Innehåll

1. Sammanfattning

Huvuddelen av all omvärldsbevakning använder idag öppna källor för inhämtning av information, både inom företag och de flesta myndigheter. Öppna källor är sådana som man har tillgång till utan att bryta mot lagen eller bete sig oetiskt, t ex tidningar och annan media, marknadsföringsmaterial mm.

En av de mest betydelsfulla konferenserna kring användningen av öppna källor för omvärldsbevakning är Open Source Solution, OSS´97. Konferensen tar främst ett myndighetsperspektiv men har under de senaste åren lockat allt fler deltagare från det privata näringslivet. När det gäller just öppna källor finns det stora likheter mellan myndigheter och företag och dessutom mycket att lära av varandras erfarenheter.

För främst polisiära och militära organisationer har de senaste åren inneburit stora förändringar vad gäller användningen av öppna källor. Också tekniskspridningen till privatpersoner som t ex GPS, kryptering och satellitbilder har inneburit att stater inte längre har monopol på teknik som tidigare enbart använts av polis och militär.

Även samhället i stor har förändrat synen på information. Med exempel från sovjetimperiets fall belystes hur öppna samhällen stärks medan slutna samhällen förtvinar och går under.

Internet är ett självklart debattämne när öppna källor diskuteras. Det var dock slående hur spridda uppfattningarna var kring Internets värde som verktyg för omvärldsbevakning. Debatten tydde också på svårigheter att hålla isär Internet som kommunikationsmedium och media i sig (WWW).

Ett genomgående tema från flera talare under konferensen var nyttan och behovet av att skapa informella nätverk inom och utom den egna organisationen. Med hjälp av sådana nätverk av experter kan man bevaka mycket större områden än vad man annars skulle mäkta med egen kraft. Men för att ett nätverk ska fungera krävs att kommunikationen är lika intensiv i alla riktningar, dvs att alla både bidrar och tar emot.

Flera intressanta fallstudie redovisades. Speciellt uppmärksammades Oxford Analyticas arbetsmodell som bygger just på en lite kärna av fasta medarbetare som har tillgång till en stor stab av externa experter. Med denna modell bedriver Oxford Analytica ett närmast industriellt bevakningsarbete. Oxford Analytica är förvisso unika, men deras metod förtjänar att studeras och kan realiseras i mycket mindre skala.

Baksidan på myntet "öppna källor" är självfallet att information om det egna företaget sprids okontrollerbart samt att konkurrenter bättre bevakar sin offentliga informationsprofil. Begrepp som Information Warefare och informationsäkerhet blir därför allt viktigare i dessa sammanhang.

OSS´97 bjöd även på en mindre men likafullt intressant utställning där leverantörer av produkter och tjänster deltog. Främst märktes amerikanska Mitres system för automatisk indexering av video (CNN Headline News), men även avancerad databasteknik för dokument visades.

2. Öppna källor för omvärldsbevakning

Inom såväl myndigheters som företags omvärldsbevakning spelar öppna källor en allt större roll. Information från öppna källor som reklam, myndigheter, tidningar och nyhetsbyråer ger det sammanhang som krävs för att förstå viktiga skeenden i samhälle och industri.

Öppna källor är sådana källor som man kan ta del av helt fritt, utan att bryta mot lagliga eller etiska regler. Andra, skyddade, källor har framförallt utnyttjats av militära och andra statliga underrättelseorgan som med satelliter och människor spionerar på motståndare. Men även vissa företag ägnar sig åt sk industrispionage där man med olagliga eller åtminstone oetiska metoder tar del av annans hemliga information.

Traditionellt har myndigheter och militär huvudsakligen litat till sina egna informationskällor och i liten grad visat intresse för eller baserat sin analys på den information som flödar öppet i samhället. Men användningen av öppna källor ökar sakta men säkert i takt med att man får upp ögonen för den kvantitet, men också kvalitet, av information som finns tillgänglig.

En av de mest betydelsefulla konferenserna som behandlar omvärldsbevakning är Open Source Solution (OSS). Årets upplaga, OSS'97, hölls i Washington D.C. i september 1997 och besöktes av drygt 400 personer. OSS-konferenserna har hållits under sex år och lockar främst deltagare från militär och myndigheter från västvärldens stater. Men i användningen av öppna källor finns mycket gemensamt att diskutera med näringslivets omvärldsbevakare och OSS lockar allt fler ur den kommersiella sektorn. När det gäller metod och IT-stöd för omvärldsbevakning är det betydligt mer som förenar än som skiljer privata och statliga aktörer åt.

KGB-general saknar förståelse

Konferensen erbjöd många erfarna talare ur olika "branscher", från pensionerade KGB-generaler till meriterade omvärldsbevakare inom näringslivet. Ett gemensamt drag var dock att alla upplevde en brist på förståelse i allmänhet om betydelsen av omvärldsbevakning med öppna källor, inte minst från sina respektive organisationers ledning.

Bland talarna från näringslivet märktes främst Max Downham, ansvarig för det omskrivna och framgångsrika Business Intelligence-arbetet inom företaget Nutrasweet. Downham, som presenterades som den av många åberopade titeln "the father of Business Intelligence" inledde med att frankt påstå att "*The concept of Business Intelligence is not understood among the business community*". Den främsta orsaken är okunskap, inte ens idag finns utbildningsprogram för omvärldsbevakning vid de prestigefyllda lärosätena Harvard och Yale. Bristen på insikt om omvärldsbevakningens betydelse leder till att många företag inte satsar på sådan verksamhet fastän det skulle vara direkt lönande. För att ge tyngd åt uttalandet att det är lönande för privata företag att bevaka sin omvärld redovisade Max Downham att hans chef, Bob Flynn, beredvilligt skröt om hur Nutrasweets satsning på Business Intelligence varje år sparade 50 miljoner dollar åt företaget.

Att förändringen för militär och polisiära myndigheter kan vara väl så stor visade flera av talarna. Till exempel har polisväsendet, av tradition en gammaldags hierarkisk organisation, haft det mycket svårt att förändra sig vad gäller arbetssätt och användning av andra källor än de vanliga,

berättade den belgiske poliskaptenen Patrick George som bl a ansvarade för utredningen kring den belgiska pedofilhärvan. Endast med exemplets makt kunde han övertyga sina överordnade om att börja använda öppna källor.

- Inte förrän jag visat mina överordnade hur jag på 30 sekunder kunde finna pedofiler på Internet fick de upp ögonen för Internets betydelse som källa, menade han.

De senaste årens förändringar i omvärlden, med bl a avsaknaden av Sovjetunionen och ett utökat europeiskt samarbete, har för världens nationer gett en markant avspegling i synen på aktuell hotbild. Dagens hot handlar många gånger om terrorism och ekonomisk krigföring, hot som tydligare kan kartläggas genom att analysera öppen information snarare än att skicka ut spioner och spionsatelliter. Ett exempel är att många extremistgrupper tämligen öppet annonserar sina avsikter på Internet.

Denna förändrade hotbild leder också till en förändrad syn på traditionell underrättelsetjänst, nämligen att öppna källor ger allt viktigare information även inom områden där man av tradition föredragit hemligheter. Vad har då orsakat förändringen i synen på öppna källor inom militären? Det är främst tre faktorer, enligt Patrick Tyrell från den brittiska underrättelseskolan:

- Informationens ökade tillgänglighet via elektroniska media,
- synen på hur information kan användas (jmf TV-kriget i Kuwait) och även
- de allmänna ekonomiska faktorerna med en allt högre förändringstakt, minskad byråkrati och mindre hemlighetsmakeri under den mildrade hotbild som råder efter kalla krigets slut.

Kring insikten om öppen informations betydelse för staters och företags omvärldsbevakning uppstår också en insikt om behovet av att skydda sin information och sina informationssystem. Givna ämnen under OSS var därför informationssäkerhet och det något mer offensiva Information Warfare, dvs krigföring med information som mål.

Öppenhet ger starka samhällen

En möjligen naturlig men knappast särskilt effektiv åtgärd är att öka hemlighållandet av t ex offentliga register. Speciellt fransmannen Maurice Botbol, redaktör för nyhetsbrevet Intelligence Review, hyllade det öppna samhället och såg det samtidigt som en förutsättning för ett starkt och framgångsrikt samhälle.

Kontrasten är det slutna samhället, det som strävar efter att hemlighålla information för omvärlden men även för sin egen befolkning. Denna förkärlek för hemligheter föder lätt ett antal problem som t ex maktmissbruk och korruption, menade Botbol, och pekade på exempel som Sovjetunionen. Dock har information en inneboende kraft som gör att den sprider sig, en process som hemligstämplar kan tjänar till att påskynda. En sådan spridning av information ger på sikt kunskaper som kan leda till det slutna samhällets uppluckring och till och med fall eller nedgång. Återigen kan man dra parallellen till det extremt slutna sovjetväldet som till slut fick oerhört svårt att behålla kontroll över informationsflödet, något som säkert påskyndade unionens splittring.

Även mindre dramatiska exempel är slående. I Frankrike tillämpar man en 50-årig preskriptionstid innan man generellt upphäver en hemligstämpel. Detta gäller t ex hemligstämplade dokument från andra världskriget som först blev tillgängliga för några år sedan medan i stort sätt samma dokument, åtminstone de som rör kommunikation mellan de allierade, fanns tillgängliga i amerikanska arkiv redan på 60-talet beroende på att USA tillämpar en blott 25-årig preskriptionstid. Konsekvensen för Frankrike blev att historiker som strävade efter att skriva andra världskrigets historia vände sig till USA och dess arkiv för sin bakgrundsforskning. Materialet som de fick tag i var ju då givetvis mera färgat av amerikanska åsikter än om de hade fått tag i de ursprungliga dokumenten ur franska arkiv. Historien har därför fått en mera amerikansk vinkling än vad som troligen hade varit fallet om franska uppgifter också hade kunnat granskas innan historieböckerna skrevs.

En snabb teknisk utveckling har också gett allmän tillgång till avancerad teknik som för bara några år sedan var topphemlig och förbehållen militären. Nyligen topphemlig teknik som kryptering kan idag användas av skolbarn på Internet och satellitbilder med god upplösning kan köpas på den privata marknaden. Ett närliggande exempel är svenska SSC Satellitbild som på sin webtjänst Spacepix (www.spacepix.com) säljer satellitbilder för mindre än tio dollar. Starka nationer kommer att släppa sina hemligheter efter hand med positiva effekter för den egna ekonomin medan de svaga nationerna kommer att överbeskydda sina.

Är fri information dålig information?

Bland de öppna källorna skiljer man ofta på informationstjänster med gratis information och värdeadderande betaltjänster. Det fanns stundtals en känsla av att en tjänst som kostar pengar automatiskt innebär bättre kvalitet, men detta synsätt pekar snarast på svårigheten att verkligen ta till sig användningen av öppna källor. Ett av de viktigaste uppgifterna vid analys av information från öppna källor är källkritiken, dvs att utvärdera trovärdigheten hos källan. Det var en besvikelse att notera att en seriös diskussion i detta avseende saknades under OSS'97.

Ett annat ämnesområde som kunde behandlats bättre var användningen av Internet där talarna intog en minst sagt splittrad hållning. Från att utnämnas till den främsta bland källor av vissa, till ett resursslöseri och "Analyst Eater" av andra. Argumenten var dock luddiga och debatten stundtals naiv. Speciellt hade man svårt att skilja på Internet som en öppen källa, dvs publika World Wide Web-tjänster, eller som en allmänt tillgänglig infrastruktur för kommunikation.

Maurice Botbol, som bland europeiska myndigheter har undersökt inställningen till Internet som kanal för omvärldsbevakning, menar att många upplever Internet som en förstahandskälla som är överlägsen färdigbearbetade analyser från analysföretag. Internet upplevs alltså av dessa myndigheter som den bästa öppna informationskällan. De största problemet med dagens öppna källor är dock bristen på trovärdighet, kvaliteten måste bli bättre.

Men belgiske polisen Patrick George var tveksam. Alla nya tillgängliga informationskällor hotar att skapa ett kvävande informationsöverflöd och det är helt enkelt inte effektivt att själv analysera alla förstahandskällor. Även polismyndigheterna måste upphöra med att göra all undersökning själva från början och istället använda sammanställda analyser som gjorts av andra, exempelvis inom den kommersiella sektorn. Det är enda sättet att istället gå mot minskat informationsöverflöd. På köpet får man också högre effektivitet och lägre kostnader.

Det är utan tvekan så att uppkomsten av en ny global infrastruktur för kommunikation innebär radikalt nya möjligheter för omvärldsbevakning. Med en snabbt ökande digitalisering av media och med Internet som en distributionskanal kan mer öppen information bevakas av fler individer än någonsin tidigare. Men som i all omvärldsbevakning är det viktigt att analytikern känner sina källor och de medium som används. En ännu ovan internetanvändare kan kanske förlora sig i ändlöst surfande, men bevisar i det inte mycket mer än sin bristande professionalitet. Som någon sade, en bra analytiker "vet när det är dags att sluta söka och börja betala"!

Det är också ett faktum att allt fler av de mycket innehållsrika databasvärdar som tidigare erbjudit sina tjänster via modemförbindelser nu börjar använda Internet som distributionsmedium. Databasvärdarnas tjänster kommer självfallet inte att vara tillgängliga via Alta Vista eller andra sökmotorer, utan enbart för betalande kunder på skyddade webplatser. Internet (WWW) verkar vid en första anblick vara oerhört stort och välfyllt – men tjänster som DIALOG uppger att de är ännu större och har bättre kvalitet på sina data. Enligt en källa från Knight Ridder, som äger DIALOG, är deras datamängd cirka 20 gånger större än den del av World Wide Web som är indexerad av Alta Vista.

OSS-konferensens ordförande Robert Steele med bakgrund inom underrättelsearbete vid amerikanska myndigheter menar att dessa behöver en miljard dollar per år för att öka tillgången till öppna källor och sprida kunskapen om deras användning. Dessutom borde det avsättas minst lika mycket för att skydda informationen och se till att dess upphovsmän får betalt.

Det informella samarbetet som källa

Användningen av öppna källor baseras på det fria flödet av information mellan samhällets olika aktörer, allt från underrättelseenheter till media och universitet. Ett sådant kontinuerligt informationsflöde är nödvändigt för att potentialen i att använda öppna källor ska kunna utnyttjas, ansåg Robert Steele som kallar företeelsen "The Information Continuum". Alla de barriärer som finns såväl mellan som inom organisationer måste rivas, ja även de mellan individer som genom ett revir- och makttänkande håller inne viktig information. Den styrande tanken borde snarare vara att ju mer information man delar med sig, desto starkare blir ens egen position, istället för att se informationsflödet som ett hot.

Behovet av att samarbeta har inte dykt upp av en slump, åtminstone inte ur myndigheternas perspektiv. Robert Steele konstaterade faktum att de främsta experterna inom många områden inte längre arbetar inom myndigheter eller militära organisationer utan i det privata näringslivet. Ett exempel är media, av många ansett som världens bästa primärkälla till information. Det handlar dock inte bara om den information som slutligen presenteras av media, utan än mer om den som aldrig kommer i tryck eller bild. En analytiker bör därför ha mycket goda kontakter i sitt nätverk med journalister och liknande aktörer.

De informella nätverken som samarbetar för att finna underrättelser kallar Robert Steele för "Virtual Intelligence Communities". I hans vision finns analytikern i mitten av flera lager omgivande cirklar av informationslämnare som sträcker sig allt längre ut från hans egen position och där cirklarna även indikerar en ökande öppenhet ju längre ut från mitten man kommer.

För att uppnå bästa resultat av sitt arbete bör man som exempelvis en analytiker inom en statlig underrättelseavdelning därför inte bara utnyttja sina egna källor utan sträva efter att kommunicera med de andra cirklarna i Robert Steeles modell Man bör t ex första prata med experter i den privata sektorn som kan tillhandahålla en generell bild av situationen. Därefter kan man ta kontakt med andra myndigheter som sitter på information som normalt inte är hemlig. Dock kan den vara mera svåråtkomlig än "ren" öppen information. Slutligen för att kunna göra en god analys bör man komplettera med sina egna hemliga källor. Då bör man ha fått en så komplett bild som möjligt utan att behöva spendera sina egna resurser där andra redan har gjort arbetet.

Man kan kritisera Robert Steeles vision om det virtuella underrättelsesamhället som fokuserad kring myndigheternas behov och möjligheter. Man kan fråga sig om det är lika intressant att ingå i detta virtuella samhälle om man ständigt befinner sig i den yttersta ringen och därmed kanske inte har någon möjlighet att "gå inåt" i modellen för att själv ta del av mera kvalificerad information. I ett väl fungerande samarbete krävs ett ömsesidigt utbyte av information och ingen ensidig låsning i roller som sändare och mottagare.

Säkerligen är det också så att privata sektorn är mera van att samarbeta och gå över gränser för att nå resultat än vad vissa myndigheter tidigare varit. Detta borde väl vara speciellt sant för klassiskt slutna myndigheter som t ex underrättelsetjänster och polisväsendet.

3. Metodik för öppna källor

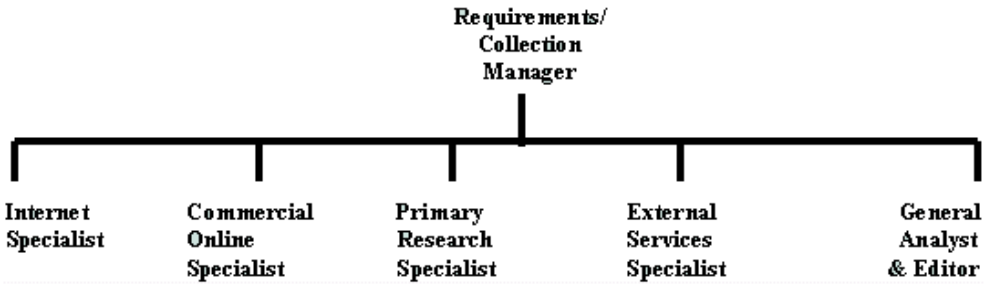
Begreppet öppna källor är ett mycket vitt begrepp som inte utesluter några källor. Bland andra konferensens ordförande Robert Steele talade ofta om bevakning av öppna källor som ”all-source intelligence”, dvs att alla källor ska vara tillgängliga för analys, oavsett format, hemliga eller öppna, interna eller externa, tryckta eller digitala källor från lokalradionyheter till satellitbilder. Erfarenheten visar, enligt Robert Steele, att 20% av all information finns on-line medan 80% är off-line.

För att man skall kunna förstå hur begreppet ”öppna källor” länkas in i det vidare begreppet ”alla källor”, kan man använda en pusselmetafor. Den yttre ramen, eller kanten, kring ett pussel ger en helhetsbild av området. Denna helhetsbild kommer från de öppna källorna och kan bidra med större eller mindre del av hela pusslet. När man slutligen lagt så många pusselbitar man kan med hjälp av sina öppna källor, så återstår det säkert ett par saknade bitar. Dessa bitar representerar ett informationsbehov som är mera kvalificerat och inte låter sig lösas med de enklare och billigare öppna källorna. Det är nu man skall inrikta sina specialresurser för att skaffa bitarna. Tillhör man en nationell underrättelsetjänst kanske man kan använda sig av satelliter, signalspaning eller spioner. Representerar man dock ett privat företag som inte har dessa resurser eller den lagliga möjligheten att utnyttja liknande tjänster, så kanske man får gå till andra källor. Exempel på sådana källor kan vara de som man uteslöt i första omgången p g a kostnader eller arbetsinsatser, inte för att de var hemliga utan för att det fanns bättre alternativ som kunde ge helhetsbilden.

Ett av konferensens mer intressanta teman behandlade därför metoder för omvärldsbevakning, dvs hur kan bevakningsarbete med öppna och alla källor organiseras bäst.

Den lilla enheten

Robert Steele gav förslag på en bra organisation av en mindre funktion för att hantera öppna källor inom både myndigheter och företag. En liten sektion med fem till sex personer kunde dela på arbetsuppgifter för att tillsammans lösa de flesta uppgifterna och ge en god täckning av bevakningsområdet.



Figur 1 Ett exempel på hur man kan organisera en mindre funktion för att hantera Open Source Intelligence

En sådan uppdelning som i figuren ovan gör att alla medarbetare kan specialisera sig inom en viss del av verksamheten. De ansvarsområden som är tänkta att besättas är:

- **Requirements/Collection manager** – leder verksamheten och analyserar den ställda uppgiften
- **Internet Specialist** – ansvarar för insamling av information via Internet
- **Commercial Online Specialist** – ansvarar för insamling av information via alla olika kommersiella databaser
- **Primary Reserach Specialist** – ansvarig och kunnig inom intervjuteknik och direkta undersökningar
- **External Services Specialist** – håller reda på externa kontakter och vilka experter som finns inom olika områden
- **General Analyst & Editor** – analyserar insamlad information enligt det ställda uppdraget samt sammanställer informationen.

Bygger man upp en funktion med denna bredd bör den enligt Robert Steele kunna utför de flesta uppgifter som vanligen åläggs en enhet för omvärldsbevakning, exempelvis strategiska och tekniska framtidsstudier, undersökningar och nyhetsanalyser. Uppgifterna kan alltså variera mellan relativt enkla rutinuppgifter som att producera en morgonrapport över nyheter till komplexa framtidsscenarier.

För att enheten skall få tillgång till så många experter som möjligt, utan att behöva avlöna ***(anställa)*** dem själva används den ovan nämnda specialisten kring externa tjänster (Externa Services). En tänkbar uppgift som en sådan person kan ha är att koordinera och administrera ett nätverk av externa konsulter. Detta förfarande kan illustreras som en pyramid där den mycket breda basen representeras av de externa experterna. I toppen sitter själva bevakningsenheten och samlar in information som de andra delarna av pyramiden rapporterar in (se också avsnitt om Oxford Analytica nedan).

En mycket viktig kärnkompetens hos en bevakningsenhet är därför att veta "vem som vet" *(knowing who knows*[1]*)* samt "vem som vet *mer*".

Nutrasweets 50 miljoner

Ett av de mest kända framgångsrika satsningarna på Business Intelligence skedde hos företaget Nutrasweet. Företaget sägs idag spara 50 miljoner dollar årligen tack vare sin BI-enhet. På OSS'97 gav en av grundarna till enheten, Max Downham, sin syn på en BI-enhets organisation.

Anledningen till att Nutrasweet överhuvudtaget började fundera i termer om omvärldsbevakning var att de började frukta den dag då deras patent på sötningsmedlet skulle gå ut. För att hjälpa till med att dra upp riktlinjerna innan patentskyddet försvann kallades den kände managementkonsulten Peter Drucker in. Han föreslog direkt att Nutrasweet måste skaffa sig en bättre kunskap om omvärlden för att möta de nya, potentiella, hoten. Den konsult som skulle bidra med kunskapen om att skapa en väl fungerande enhet för omvärldsbevakning var Jan P. Herring, en före detta CIA-anställd.

Herring tog med sina erfarenheter från CIA:s underrättelsemetoder till Nutrasweet som började att bygga upp ett liknande system. Metoden som sedan dess blivit tongivande bygger på följande steg:

- Fokusera på nyckelområden
- Samla information
- Analysera

[1] Detta uttryck sägs ursprungligen vara myntat av Dr Stevan Dedijer, professor vid Lunds Universitet och av många ansedd som den skapade begreppet Business Intelligence.

- Sprid informationen

Det är intressant att notera att den enhet som sattes upp kunde klara cirka tre till fem samtidiga uppdrag. Inte ens ett stort företags BI-enhet bör alltså ha fler bevakningsuppgifter vid ett givet ögonblick. Max Downham poängterade också vikten av att prioritera bland uppgifterna. En bra tumregel är att prioritera de frågor som ”höll VD vaken om natten”.

Arbetsmetoden som tillämpades av Nutrasweet är cyklisk i det att fokusering och strategier måste förändras när ny information dyker upp.

Valet av personal till en BI-enhet är viktigt menade Downham. De personliga egenskaperna påverkar arbetets resultat i stor utsträckning. En Business Intelligence-enhet måste försöka vara så fri som möjligt från förutfattade meningar. Max Downham sammanfattade några viktiga egenskaper som en Business Intelligence-person bör ha:

- Vara öppen för nya idéer
- Villig att ta risker
- Samarbeta väl med ledningen
- Kunna skapa förtroende för sig själv och för funktionen

Vad var då avgörande för Nutrasweets framgång inom området? Jo:

- Enheten måste vara flexibel
- Tillgång till rätt arbetskraft
- Stöd hos den översta ledningen
- Vara tålmodig

En industriell process – Oxford Analytica

Oxford Analytica är ett analysföretag som har sitt säte i universitetsstaden Oxford, England. Det skapades ursprungligen av en amerikan som insåg att den stora kompetens som fanns bland de lärda i staden borde kunna utnyttjas till privat analysverksamhet. Ursprungligen ville man skapa en version av den dagliga briefing som den amerikanske presidenten erhåller, fast med inriktning mot vad den privata sektorn har för informationsbehov.

Idag ligger Oxford Analyticas styrka inom områden som politik, nationalekonomi, ”public policy” och ”sectoral issues”. Företagets ursprungliga briefingtjänst har idag utökats med flera andra tjänster, t ex ”country risk/sectoral analysis”, ”monitoring services” och ” multi-client research projects”. Deras kunder finns sig över hela världen och inom de flesta olika branscher samt är av olika storlek, från stora företag till hela stater. Det är dock inga mindre företag som köper tjänsterna, då prissättningen är tämligen hög.

Oxford Analyticas verksamhet kan låta ganska unik, men av deras arbetssätt finns mycket att lära även för den som arbetar i mindre skala med Business Intelligence inom ett företag. Speciellt är det Oxford Analyticas medvetna satsning på ett samverkande internt och externt nätverk av experter som är intressant att studera närmare.

Arbetsgången baserar sig på en kärngrupp som arbetar heltid (dygnet runt) i Oxford. Denna grupp samlar in all information som sedan läggs i mappar och struktureras. Varje morgon hålls ett morgonmöte där de s k region-heads samlas som var och en ansvarar över analyser för en del av världen. De läser sedan innehållet i mapparna och bestämmer vad som skall fokuseras närmare för vidare undersökning och informationsinhämtning och bestämmer dessutom vad som skall ingå i den dagliga briefingen, vilken senare under dagen görs tillgänglig för alla prenumeranter. Dessa morgonmöten upplevs inom organisationen som bland deras viktigaste verksamhet, där samlas nämligen både kreativitet och beslutsfattande i samma plenum.

De ämnen som valts ut att fokuseras mera går tillbaka till kärngruppen och man börjar bygga upp en ”task force” utifrån de ca 1000 tillgänglig experter som finns att nå runt om i världen. De

externa experternas arbete koordineras via respektive region-head från Oxford samt att kärntruppen fungerar som en redaktion för producerat material.

Ingen organisation kan klara av dagens enorma informationsflöde med egna resurser. Oxford Analytica representerar ett nytt tänkande med en liten kärna och ett stort yttre nätverk. Nätverket är i ständig förändring och skiftar allt efter behov. För att komma med i kompetensnätverket måste man antingen bli rekommenderad via någon tidigare medlem i nätverket eller utvald p g a sina tydliga akademiska meriter. Oxford Analytica accepterar därför mycket sällan några externa "experter" som på eget initiativ söker sig till dem.

För att kunna agera i en global miljö har vissa i den inre kärnan en språkkompetens som medger direkt analys av ursprungsmaterial på t ex arabiska. Finns det inte någon inom organisationen som har kunskap i det aktuella språket, hyrs externa översättare in.

Oxford Analytica försöker också bevaka resultaten av de förutsägelser och analyser man gör och dessutom motivera varför utvecklingen följer det ena eller andra spåret. Skulle det visa sig att de gör flera felaktiga förutsägelser eller bedömningar inom ett visst område så genomförs en analys av vad som måste förändras för att produkten, analysen, skall bli bättre.

Oxford Analytica har alltså en beprövat effektiv metod för underrättelsearbete som kan tillämpas i andra typer av organisationer där det behövs ett storskaligt och effektivt arbete. Tillvägagångssättet att sätta ihop särskilda grupper kring ett ämnesfokus under en begränsad tid har föreslagits av andra i branschen, t ex Benjamin Gilad som rekommenderar sk SWAT-teams, vilket är löst sammansatta grupper som endast skall lösa en "So what?" fråga.

Efterlyses: Beställarkompetens

Omvärldsanalytikern måste idag sätta kundens behov och frågeställningar i centrum för sitt analytiska arbete. Det duger inte att svara på de frågor man hoppats få, utan det gäller att verkligen besvara den liggande frågeställningen.

Robert Steele berättade om hur en befälhavare under Gulfkriget hade uttryckt följande:

> *I have more use for information that is 85% correct and on time, compared to a 100% correct, top secret codeword document, that is too much and too late, and requires a safe and three security officers just to carry around the battlefield.*

Citatet ovan är ett bra uttryck för hur viktigt det är att de som producerar information till beslutsfattare sätter sig in i deras situation. Är det t ex VD som skall ha informationen så är det kanske bättre att kondensera ner texten till endast en sida som verkligen blir läst, än att skapa ett stort gediget dokument som endast blir liggande – oläst. Däremot så kanske det lämpligare att förse företagsstrategen med gedigna dokument, vilka då bättre motsvarar dennes krav på faktadjup och analyser.

Nyckeln till att få en situation där rätt underrättelser finns framme vid rätt ögonblick är att det finns en mycket god förståelse hos analytikerna om vilket underrättelsebehovet är, men det är lika viktigt att beställaren av underrättelser, kunden, har insikt i vilka frågor han kan ställa och vilka möjligheter analytikerna har att besvara dem. *Beställarkompetens* i det här sammanhanget handlar alltså om att ha insikt i underrättelsearbetets arbetsprocess, något som även betonades av flera talare under konferensen

Analytikerna måste idag stödja beslutsfattarens behov av beslutstödsinformation i realtid. Man kan inte exakt förutsäga informationsbehovet i förväg, men ändå måste färska underrättelser alltid finnas, eller kunna tas fram på mycket kort tid, vid behov. Det duger dock inte att arbeta efter en "just-in-case" princip, utan det är "just-in-time" som gäller. Analytikerna är allt mer stressade och upptagna människor och har inte tid att ta fram rapporter som inte behövs. De måste istället koncentrera sig på att besvara den uppsatta frågeställningen.

Något som flera talare också belyste under konferensen var frågan om vem som är kunden, eller slutanvändaren, för de olika slutprodukterna från bevakningsarbetet.

4. Hot och skydd

Uttrycket Information Warefare vilket ungefär kan översättas till ”informationskrigföring” började användas inom amerikanska försvaret där man har tillämpat Information Warfare i bland annat Gulfkriget, då man hade mycket stor kontroll över såväl massmedia och opinion som Iraks informationsförsörjning.

Men begreppet har plockats upp även av privata företag och breddats till att innefatta många olika aspekter. Man kan t ex ha en utgångspunkt i vem som är mål för angreppet som kan ske på:

- *Personlig nivå.* Information Warfare med inriktning mot en enskild individ.
- *Företagsnivå.* Här utnyttjar man information om ett enskilt företag för kommersiella eller ekonomiska intressen.
- *Global nivå.* På denna nivå är det nationella intressen som är det primära målet för attacken.

En annan utgångspunkt är angriparens motiv:

- *Hacker.* Är en relativt harmlös angripare vars främsta syfte är att bryta sig in i datasystem för att se om det går.
- *Cracker.* Har ett motiv till angreppet. Det är då framförallt personliga intressen som spelar in, såsom att skapa konkurrensfördelar, ekonomiska fördelar, skada en konkurrent eller annan motståndare, mm.
- *Maktfullkomlig.* Är den angripare som vill projicera makt. Till denna kategori hör terrorister, underrättelsetjänster, kriminella organisationer, anarkister, psykopater, mm.

En tredje utgångspunkt är den egna organisationen. Detta gäller främst försvaret, där följande exempel är hämtat från amerikanska försvarsdepartementet:

- *Offensiva aspekter.* Vad kan man sätta emot när man blir utsatt för Information Warfare? Vad kan vi själva göra för att bedriva Information Warfare?
- *Defensiva aspekter.* Dessa tar hänsyn till att det är viktigt att skydda den egna informationen. Problemet är att mycket av den information man är beroende av inte kontrolleras av den egna organisationen.
- *Infrastrukturen.* Hur skall vi skydda våra egna nät, och hur skall vi upprätthålla bästa möjliga kommunikation med våra egna system?

Parallellt med alla dessa utgångspunkter finns det även ett antal definitioner som kommer från både näringsliv och försvar. Problemet med dessa är att de från näringslivet tenderar att bli väldigt breda och intetsägande, medan de från försvaret missar ekonomiska, politiska och företagsmässiga aspekter. Man föreslog då följande definition:

> *Information Warfare är de åtgärder man vidtar för att skydda, utnyttja, förvanska, förneka eller förstöra information eller informationskällor med avsikt att få en signifikant fördel, nå ett mål eller vinna en seger över en motståndare.*

I och med denna definition får man med både de aspekter som är viktiga för försvaret samt de som näringslivet fokuserar på. Man skall dock vara medveten om att det som ytterst uppfattas som Information Warfare beror på den verksamhet man bedriver.

Information Warefare har blivit aktuellt därför att det idag relativt enkelt att bedriva. Det är framförallt sex faktorer som ligger till grund för detta:

- **Teknikutvecklingen** gör det billigt och lättillgängligt. Den ökade elektroniska kommunikationen påverkar det sätt vi bedriver vår verksamhet.
- Den västerländska **samhällsstrukturen** inbjuder till att utmana personer och organisationer till att bedriva Information Warfare. Eftersom vi lever i ett informationsintensivt samhälle kommer även konflikter att bedrivas med information.
- De länder som räknas till tredje världen har **allt att vinna och inget att förlora**. De ser hur den rika delen av jorden blir rikare och vill då själva ha en bit av kakan. Den billiga och förhållandevis enkla tekniken gör det möjligt för organisationer och personer i tredje världen att bedriva Information Warfare. Dessutom är chansen för rättsliga påföljder i stort sett obefintliga.
- **Girighet** är ytterligare en faktor som spelar in. Dels är det ekonomisk girighet, men även hungern efter makt och kontroll spelar in.
- Information Warfare kan skötas på **distans**. Detta hör ihop med den snabba teknikutvecklingen men med ett fokus på att den som utövar Information Warfare inte behöver vara fysiskt närvarande vid informationskällan. Det är dock vanligt att ett dataintrång föregås av ett inbrott i en kontorslokal för att stjäla ett lösenord eller lägga in en bakdörr i ett nätverk.
- Den främsta orsaken är dock att **Information Warfare finns därför att möjligheten till det finns.** All ny teknik kommer förr eller senare att utnyttjas vid konflikter och i destruktivt syfte.

Man får inte glömma bort att det som är viktigt ur ett personligt, organisatoriskt eller samhälleligt perspektiv också är sårbart. Ju mer vi litar till och bygger upp vår tillvaro runt något, desto större blir chansen att någon utnyttjar detta för att få en signifikant fördel, nå ett mål eller vinna en seger.

Intrång och spionage…

Med kunskap om vad som är möjligt att åstadkomma med modern teknik för informationsinhämtning och analys sprider sig oron längs två fronter, dels den egna exponeringen mot konkurrenter, dels att konkurrenterna ska få ökad medvetenhet om riskerna och därigenom skydda sig bättre.

Ett område som säkert kommer att behöva ses över vad gäller informationssäkerhet är tekniska mässor och konferenser. Många deltagare drog på smilbanden då någon nämnde att det ju var allmänt känt att tekniker älskade att prata om sitt jobb – bara någon lyssnade. Sådan pratsamhet innebär en risk att viktig information läcker ut och att personen som pratar bredvid mun inte ens är medveten om att han/hon blir pumpad på hemliga uppgifter. Som lösning på detta problem såg flera att det krävdes någon form av säkerhetsklarering av föredrag, presentationer och broschyrer innan deltagare åker iväg på dessa externa arrangemang.

Det är idag mycket enkelt att hitta samband mellan olika företeelser som man egentligen inte tänker på. Ett exempel på detta:

> *VDn för elektronikföretaget SkarmAB antyder i en artikel att de har en ny produkt på gång som kommer att påverka deras halvårsresultat mycket positivt. Samtidigt har företagets två bästa tekniker anmält sig till en konferens som handlar om de nya platta färgskärmarna som är en het forskningsfråga nu. Medan de är på konferensen står deras närmaste kollegors bilar på företagets parkering nästan dygnet runt. Allt detta ser SkarmABs konkurrent Skärmören, som dessutom har bra kännedom om färgskärmsmarknaden och har följt sina konkurrenter ett tag.*

Det vi beskrivit ovan är ett hypotetiskt exempel, men med tanke på att all den information Skärmren använt sig av finns tillgänglig genom deltagarlistor, tidningsartiklar, pressreleaser, trycksaker från SkarmAB, mm är det inte särskilt svårt att lägga ett informationspussel. Om man dessutom tar hjälp av de verktyg som finns idag för omvärldsbevakning, till exempel ett verktyg som kartlägger relationer mellan olika företeelser, blir det ännu enklare.

Vad kan då den kartläggning som Skärmören gjort användas till? Först och främst så är det intressant för dem att se vad deras konkurrenter håller på med, så att de inte hamnar efter. Sedan kan en kartläggning av en organisation eller person användas i syfte att smutskasta eller sprida falsk information i annans namn. Det är idag väldigt enkelt för en person att skicka brev och epost i någon annans namn. Har man dessutom lite kunskap om vad som är aktuellt för ett företag kan falska meddelanden i både brev, epost och diskussionsforum bli väldigt trovärdiga.

Hur skyddar man sig mot detta? Precis som med så mycket annat är **medvetenhet om problemet** en bra början. När organisationer blir mer medvetna om hur enkelt det egentligen är att lägga ett pussel av den information som finns tillgänglig, kommer de också att arbeta mer fokuserat med att inte sprida information omkring sig. Detta kommer att innebära att såväl ledning som övriga anställda måste bli försiktigare med vad de säger och till vem, var de registrerar sig i olika sammanhang, mm. Tekniker som skall tala på konferenser och seminarier kommer att få manus som de måste hålla sig till. De tekniker som åker som åhörare kommer kanske att anmäla sig med alias.

Vems ansvar är det att arbeta med informationssäkerheten i en organisation? En bra princip som man ska gå efter är att de som arbetar med informationsinhämtning, alltså omvärldsbevakning, också är de som vet hur andra (till exempel konkurrenter och fiender) hittar information om den egna organisationen. Omvärldsbevakaren kan inhämtningsprocessen vilket gör att de också vet hur man kan förebygga oönskad informationsspridning.

Detta ger då att vi redan idag bör tänka på all den information vi lämnar ut, både medvetet och omedvetet registreras och kan därigenom användas av de som är intresserade av vår verksamhet.

När det gäller intrång via datanäten är det ett problem som många organisationer känner av mer och mer, framförallt i samband med Internet där deras egna hemsidor blir hackade. När det gäller just intrång finns det en generell fråga som är mycket svår att besvara (om det ens är möjligt att få svar på den), och det är om den eller de personer som försöker tränga in i systemen är spioner eller hackare. Skillnaden mellan dessa två grupper är markant; en hackare har ofta intresse av att synas, medan spionen vill vara osynlig. Detta gör att en hackares intrång ganska snabbt blir upptäckt genom att filer har ändrats (exempelvis företagets hemsida), att diskutrymme har används eller att lösenord har ändrats. Spionens ingrepp kan däremot vara dolt länge, och i värsta fall upptäcks skadorna kanske inte alls.

Hur kommer man då åt problemet med oönskat intrång? Tidigare räckte det med att låsa in datorn i ett rum med tjocka väggar, men i samband med att man började bygga och använda nätverk fungerade inte denna lösning längre. I stället skapade man brandväggar, inloggningar och krypteringar. Inget av detta kan dock hålla eventuella informationstjuvar ute. Innebär detta då att inga av de system vi använder oss av kan anses vara säkra? För att svara på den frågan måste vi först fundera på vad vi menar med ”säkra system”. Om vi menar att ett system skall vara ointagligt så har vi inga säkra system som är kopplade till Internet. Om vi å andra sidan menar att ett säkert system är ett system som står emot ett intrångsförsök tillräckligt länge för att

vi skall kunna upptäcka samt reagera på försöket, ja då har vi idag många system som är tillräckligt säkra.

… och etik för omvärldsbevakning

En viktig fråga för den som sysslar med omvärldsbevakning är när inhämtning av en viss informationsbit innebär ett brott mot lag och/eller moral. De flesta håller säkert med om att direkt inbrott inte ska förekomma, men om en konkurrerande säljares dator "hittas" på en mässa, kan man då titta på dess innehåll? Eller är det korrekt att anordna falska anställningsintervjuer för att på den vägen få information om en konkurrent?

Föreningen SCIP, Society of Competitive Intelligence Professionals, höll under OSS-konferensen ett seminarium på temat etik för omvärldsbevakning med anledning av en relativt ny lag i USA under namnet Economic Espionage Act (EEA) och hur det påverkar arbetet med Business Intelligence. SCIP är en global sammanslutning av personer som arbetar inom eller är intresserade av området Competitive Intelligence. Dessa personer, som är cirka 6000 spridda över hela världen, kommer främst från den privata sektorn.

Den jurist som höll fördraget om EEA jämförde lagen mot de regler för uppträdande som SCIP har ställt upp för sina medlemmar – de s k Code-of-Ethics. Resultatet från denna jämförelse och den efterföljande diskussionen var att riktlinjerna från SCIP väl ligger inom lagens ramar och att EEA inte innebär något hot mot att verka inom Business Intelligence i USA. Vissa sätt att bedriva undersökningar kan dock uppfattas som omoraliska , t ex att utge sig för att vara någon annan (misrepresentation), men är inte olagligt i sträng betydelse. Detta sammanfattades på typiskt amerikanskt med "It's not illegal to lie – just immoral"

SCIP:s Code-of-Ethics

- *To continually strive to increase respect and recognition for the profession.*
- *To pursue one's duties with zeal and diligence while maintaining the highest degree of professionalism and avoiding all unethical practices.*
- *To faithfully adhere to and abide by one's company's policies, objectives and guidelines.*
- *To comply with all applicable laws.*
- *To accurately disclose all relevant information, including one's identity and organization, prior to all interviews.*
- *To fully respect all requests for confidentiality of information.*
- *To promote and encourage full compliance with these ethical standards within one's company, with third party contractors, and within the entire profession.*

5. Teknik för öppna källor

Den utställning som pågick parallellt med konferensen bestod av ca 35 utställare som representerade informationsleverantörer (Knight-Ridder, Lexis-Nexis, etc), intresseorganisationer (främst amerikanska försvars- och myndighetsorganisationer), leverantörer av kartor och satellitbilder, samt leverantörer av verktyg för informationshantering / omvärldsbevakning. När det gäller den sista gruppen utställare, verktygsleverantörer, kan dessa delas in i tre kategorier; 1) digitala bibliotek, 2) nyhetsbevakning och 3) sambandsanalys.

Med **digitala bibliotek** menas de verktyg som katalogiserar och indexerar information. De verktyg som passar in under denna rubrik är:

- Excalibur
- KnowledgeLink
- Memex
- DR-LINK
- WebSumm
- DCARS

Nyhetsbevakning är verktyg som klarar av att automatiskt hantera flöden av information, till exempel nyhetsutsändningar från radio och TV, notiser från TT och REUTERS, mm. Det var egentligen bara ett verktyg som hade tyngdpunkten på nyhetsbevakning.

- Broadcast News Navigator

Sambandsanalys är verktyg som analyserar relationer mellan personer, organisationer, händelser, produkter, mm. De verktyg som passar in i denna kategori är:

- Analyst Notebook
- CHESS
- Wisdom Builder
- NetOwl

Denna lista är inte absolut, utan de 11 olika verktygen har även funktionalitet som spänner över alla tre kategorier. Flera av verktygen kan även hantera till exempel flöden av information såsom notiser från TT och REUTERS, men deras fokus ligger inom det område de står uppräknade under.

Lösta och olösta problem

När det gäller omvärldsbevakning och knowledge management är det vissa saker som inte längre är ett problem. Ett exempel på detta är databaser. Det finns i dag ett stort antal olika leverantörer av databaser för såväl stordator, UNIX och PC. Lagringskapacitet är även det ett problem som numera är löst. Hårddiskar på 10 gigabyte kostar idag 10 – 15 tusen kronor. Nätverk, både globala och lokala, är även det ett problem som är löst.

Däremot är ett av de kvarvarande problemen för de flesta verktygstillverkare fortfarande att hantera sökningar på ett för användaren enkelt och överskådligt sätt. Problemet är egentligen uppdelat på tre delproblem:

- För det första är sökverktygen alldeles för trubbiga. De klarar inte av mer komplexa frågor, till exempel i naturligt språk.
- För det andra är det mycket svårt att se helheten i sökresultaten. Den träfflista som presenteras är ofta alldeles för lång, och relevansen i de enskilda träffarna är ofta låg.
- För det tredje finns det idag alldeles för dåligt stöd för att analysera den information man fått fram i sina sökningar. Det är dock viktigt att komma ihåg att analysen är en mänsklig process, men med tanke på den komplexitet som till exempel vissa sambandsanalyser kan föra med sig är det viktigt att ha ett bra analysstöd.

Det finns ytterligare ett par problem som är relaterat till sökningar, men då enbart sökningar på Internet. Det finns idag ingen sökmotor som klarar av att indexera dynamiska webbsidor, det vill säga sidor som genereras då användaren begär dem. De dynamiska sidorna är ofta sidor som visar på innehåll i databaser, till exempel sökträffar vid sökningar i artikeldatabaser. Så länge innehållet i dessa databaser inte kan hanteras av de sökmotorer som finns, kommer inte kunskap om databasernas innehåll att spridas till alla som behöver informationen.

Det händer alldeles för ofta att den metainformation[2] som finns på webbsidorna inte stämmer överens med innehållet på sidan. Det för med sig att de sökträffar som presenteras ibland kan innehålla information som inte har någonting att göra med det man letar efter.

Internet växer fort. Detta är bra, men det för med sig komplikationer. Det finns framförallt ett problem med den snabba tillväxttakten som påverkar sökningar på Internet. Ingen av de största registren och sökmotorerna på Internet klarar av att indexera alla nya sidor i samma takt som de dyker upp, förändras eller försvinner. Vi använder oss alltså alltid av verktyg som inte har överblick över allt som finns på webben, vilket gör att man får olika träffar med samma sökbegrepp när man använder olika verktyg.

Många av de produktleverantörer som var representerade på utställningen börjar dock titta vidare på några av dessa problem (se nedan) och man kan redan nu börja se en positiv utveckling inom området.

Trender inom verktygsområdet

Naturligt språk

För att komma åt problemet med komplexiteten i sökningarna har flera leverantörer börjat titta på hur de kan använda naturligt språk för att söka i stora textmassor.

DR-Link och NetOwl är exempel på två verktyg som använder sig av denna teknik. Skillnaden mellan verktyg som baserar sina sökningar på naturligt språk (natural language processing, NLP) och vanliga verktyg som använder indexregister, är att NLP-verktyg utgår ifrån lingvistisk och semantisk analys av texten. Det innebär att verktyget klarar av att söka efter saker i ett sammanhang och därigenom hålla isär filen som snickaren använder med filen som bilen kör i.

Det är dock viktigt att veta att vi än så länge bara är i början av användningen av naturligt språk vid sökningar i textdatabaser. De produkter vi sett är i version 1.0 eller i betaversion. Problemet med att använda sig av naturligt språk är att det är både språkberoende och domänberoende. Meningar är byggda på olika sätt på olika språk (det är till och med skillnad på brittisk och

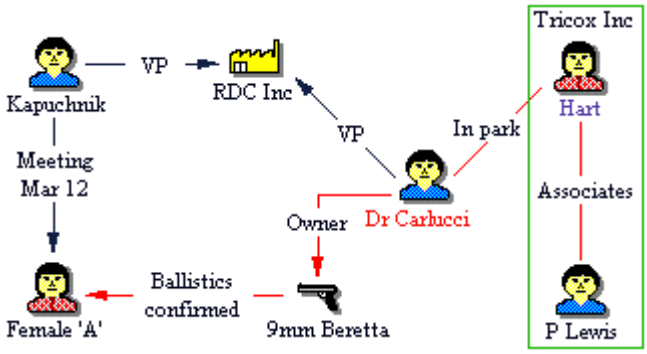
[2] Dold information om innehållet i ett HTML-dokument som flertalet sökmotorer använder sig av för att identifiera en webb-sida.

amerikansk engelska), och det är även skillnad på meningsbyggnaden mellan olika ämnesområden.

Analysstöd

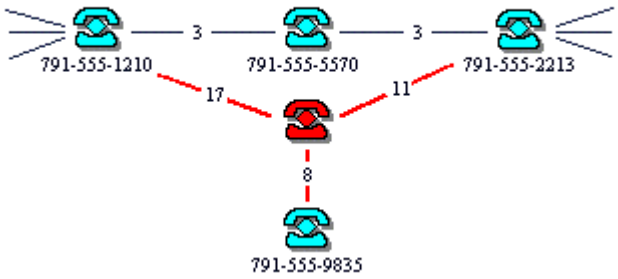
När det gäller analysstöd var det främst i2:s produkt Analyst Notebook som stack ut från mängden. Verktyget är till för att lyfta fram de samband som kan dölja sig i stora mängder information. Analyst Notebook är framtaget för polis, tull och andra myndigheter för att utreda kriminell verksamhet.

I bilden nedan har man gjort en länkanalys där man ser vilka relationer ”Dr Carlucci” har till personer, företag och mordvapnet. Länkanalysen kan visa relationer mellan olika personer, fordon, organisationer och andra nyckelobjekt samt flöden av varor eller pengar.



Figur 2. Länkanalys med Analyst Notebook.

Ett annat sätt att åskådliggöra stora mängder information som finns lagrade i databaser är genom nätverksanalys. Denna typ av visualisering är särskilt användbar när man vill titta på telefon- och internettrafik samt pengatransaktioner. I bilden nedan visas 5 telefonabonnemang och den trafik som dessa har haft med varandra.



Figur 3 Analyst Notebook.

Nyhetsbevakning

Det enda renodlade verktyget för nyhetsbevakning var MITREs Broadcast News Navigator (BNN). MITRE är en amerikansk forskningsorganisation vars uppgift är att hjälpa offentlig sektor och militär med att effektivt utnyttja IT.

BNN är en webbaserat sökverktyg för nyhetsutsändningar. Verktyget är anpassat för de inslag som CNN Online lägger ut på sin hemsida. BNN analyserar nyhetsinslagen enligt en lingvistisk modell, och sökresultatet presenteras sedan med information om de inslag som bäst stämde överens med sökningen (se bild nedan). Styrkan med detta verktyg är att det automatiskt analyserar och indexerar alla inslag som systemet tar emot. Detta gör att användaren kan få en

automatisk sammanfattning av de mest intressanta inslagen från det senaste dygnets utsändningar direkt till sin dator. Det fattas dock än så länge sammanfattningar av inslagen då MITRE anser att det ännu inte finns några verktyg som på ett bra sätt tar fram sammanfattningar av textmassor.

Figur 4. BNN.

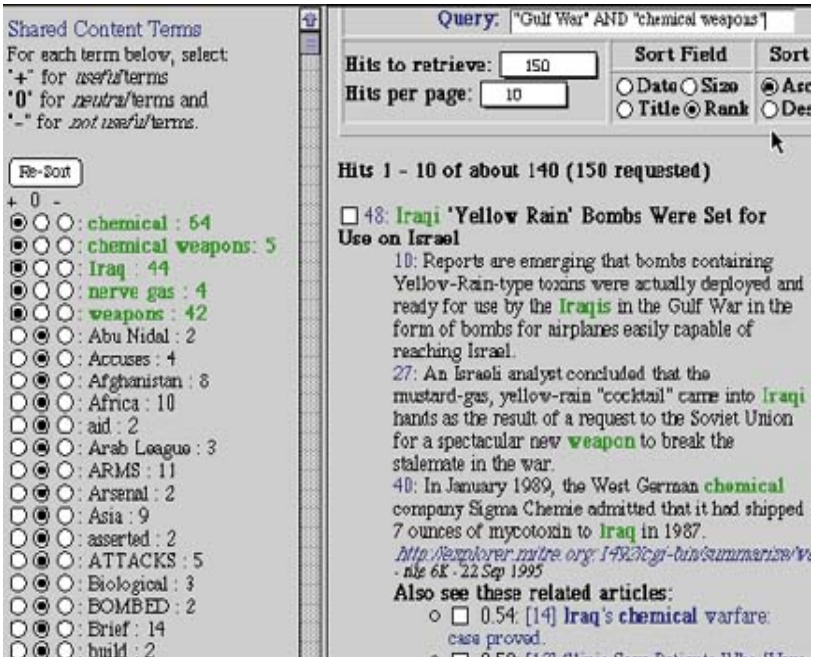
I bilden ovan har man gjort en sökning på Israels premiärminister Benjamin Netanyahu, och det är sammanfattningarna av de två bästa träffarna som visas i bild.

Då MITRE inte är en produktutvecklande organisation arbetar de mestadels med prototyper. BNN finns inte som produkt (ännu) men konceptet är väldigt intressant då det idag går att tolka och lagra ljud- och filmsekvenser för att senare göra sökningar bland dessa. Detta skulle innebära att omvärldsbevakaren varje morgon får de fem viktigaste nyhetsinslagen från det senaste dygnets utsändningar presenterade för sig. Oberoende av program.

Överskådlighet i sökresultat

Det andra verktyget som MITRE presenterade på utställningen var Web Summ. vilket är en applikation som läggs som ett lager ovanpå AltaVista. Det problemet som idag finns med AltaVista, Hotbot och de andra sökmotorerna på Internet är att de träffar man får oftast inte rankas i den ordning man själv skulle vilja ha. WebSumm analyserar sökträffarna även ur ett innehållsmässigt perspektiv, då verktyget bland annat tar hänsyn till avstånd och relationer mellan ord. Det går också att ange att man vill hitta nya dokument som liknar ett redan hittat

dokument.



Figur 5. WebSum från MITRE ger möjlighet att efterbearbeta sökresultat från Alta Vista.

I bilden ovan har man gjort en sökning i AltaVista på ”Chemical weapons OCH Gulf War” och fick 140 träffar. När man sedan väljer att använda sig av WebSumm genereras ett index med de ord som förekommer oftast i de 140 dokumenten. Indexet visas till vänster i bilden. Genom att välja några av dessa ord sorteras de 140 träffarna om och presenteras i en ordning som bättre stämmer överens med vad användaren egentligen var ute efter. I exemplet ovan har den träff som AltaVista presenterade på plats 48 flyttats fram till plats 1 i WebSumm och visas till höger i bilden. För att man lättare skall få en överblick över de träffar som presenteras får man dessutom en sammanfattning av dokumentet. Sammanfattningen består av de meningar som de angivna sökorden ingår i, där sökorden är markerade. På så sätt får man en snabb inblick i vad de enskilda dokumenten handlar om, utan att för den skull behöva öppna dem.

Det kommer att ske en kraftsamling på utvecklingen av sökverktyg, både vad gäller möjligheterna till att definiera sökningar som ger svar på det man egentligen frågar efter, och dessutom även vad gäller presentationen av sökresultaten. Vi kommer att få se grafiska presentationer av sökträffarna i mycket större utsträckning i framtiden än vad man använder det idag.

Varför har då MITRE tagit fram dessa två prototyper? Vi människor har en begränsad kapacitet när det gäller att bearbeta information. Vi behöver därför hjälp av olika verktyg för att inte drunkna i den enorma mängd information som vi kommer över. Dessa verktyg kan då vara de hjälpmedel vi skulle kunna använda oss av.

Nya strategier

Förutom MITREs WebSumm använder sig även företagen Kalspan och KnowledgeLink av ett koncept som vi kommer att se mer av framöver. KnowledgeLink är ett verktyg för att publicera information på ett lättillgängligt sätt, och har då valt att använda sig av metaforen med en tidnings framsida. Verktyget finns än så länge endast som betaversion och företaget väntas komma med en första version i december 1997. Kalspans DCARS är ett analys- och presentationsgränssnitt som lagts över Excalibur Retrievalwares databas.

Det gemensamma drag som dessa tre verktyg har, är att de använder sig av State-of-the-Art vad gäller befintlig teknologi och bygger sedan på med delar de själva anser fattas. KnowledgeLink anser att det redan finns bra verktyg för datainsamling och lagring, och har då valt att använda

sig av några av de verktyg som finns. I stället för att bygga ett verktyg från grunden har de specialiserat sig på att bygga ett presentationsgränsnitt för den information man har samlat in och vill titta på. Kalspan anser att analysen och presentationen brister, men de har valt att basera sitt verktyg på Excaliburs verktyg (vilket i sig är en förhållandevis dyr och komplex programvara).

Det finns ytterligare ett koncept som är intressant i fallet med KnowledgeLink. De säljer sin programvara färdig och paketerad i en maskin. En färdiginstallerad file-server (Windows NT) med programvara och 50 licenser kostar ca $15.000 (120.000 kr). Att sälja färdiginstallerad programvara i en dator är inget nytt i sig. Detta har stor-, mini- och UNIXdatorleverantörer gjort länge. Det är dock en ganska ny företeelse när det gäller PC, och det är helt nytt när man talar om den här typen av applikationer.

För den dagliga omvärldsbevakningen kommer informationen att presenteras mer och mer på användarnas personliga webbsidor, där innehållet specificeras enligt fördefinierade användarprofiler. Detta innebär att istället för att tala om push- eller pull-teknik kommer man att kombinera dessa två sätt att sprida information på och således få en push- och pull-teknik. Sammanfattningar kommer då att skickas till användaren i form av e-post meddelanden eller presenteras som en egen webbsida (push). När man sedan hittar något man vill titta närmare på laddar man ner mer information om detta (pull). Det kommer således att mer och mer bli en fråga om rätt mängd information i rätt tid.

6. Webadresser

Organisation	URL
AltaVista	www.altavista.digital.com
Excalibur Retrievalware	www.excalibur.com
i2 (Analyst Notebook)	www.i2ltd.demon.co.uk
Infowar.Com	www.infowar.com
Calspan (DCARS)	www.calspan.com
KnowledgeLink	www.k-link.com
Manning & Napier (DR-LINK, CHESS)	www.mnis.net
Memex	www.memex.co.uk
MITRE (WebSumm, BNN)	www.mitre.org
Open Source Solutions	www.oss.net
SSC Satellitbild Spacepix	www.spacepix.com
SRA International (NetOwl)	www.sra.com, www.isoquest.com
WisdomBuilder	www.wisdombuilder.com