a person who wishes to mislead one or several receivers of information in our globalised society. It also deals with whether, and if so and how, we can obstruct Internet-based deception that could have unacceptable consequences. The underlying question concerns the information society's vulnerability as seen from the perspective of democracy and security policy. This topic clearly represents a worst-case perspective, and we, the authors of the report, are well aware of the many beneficial effects of information technology and Internet. Our intention, however, is not to judge how ”dangerous” Internet-based deception is. Deception need not be illegal, nor should measures always be taken against it. *With respect to security policy, the ”danger” of deception is ultimately tied to its consequences – and not to its methods*. Our aim is instead to develop a starting point from which to study problem areas and thereby to increase understanding of the *potential* Internet-based deception could have as an instrument of power and influence.

Deception here means *dissimulation* or *simulation* for the purpose of changing an actor's perception or evaluation of a situation or phenomenon. For example, dissimulation may mean that some features of a given phenomenon are hidden or disguised so effectively that their appearance becomes more favourable in the eyes of those who are the objects of deception. In contrast, simulation, in order to attain

* *Gunnar Sjöstedt* is a researcher at The Swedish Institute of International Affairs (UI) and senior lecturer in political science at Stockholm University. *Paula Stenström* has a BSc in political science and was previously engaged at The Swedish Defence Research Agency (FOI) and The National Board of Psychological Defence (SPF).

the same effect, takes place when new characteristics are invented for deception purposes.

Studies of information technology (IT) threats are often focused on technical vulnerability. But in an investigation of deception on the Internet, factors other than the technological must be included, such as the actors, intentions, strategies and not least the possible effects of the deception. Given this ambition, "deception on the Internet" proved to be a complex as well as relatively unexplored area. It was not least for this reason that we found the topic interesting. As a first step, we felt it was important to get as close to reality as possible. We have tried to accomplish this partly through *interviews* with various actors with great experience and knowledge in relevant areas (media, industry, the judicial system, defence and the central public administration), and partly through identifying and collecting concrete *cases* of Internet-based deception.

Sixteen cases are examined in which one person, or organisation, has attempted to deliberately deceive another party with the help of the Internet in order to achieve a specific objective, such as character assassination or economic gain.

All cases of deception included in the study produced a situation that should have been disturbing, or at least irritating, to those who were the targets of deception. For example, in one case, men looking for a prostitute had harassed a young lady. These men had found her address and telephone number on a fabricated advertisement on the Internet, which had been set up by a vengeful former boyfriend. In several other cases, an individual, a product or a firm had likewise been vilified in some way or another. However, none of the cases studied included actions that required or motivated extraordinary measures by those institutions that share the responsibility for protecting society from internal or external security threats. In most cases, the deception measures undertaken did not even represent criminal acts.

Still, the purpose of this study has been to assess how Internet-based deception *could have* intolerable repercussions for democratic processes or national security in a country such as Sweden. The search for actual current incidents of deception with such sinister consequences has been virtually fruitless. However, our position is that this result cannot be interpreted as a guarantee that deception on the Internet will never in fact produce real threats. For example, it is not inconceivable that some actors could, in a case of societal or economic destabilisation, lose their normal inhibitions and use measures such as malignant deception to defend their interests. Either the stakes will then increase dramatically for some actors or the prevalent norm system will begin to break down. Therefore, it is important to find ways to improve our knowledge of deception on the Internet; how it might occur and how it might affect selected targets, thus causing negative repercussions for democracy and national.

A crucial issue in this project has been how to – based on the sixteen cases included in the study – draw conclusions about the security significance of deception on the Internet. One approach is that of generalisation. It can be argued that all incidents of deception, regardless of their intentions and effects, share certain basic elements that can be captured with the help of the analytical concept *deception operation*. Departing from the common understanding of deception as *simulation* or *dissimulation* of actors, phenomena or events, deception operation captures the key elements of a process leading to the outcome that one actor (e.g., the agents of a firm) purposefully deceives other actors (e.g., likely clients

of another company). In order to permit systematic comparison of cases, the theoretical conception of ”deception operation” has been reframed into more operational terms highlighting the following elements: *deceiving agent, target of deception, deception aims, deception ploy, deception tools, and impact on target*. The case analyses strive to elucidate these elements to the highest degree possible.

A general overview of the sixteen cases reveals little of significance for Swedish security concerns. The basis for generalisation from tolerable to malignant cases of Internet-based deception rests in its ”toolbox” and the range of operational methods that are directly linked to it. The comparative analysis reveals that the methods used for trivial deception purposes are flexible, easily adaptable to different kinds of situations and purposes, including national security concerns. Thus, with the help of invented scenarios, we elaborate on how deception techniques used for trivial purposes could be employed for more sinister purposes related to national security.

One of the concluding chapters of the report discusses and assesses the vulnerability of Swedish society in the face of possible threats represented by deception operations aided by the Internet. Another concluding chapter concerns feasible counter-measures in a democratic polity situated in an open society. In such a setting, certain control measures undertaken by state authorities might be regarded as more disturbing than the occurrence of disinformation and deception.

REFERENSER

Intervjuer

Intervjuer har gjorts med representanter från medier, näringsliv, rättsväsende, försvar och den centrala statsförvaltningen. Syftet med intervjuerna har varit att förankra undersökningen till olika beslutssituationer, rutiner, attityder och erfarenheter med avseende på vilseledning med hjälp av Internet och besläktade frågor.

Ulf Petersson, Managing Director, *Provesta Country and Business Analysis.*

Lennart Brittner, Försvarsdepartementet (arbetar med politisk och militär omvärldsanalys för Försvarsdepartementet, UD och Statsrådsberedningen).

Magnus Ek, Vice President, *Risk Management and Security* Telia AB Risk Management.

Christian Palme, *Dagens Nyheter.*

Mats Björe, f.d. chef för MUST SÖK (militära underrättelsetjänstens avdelning för omvärldsanalys via öppna källor).

Anders Lignell, utrikeschef på TT.

Jon Karlung, VD på Internetoperatörföretaget Bahnhof International AB.

Björn Häger, journalist på Sveriges Radios nyhetsredaktion och ordförande i föreningen Grävande journalister.

Anders R Olsson, frilansjournalist och vice ordförande i föreningen Grävande journalister.

Paolo Felix, arbetar med IT-relaterad brottslighet på Europol.

Föredrag m.m.

Under 1999 och 2000 har författarna deltagit i ett antal konferenser, kurser, workshops, seminarier och föredrag inom olika områden med anknytning till vilseledning på Internet. Dessa har på många sätt varit betydelsefulla för att hålla sig à jour med diskussionen om sårbarhet på IT-området, och för att få bättre förståelse för hur man tänker inom olika områden.
Några tillfällen som kan nämnas är:

”IT-samhällets utveckling och sårbarhet” *– konferens anordnad av Stockholms läns försvarskommitté* 11-12 mars 1999.

ÖCBs forskningsdagar 16-17 mars 1999.

Kurs i Psykologiska Operationer (PSYOPS) *på Försvarshögskolan där bl.a. Maj John Beer från den brittiska underrättelseskolan Chicksand föreläste* (v. 9 1999).

Seminarium och möte om informationskrigföring på Försvarets forskningsanstalt, avdelningen för försvarsanalys 28 och 29 april 1999.

InfoWarCon i London anordnat av MiS Training och Winn Schwartau 26-28 maj 1999.

Seminarium på Utrikespolitiska Institutet om JMG Granskarens resultat av *"Svenska medier om Kosovo"* juni 1999.

"A short course in information warfare", *seminarium på Försvarshögskolan med Dan Cuehl från National Defence University* 21 september 1999.

"Medel, strukturer och policy inom området informationskrigföring" – *rapportseminarium med Anna Sundberg,* Försvarshögskolan 30 september 1999.

"IW in The Middle East", *seminarium av Ariel Sobelman från Centre for Strategic Studies, Tel-Aviv University* på Försvarets forskningsanstalt, avdelningen för försvarsanalys 1999.

"När ord blir vapen – medier i krig", journalistseminarium, Karlstads Universitet 6 oktober 1999.

Rikskriminalens konferens om IT-kriminalitet, Eurostop 22-23 februari 2000.

Föredrag av James Adams (iDefence) på Försvarshögskolan, 14 mars 2000.

Litteratur

Litteraturen är hämtad från många olika områden, bl.a böcker om Internet och demokrati, om påverkan i informationssamhället och vilseledningsstrategier. Statliga utredningar, nationell och internationell press, webbplatser, elektroniska nyhetsbrev, konferensmaterial, avhandlingar etc.

Brottsförebyggande rådet; *IT-relaterad brottslighet,* BRÅ-rapport 2000:2.

Carlén-Wendels, Thomas; *Nätjuridik – Lag och rätt på Internet,* Norstedts Juridik AB, ISBN 91-39-20134-1 Stockholm 1998.

Carlsson, K. Dellström, S. Eriksson, M. Roxberg, M; *Propaganda och Internet – innehållsanalys av fyra proserbiska webbplatser, B-uppsats i Journalistik och Multimedia* vid Södertörns högskola 31 maj 1999.

Cordesman, Anthony H; *Defending America – Redefining the Conceptual Borders of Homeland Defense,* Critical Infrastructure Protection and Information Warfare Center for Strategic and International Studies (CSIS), Rough draft comment 16 juli 2000.

Engström, Ulf & Jan Sandgren; *Etik och Internet – en kompass i Cyberrymden,* Argument Förlag Uppsala Publishing House, Tryckeri AB Småland Quebecor, Jönköping 1999 ISBN 91-7005-162-3.

Eriksson, Anders E. & Malin Fylkner; *IT-related Threats in the Network Society – Suggestions for a Swedish Proactive Agenda,* Försvarets Forskningsinstitut (FOI) december 1999, ISSN: 1104-9154.

Furustig, Hans & Gunnar Sjöstedt; *Strategisk omvärldsanalys,* Studentlitteratur 2000, ISBN 91-44-01216-0.

Fylkner, Malin, Josefin Grennert & Eva Mittermaier; *Internationellt samarbete kring IT-hot – Aktörer och initiativ – några exempel,* Försvarets forskningsinstitut (FOI) FOA-R–00-01517-170–SE 2000.

Försvarsdepartementet; *Regleringsbrev för år 2000 avseende Styrelsen för psykologiskt försvar.*

Försvarsdepartementet; *Ds 1999:55 Europas säkerhet – Sveriges försvar,* Försvarsberedningen, Regeringskansliet.

Försvarsmakten; *Ledningskrigföringsstudie* H 21 120:8462 1998.

Haswell, J; *The intelligence and deception of the D-day landings,* Batsford: London 1979.

Howard, John D; *An Analysis of Security Incidents on the Internet 1989-1995,* Doktorsavhandling (stencil), Carnegie Mellon University (CMU), Carnegie Institute of Technology 1997. CMU är kopplat till CERT / CC (Computer Emergency Response Team Coordination Center).

Häger, Björn & Anna Strömblad; *Internet – en handbok för faktasökare,* Sveriges Radios Förlag, BTJ Tryck AB, Lund, december 1998.

Jakobsson, Peter; *Internet som strategiskt kommunikationsverktyg,* Studentlitteratur Lund 1995, 1998 ISBN 91-44-00338-2.

Keohane & Nye; *Power and Interdependence,* andra upplagan 1989.

Küchler, Marcus; *Dataintrång – om personlig integritet och bevisfrågor,* Examensarbete i rättsinformatik, Stockholms Universitet 2000.

Lerdell, David; *Hanteringen av IT-relaterade säkerhetsfrågor inom Internetorganisationerna,* Försvarets forskningsinstitut (FOI) FOA-R-00-01460-170-SE, 2000.

Leth, Göran & Torsten Thurén; *Källkritik för Internet,* Styrelsen för psykologiskt försvar, rapport nr 177, 2000.

Mittermaier, Eva & Peter Westrin; *Infrastrukturens sårbarhet med avseende på logiska, IT-relaterade hot,* Försvarets forskningsinstitut (FOI) FOA-R-99-01052-240-SE 2000.

Nordicom; *Mediebarometer* 1999 i samverkan med CIA Marketing, Dagens Nyheter, Dagspresskollegiet, Göteborgs Universitet, Göteborgs-Posten, Styrelsen för psykologiskt försvar, Sveriges Radio, Sveriges Television och TV4.

Nationalencyklopedin, Band 9 (HIM-ISSK), uppslagsord: ”informationsteknik”, Bokförlaget Bra Böcker AB: Höganäs 1992.

Nordfors, Lennart & Bert Levin; *Internetrevolutioner,* Ekerlids Förlag Fälth & Hässler, Smedjebacken, oktober 1999.

Norgren, Bo (Kriminalinspektör); *Informationsoperationer och skydd av kritisk infrastruktur – vilken roll har Law Enforcement?* Försvarshögskolan, Operativa Institutionen, Informationskrigskansliet 2000.

Nydén, Mikael; *Hotet från IT,* Styrelsen för psykologiskt försvar, meddelande 138, 1995.

Nydén, Mikael; *Myndigheter, Internet och integritet,* Styrelsen för psykologiskt försvar, meddelande 153, 2000.

Nørretranders, Tor; *Platsen som inte finns – en bok om Internet,* Bokförlaget DN 1998 (Originaltitel: ”Stedet som ikke er”) Första utgåva: Aschehoug, Köpenhamn 1997) ISBN 91-7588-191-8.

Post- & Telestyrelsen (PTS); *Exempel på IT-incidenter,* PM 16 mars 2000 (bilaga till utredning om oberoende Internet).

PTS; *Förutsättningar för att inrätta en särskild funktion för IT-incidenthantering,* 28 november 2000, Dnr 99-19448.

PTS; *Översikt över funktionen för IT-incidenthantering,* 18 februari 2001, Dnr 01-8289.

Regeringens försvarsproposition 1998/99:74; *Förändrad omvärld – omdanat försvar.*

Regeringens försvarsproposition 1999 / 2000:30; *Det nya försvaret.*

Regeringens proposition 1999/2000:86; *Ett informationssamhälle för alla.*

Regeringsbeslut; *N1999/11654/ITFoU,* 25 november 1999.

Riksrevisionsverket; *Datorrelaterade missbruk och brott,* En kartläggning gjord av Effektivitetsrevisionen RRV 1997:33.

Rothstein, Bo; *Demokrati som dialog,* SNS Stockholm 1995,

Sjöstedt, Gunnar; *Desinformation, vilseledning och nationell säkerhet,* Styrelsen för psykologiskt försvar, rapport 148, 1988.

SOU 1992:110; *Datastraffsutredningen.*

SOU 1995:19; *Ett säkrare samhälle,* Huvudbetänkande från Hot- och riskutredningen, Försvarsdepartementet, Norstedts Tryckeri AB, Stockholm.

SOU 1995:47; *Polisrättsutredningen.*

SOU 1997:73; *Säker elektronisk kommunikation* (IT-kommissionens rapport 6 / 97).

SOU 2000:1; *Demokratiutredningen.*

SOU 2000:55; *Radio och TV i allmänhetens tjänst – ett beredningsunderlag, Slutbetänkande.*

Statskontoret; *Offentlig förvaltning och demokrati i informationssamhället,* 1998:2 Williamssons Offset, Solna 1998
ISBN: 91-7220-300-5.

Stenström, Paula; *Lönande lögner* FOA-R-9700483-240-SE oktober 1997, ISSN 1104-9154.

Stenström, Paula; *Med sanningen som insats,* FOA-R-98-00697-111-SE, januari 1998, ISSN 1104-9154.

Stenström, Paula & Åke Wiss; *Pålitlig påverkan,* FOA-R-99-01057-170-SE, mars 1999, ISSN 1104-915.

Svenska Akademiens ordlista 1998.

Taylor, Philip; *Psychological Operations in the Post Cold War Era,* University of Leeds (stencil) 2000.

The Presidents Working Group on Unlawful Conduct on the Internet; *The Electronical Frontier; The Challenge of Unlawful Conduct Involving the Use of the Internet,* februari 2000.
www.politechbot.com / docs / unlawfulconduct.txt.

Thurén, Torsten; *Källkritik,* Almquist & Wiksell, Falköping 1997.

Truedson, Lars; *Internet och demokratin*, Världspolitikens Dagsfrågor 1999:6, Utrikespolitiska Institutet.

Wik, Manuel W; *Informationsoperationer – en strategi för fred. Informationskrigföring – en avgörande spjutspets i krig*, Särtryck ur Krigsvetenskapsakademiens Handlingar och Tidskrift, 3 häftet 1999.

Åkerström, Marja; *Internet och demokratin*, Media and Communication Studies, Lund University Workingpaper 1999:2.

ÖCB-rapport till regeringen; *Infrastrukturuppdraget* – om sårbarheten i den tekniska infrastrukturen, Överstyrelsen för Civil Beredskap (ÖCB) Dnr 5-183 / 99 daterad 15 mars 2000, ISBN 91 7097 069-6.

Österman, Torsten; *Förtroende*, Styrelsen för psykologiskt försvar, meddelande 148, 1999.

Artiklar

Adams, James; ”How did we top Gutenberg? And Where do we go from here?” CEO, Infrastructure Defence Inc. (iDEFENCE) *Internet World* 5 februari 1999.

Adams, James; ”The Future of Publishing” utskrivet tal från *Seybold Seminars Panel* San Fransisco september 1998.

Adams, James; ”OPINION: Hacker Pranks Are No Laughing Matter” *The Bridge News Forum* (daterat 8 juni 1999) Bridge Information Systems, Inc. www.bridge.com

Bolander, Hans; ”IT-bolagen sprider vilseledande information” *Expressen* 23 november 1999.

Center for Strategic and International Studies (CSIS); ”Critical Infrastructure Protection and Information Warfare”, 16 juli 20.

Eriksson, Göran; ”Kamp mot ekonomins makt”, *Dagens Nyheter,* 13 juli 2000.

Geary, James; ”How to Spot a Liar”, *Time*, (London) 13 mars 2000.

Gustavsson, Lena; ”Analys ger säkrare IT-system” artikel i *Beredskap* (utges av Överstyrelsen för civil beredskap, ÖCB) nr 1, 2000.

Jigenius, Pär-Arne ”Övertramp på nätet hotar hela processen”, Debattartikel i *Dagens Nyheter* 24 november 1999.

Knightley, Philip; ”Så skapas ett krig” (översättning Ola Larsmo), *Dagens Nyheter,* Kultur, 19 november 1999.

Kälvemark, Torsten; ”Den fria debatten finns på nätet”, *Aftonbladet*, Kultur, 20 april 1999.

Lacayo, Richard m.fl; ”Rage Against the Machine: despite, and because of, violence, anti-WTO protesters were heard”, *Time,* 13 december 1999.

M2 Communications, London 18 juni 1999.

Mitalka, M.; ”Soviet Strategic Deception, 1955 – 1981” *Journal of Strategic Studies*, Vol. 5, Nr.1, 1982.

NIPC Watch, 7 december 1999 och 2 februari 2000.

Udén, Cecilia; rapport för Dagens Eko, *Sveriges Radio* från Washington, 5 januari 2000.

Uppsnappat klipp från nr 370, 29 augusti 2000.

Wästberg, Olle; ”Kan vi lita på våra ögon?” Krönika i *Arbetet*, Nyheterna, augusti 1999.

SPFs SENASTE RAPPORTER

184 **Nordström, Gert Z**: *Terrorkriget i kvällspressen*. Stockholm 2002.

183 **Sjöstedt, Gunnar & Stenström, Paula**: *Vilseledning på Internet – en analysansats*. Stockholm 2002.

182 **Hedquist, Rolf**: *Trovärdighet – en förutsättning för förtroende*. Stockholm 2002.

181 **Pettersson, Rune**: *Bildmanipulering*. Stockholm 2001.

180 **Pettersson, Rune**: *Trovärdiga bilder*. Stockholm 2001.

179 **Larsson, Larsåke & Nohrstedt, Stig Arne** (Red.): *Göteborgsbranden 1998: En studie om kommunikation, rykten och förtroende*. Stockholm 2000.

178 **Ghersetti, Marina & Hvitfelt, Håkan**: *Slutet på sagan: Prinsessan Dianas död i press, radio och tv*. Stockholm 2000.

177 **Leth, Göran & Thurén, Torsten**: *Källkritik för Internet*. Stockholm 2000.

SPFs SENASTE MEDDELANDEN

160 **Bennulf, Martin**: *Nya hot och risker. Opinion 2001. Den svenska allmänhetens syn på samhället, säkerhetspolitiken och försvaret*. Stockholm 2001.

159 **Palm, Lars & Nilsson, Anna**: *Föreställningen började innan publiken anlänt: En analys av regeringens folkbildningsinsats om EMU*. Stockholm 2001.

158 **Norling, Anna**: *Olycksplats Borlänge bangård*. Stockholm 2001.

157 **Malešič, Marjan**: *Peace Support Operations, Mass Media, and the Public in former Yugoslavia*. Stockholm 2000.

156 **Stütz, Göran**: *Opinion 2000. Den svenska allmänhetens syn på samhället, säkerhetspolitiken och försvaret*. Stockholm 2000.

155 **Åkerström, Marja**: *Sanning eller konsekvens? Argument och perspektiv i mediedebatten under 1998 och 1999 om den svenska underrättelse- och säkerhetstjänstens personalkontroller*. Stockholm 2000.

154 *Nyhetsbilder–etik–påverkan*: En antologi. Stockholm 2000.

153 **Nydén, Michael**: *Myndigheter, Internet och integritet*. Stockholm 2000.

VILSELEDNING PÅ INTERNET – EN ANALYSANSATS

Internet innebär oerhörda möjligheter i yrkesliv och utbildning liksom för demokrati och rekreation. Men Internet kan missbrukas – och missbrukas! Det finns t.ex. ingen garanti för att informationen på webbsidor eller i e-postmeddelanden är korrekt.

Denna studie vill diskutera på vilket sätt Internet skulle kunna utnyttjas för medveten vilseledning med så allvarliga konsekvenser så att demokratin och den nationella säkerheten hotas. Sexton exempel på avsiktlig vilseledning med hjälp av Internet i privat- och affärslivet har undersökts med hjälp av ett särskilt utvecklat analysschema. Därefter analyseras vilseledningsteknikerna i de undersökta fallen för att visa hur dessa skulle kunna användas för andra syften som sammanhänger med demokrati och nationell säkerhet.

Gunnar Sjöstedt är forskare vid Utrikespolitiska institutet (UI) och docent i statskunskap vid Stockholms universitet.

Paula Stenström är fil kand i statsvetenskap och tidigare verksam vid Försvarets forskningsinstitut (FOI) och Styrelsen för psykologiskt försvar (SPF).

Tryckbolaget AB, Stockholm, 2002.

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