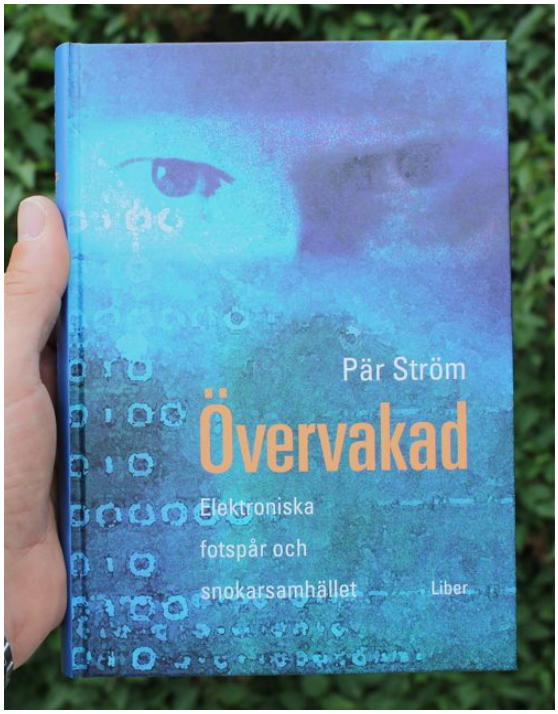
Amerikansk avlyssning från Echelon till Prism

Två kapitel ur boken ”Övervakad”

Pär Ström



Introduktion till denna pdf

De avslöjanden om amerikansk avlyssning och övervakning som Edward Snowden kom med sommaren 2013 borde egentligen inte förvåna någon. På det principiella planet är likheterna mycket stora med det sedan länge avslöjade amerikanska övervakningssystemet Echelon, vilket jag skrev ett kapitel om i min numera slutsålda bok ”Övervakad” (Liber 2003).

I detta pdf-dokument återpubliceras det aktuella kapitlet, som bland annat innehåller fascinerande vittnesmål från avhoppare om Echelons förmåga. Här finner du också ett annat kapitel från boken Övervakad, nämligen det som handlar om misstankarna om att amerikansk underrättelsetjänst sett till att bygga in så kallade bakdörrar i krypteringsprogramvara och operativsystemet Windows.

Den som vill läsa hela ”Övervakad” kan finna boken på många bibliotek. Så här skrev Charlotte Cederschiöld, som då var vice talman i Europaparlamentet, om boken på dess baksida: ”Pär Ström ger en lättbegriplig bild av det komplexa kontrollsamhälle som modern IT-teknik möjliggör. En viktig bok för alla – fylld med sprängstoff”.

 Du finner detta dokument på

`http://www.atomerochbitar.se/avlyssning.pdf`

Abonnera på mitt nyhetsbrev

Vill du abonnera på mitt nyhetsbrev Big Brother Bulletin (BBB), som handlar om övervakningssamhället, kan du anmäla dig på

`http://www.atomerochbitar.se/ddr-bbb-nyhetsbrev.php`

Innehåll

Echelon – det globala övervakningssystemet

> *”Utan politisk och rättslig kontroll kan Echelon bli ett slags hemlig cyberpolis, utan domstolar, juryer eller någon rätt för individen att försvara sig.”*
>
> James Bamford i boken ”Body of Secrets”

Echelon är ett mycket omfattande och kraftfullt system för övervakning av elektronisk kommunikation. Det har global täckning och bevakar bl a telefonsamtal, faxmeddelanden, e-post, telex, videokonferenser och vanlig radiokommunikation – i princip täcks alla typer av elektronisk kommunikation. Uppgifterna varierar, men det har sagts att systemet har kapacitet att snappa upp tre miljarder meddelanden per dygn.

Margaret ”Peg” Newsham är en avhoppad Echelon-anställd. I tio år arbetade hon åt olika leverantörer av avlyssningsutrustning till NSA (National Security Agency, USA:s mäktigaste underrättelseorganisation, så hemlig att akronymen länge uttyddes ”No Such Agency”). I två år – fram till 1984 – var hon en av de ansvariga för den dagliga driften av Echelons datornätverk på den brittiska Echelon-stationen i Menwith Hill. Så här beskriver hon Echelon i en intervju för den danska tidningen Ekstra Bladet (som i ett stort antal artiklar försökt kartlägga Echelon):

> *”Övervakningen hade en fantastisk precision. Vi kunde peka ut en enskild person eller organisation och övervaka all elektronisk kommunikation – real time – hela tiden. Det skedde utan att personen hade någon chans att upptäcka det, och den mesta informationen skickades snabbt vidare till en annan station med hjälp av de enorma digitala möjligheter vi hade. Det hela skedde utan domares beslut [...] Det är som en sökmotor på Internet. Man kan söka på bestämda nummer, personer eller begrepp, och så kommer allt det upp som är relaterat till det man skrivit in.”*

Echelon bygger på ett gigantiskt nätverk av avlyssningsutrustning av olika slag: Bland annat jättelika parabolantenner på baser i alla fem världsdelar, satelliter (det lär röra sig om cirka 120 stycken), avlyssningssystem på fartyg som kryssar längs avlyssnade länders kuster, avlyssningsanordningar på undervattenskablar (en sådan blev upptäckt 1982) och antenner på ambassader och konsulat. Ovan nämnda Menwith Hill i Storbritannien är en av systemets viktigaste knutpunkter, med ett 30-tal jättelika golfbollsliknande parabolantenner, väldig datorkraft samt minst tre fiberoptiska huvudkablar anslutna till det brittiska telefonnätet (enligt R G Morris, som är chef för Emergency Planning på British Telecom). En annan central knutpunkt är NSA:s högkvarter i Fort Meade i den amerikanska delstaten Maryland.

Namnet på övervakningssystemet är inofficiellt – de deltagande länderna har aldrig erkänt dess existens. Länge pågick därför en debatt om huruvida Echelon över huvud taget existerar eller bara är ett rykte. På senare år har dock bevisen för systemets existens blivit alltmer otvetydiga, och nu får man väl säga att EU har avgjort saken. För några år sedan tillsatte Europaparlamentet en kommitté för att utreda frågan – Tillfälligt utskott för avlyssningssystemet Echelon. Slutresultatet blev att Europaparlamentet i september 2001 antog en resolution (A5-0264/2001) där det slås fast bl a följande:

- Att ”det inte längre finns något tvivel om existensen av ett sådant system”, även om det ifrågasätts om systemets kapacitet är så stor som vissa medieuppgifter gjort gällande.
- Att “det inte är någon tvekan om att syftet med detta system är att i vart fall övervaka privat och kommersiell kommunikation och inte militär kommunikation”.
- Att ”avlyssning av privata meddelanden är ett allvarligt ingrepp i den personliga integriteten, som är garanterad i artikel 8 i Europakonventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna” (och som bara får åsidosättas under vissa, mycket noggrant specificerade omständigheter, såsom för att skydda den nationella säkerheten).
- Att ”det kan antas att Echelon strider mot de principer om skydd för privatlivet som beslutats av Europadomstolen [Europeiska domstolen för de mänskliga rättigheterna i Strasbourg, förf anm]”.

I åtminstone tre europeiska länder – Frankrike, Belgien och Nederländerna – har respektive lands parlament också antagit resolutioner där man konstaterar Echelons existens. I sin resolution ger Europaparlamentet ett antal rekommendationer. Till exempel rekommenderas företag inom EU att använda sig av programvara med öppen källkod, eftersom det är enda sättet att gardera sig mot s k bakdörrar. Dessutom uppmanar man USA och Storbritannien att ömsesidigt avtala om att tillämpa egna regler om skydd för privatliv och företagshemligheter även på det andra landets invånare och företag. Bakgrunden är att det sägs att förbud mot att spionera på det egna landets medborgare och institutioner kringgås genom att man inom ramen för Echelon-samarbetet spionerar på varandras medborgare och institutioner, och sedan utbyter information. Storbritannien och Tyskland uppmanas också att kräva garantier, som ett villkor för att USA:s underrättelsetjänst ska få fortsätta sin verksamhet på dessa länders territorier, för att denna verksamhet inte strider mot Europakonventionen.

Ekonomiskt spionage hjälper amerikanska företag?

Echelon används delvis på ett sätt som nog uppfattas som etiskt riktigt av de flesta i vår kultur, exempelvis för bekämpning av terrorism, illegal vapenhandel och annan mycket grov brottslighet. Om systemet enbart användes på det viset skulle det inte vara särskilt kontroversiellt.

Mycket tyder dock på att verkligheten är mindre vacker. Så här uttrycker sig Carlos Coelho, som var ordförande i Europaparlamentets Echelon-kommitté: ”Om du har ett verktyg, och du kan vinna fördelar av att använda det verktyget, och ingen kan kontrollera din användning av verktyget, kommer du att använda det?” Det finns starka indikationer på att Echelon används för sådant som industrispionage och övervakning

av oliktänkande, politiska motståndare till makthavarna och ideella organisationer. Låt oss börja med att behandla industrispionage och annat ekonomiskt spionage.

Inom det amerikanska näringsdepartementet, Department of Commerce, finns en enhet som ursprungligen bar namnet Office of Intelligence Liaison (vilket ungefär kan översättas med ”Kontoret för underrättelseförbindelser”). År 1996 döptes enheten om till Office of Executive Support. Det sägs att dess syfte är att kanalisera kommersiell information från underrättelseverksamhet vidare till amerikanskt näringsliv. Det sägs också, dock utan att bevis kunnat läggas fram, att sådan information i särskilt hög utsträckning skickas till amerikanska företag som är leverantörer till och partners med NSA och övriga organ inom underrättelseverksamhet. Dessa företag är i många fall stora bidragsgivare vid politikers valkampanjer, vilket sägs skapa ett ömsesidigt beroende mellan företagen och politiska beslutsfattare.

Den skotska undersökande journalisten Duncan Campbell har vigt en stor del av sitt liv åt att kartlägga Echelon, och han har bl a anlitats som expert i frågan av Europaparlamentet. I sin omtalade rapport för Europaparlamentets räkning från år 1999, ”Interception Capabilities 2000”, skriver han att systemet verkligen har använts som ett verktyg för politiskt grundat industrispionage, dvs som ett verktyg för att främja amerikanska företag i konkurrensen på världsmarknaden. De exempel som läckt ut är många. Låt oss börja med två av dem, citerade direkt ur Campbells rapport.

> *”År 1994 snappade NSA upp telefonsamtal mellan [elektronikföretaget] Thomson-CSF och Brasilien avseende SIVAM, ett 1,3 miljarder dollars övervakningssystem för regnskogen i Amazonas. Företaget anklagades kort därefter för att ha mutat medlemmar i den brasilianska regeringens urvalskommitté. Kontraktet gick i slutänden till det amerikanska företaget Raytheon Corporation – som sa efteråt att ’Department of Commerce arbetade mycket hårt för att stödja amerikansk industri i detta projekt’. Raytheon levererar också underhåll och tekniska konsulttjänster till NSA:s satellitspaningsstation vid Sugar Grove.”*

> *”Från en kommersiell kommunikationssatellit snappade NSA upp alla faxmeddelanden och telefonsamtal mellan det europeiska konsortiet Airbus, det saudiarabiska nationella flygbolaget och Saudiarabiens regering. NSA fann att Airbus representanter erbjöd mutor till en saudisk tjänsteman. Denna information skickades vidare till amerikanska tjänstemän som pressade budet från Boeing Co och McDonnell Douglas Corp, som triumferade förra året [1994] i affären på 6 miljarder dollar.”*

Så här kommenteras det senare ärendet av Fred Stock, en annan avhoppad Echelonmedarbetare, i en intervju som genomförts av Ekstra Bladet:

> *”Vi visste vilket plan Frankrike ville sälja och till vilket pris. Vi kände i princip till allting som hade med större transaktioner att göra, sådant som vilka som gav anbud och siffrorna de opererade med, hur mycket de var villiga att betala och sälja för. Vi höll ett vakande öga på vad som hände inom jordbrukssektorn också. Stora veteaffärer, till exempel [...] Vi höll oss uppdaterade med många företags förhandlingsposition. Vi visste vilka anbud de la och när. Över huvud taget var vi mycket väl informerade om deras ärenden.”*

Fred Stock var kommunikationsoperatör på högkvarteret för den kanadensiska underrättelseorganisationen Canadian Security Establishment (CSE). Han hade arbetat där i

20 år när han blev uppsagd 1993 för att ha ställt för många frågor (och har sedan dess haft mycket svårt att hitta ett nytt arbete, något som även gäller arbeten som vanlig tjänsteman utan underrättelseanknytning). Stock uppskattar att han personligen hanterade upp till 3 000 underrättelser om dagen. Han arbetade tillsammans med 55 agenter som hade samma arbetsuppgifter.

Fred Stock berättar i Ekstra Bladet om hur han mot slutet av 1980-talet såg målet för Echelons övervakning skifta karaktär:

> *”En förändring inträffade omkring 1987. Det var då jag plötsligt började se mer och mer meddelanden som hade att göra med Tyskland, Frankrike, Nederländerna, Danmark och andra europeiska allierade. Men det är viktigt att understryka att vi utförde ett väldigt värdefullt arbete för hela den Fria Världen under det kalla kriget [...] Det var därför obehagligt att ta emot meddelanden från NSA som sa att nu var EU, centrerat kring Tyskland, en fiende. Meddelandena handlade också om den asiatiska ekonomin och särskilt Japan. Det var omkring 1990.”*

Stock, som ju egentligen arbetade för Kanada, berättar också om hur USA-centrerad verksamheten var: ”Det är viktigt att göra en sak klar: All information som snappades upp runtom i världen sändes genast till den amerikanska underrättelseorganisationen, NSA. De avgjorde sedan vad som skulle skickas vidare till andra länder.”

Fred Stocks uppgifter om att Echelon i hög utsträckning används för industrispionage bekräftas av en annan tidigare medarbetare på kanadensiska CSE, Edwina Slattery, som också intervjuats av Ekstra Bladet. Hon säger: ”Mitt jobb handlade bara om att analysera övervakning riktad mot the bad guys [det forna östblocket]. Men det fanns andra avdelningar som tog hand om finansiellt och industriellt spionage.”

I Duncan Campbells EU-rapport ”Interception Capabilities 2000” anges fler exempel på att Echelon använts för ekonomiskt spionage. Exempelvis ska det franska deltagandet i världshandelsförhandlingarna inom GATT år 1993 ha avlyssnats. Ett annat exempel är att i september 1993 ska USA:s president Bill Clinton ha beordrat CIA att spionera på japanska biltillverkare i arbete med att utveckla bilar med noll-emissioner (inga utsläpp). Den uppsnappade informationen ska ha skickats vidare till de tre stora amerikanska biltillverkarna: Ford, General Motors och Chrysler.

Tidskriften Insight Magazine rapporterade i en serie artiklar 1997 att president Clinton beordrade NSA och FBI att iscensätta en massiv avlyssningsoperation vid toppmötet Asian/Pacific Economic Conference (APEC) i Seattle 1993. Och den förre lingvisten på den kanadensiska säkerhetstjänsten CSE, Jane Shorten, säger att hon sett rapporter med uppsnappad kommunikation från de mexikanska delegaterna under förhandlingarna 1992–1993 om frihandelsavtalet Nafta.

Den japanska dagstidningen Mainichi Shimbun hävdar att NSA under 20 års tid avlyssnat japansk diplomatisk kommunikation i syfte att komma över ekonomisk information. Tidningen skriver i en artikel från 2001:

> *”Under 1980-talet fångade nätverket [Echeleon] upp information om den japanska regeringens förhandlingar om kolpriser, vilket ledde till att Nya Zeeland fick ett förmånligt avtal för sin kolexport. Det antas att Echelon användes för att snappa upp information från Japan som skulle visa sig förmånlig för företag i Nya Zeeland.”*

På flera håll i Europa har det påstådda industrispionaget kommit upp på högsta politiska nivå. Exempelvis sa Frankrikes tidigare justitieminister, Elisabeth Guigou, i ett tal

till den franska Nationalförsamlingen år 2000, att övervakningsnätverket Echelon ”uppenbarligen omdirigerats till ekonomiskt spionage och övervakning av konkurrenter”.

”Ja, vi har spionerat på er”

Ett partiellt medgivande har faktiskt kommit från amerikanskt håll. Den förre chefen för den amerikanska underrättelseorganisationen CIA, James Woolsey, skrev i en artikel i den amerikanska börstidningen Wall Street Journal i mars 2000 bl a följande:

> *”[...] Ja, mina kontinentala europeiska vänner, vi har spionerat på er. Och det är sant att vi använder datorer för att gå igenom data med användning av nyckelord. Har ni någonsin stannat upp för att fråga er vad det är vi letar efter?*
>
> *Europaparlamentets nyligen avlämnade rapport om Echelon, skriven av den brittiska journalisten Duncan Campbell, har resulterat i arga anklagelser från kontinentala Europa om att amerikansk underrättelsetjänst stjäl avancerad teknologi från europeiska företag så att vi kan – notera detta – ge det till amerikanska företag och hjälpa dem att konkurrera. Mina europeiska vänner, bli realistiska. Det är sant att på en handfull områden är europeisk teknologi överlägsen amerikansk, men, för att säga det så milt jag kan, antalet sådana områden är mycket, mycket, mycket litet. Det mesta av europeisk teknologi är helt enkelt inte värd att stjäla [...].*
>
> *[...] Det är rätt, mina kontinentala vänner, vi har spionerat på er för att ni mutar. Era företags produkter är ofta dyrare, mindre tekniskt utvecklade eller bägge delar, än era amerikanska konkurrenters. Därför mutar ni mycket. Så delaktiga är era regeringar att i många europeiska länder är mutor fortfarande skattemässigt avdragsgilla. När vi har tagit er på bar gärning, kanske ni vill veta, har vi inte sagt ett ord till de amerikanska företagen i konkurrensen. Istället går vi till regeringen som ni mutar och säger till dess företrädare att vi inte ser välvilligt på sådan korruption. De svarar ofta med att ge det mest förtjänstfulla anbudet (ibland amerikanskt, ibland inte) hela eller delar av kontraktet [...].”*

Notera att det partiella erkännandet gäller industrispionage generellt sett, inte existensen av Echelon. Ingen av nationerna som står bakom Echelon har hittills gjort några medgivanden om systemets existens. Duncan Campbell säger så här i ärendet, och lyckas förmodligen på ett bra vis sätta ord på de tankar som många européer har: ”Siffrorna – att amerikanska företag har fått affärer för miljarder dollar – kommer att förbluffa och väcka vrede, inte för att europeiska politiker skulle förneka att en del av deras företag går över gränsen, utan för att USA inte har något rätt att vara såväl domare, jury som bestraffare i detta.”

För övrigt verkar inte ens amerikanska källor samstämmiga när det gäller den förre CIA-chefens förnekande av att avlyssnad ekonomisk information skickas vidare till amerikanska företag. Så här skrev den amerikanska tevekanalen ABC i sin nyhetstjänst på Internet, ABC News, i februari 2000:

> *”Amerikanska myndighetspersoner har förnekat att den underrättelseorganisation som är ansvarig för avlyssning av utländsk kommunikation,*

NSA, har eller skulle kunna ge den informationen till amerikanska företag [...] Men amerikanska myndighetspersoner medger privat att NSA verkligen ger sådan information till ett antal andra myndigheter, inklusive Commerce Department [Handelsdepartementet], som ofta arbetar med att hjälpa amerikanska affärsprojekt utomlands. Och en myndighetsperson som bad att få vara anonym sa att myndighetspersoner på Commerce [Department] kan ha delat med sig av sådan information till amerikanska företag som konkurrerar i internationella affärer [...]

En myndighetsperson vid Utrikesdepartementet upprepade idag [talesmannen på Utrikesdapartementet] Rubins försäkran att NSA inte ger sådan information till amerikanska företag, men avböjde att kommentera frågan om huruvida Commerce [Department] kan ha gjort det [...] Dokument på Commerce Departments webbplats bekräftar att departementet tar emot information från underrättelsevärlden. Sådan information handläggs av departementets Office of Executive Support, som fram till 1996 kallades Office of Intelligence Liaison. Webbplatsen säger dock ingenting om hur underrättelseinformationen används av Commerce."

Ett annat partiellt bekännande har enligt Le Monde Diplomatique kommit från Zbigniew Brzezinzki, som var säkerhetspolitisk rådgivare åt president Jimmy Carter. Enligt tidningen har Brzezinzki sagt att när man har tillgång till information är det svårt att sätta en gräns för hur mycket man ska uppfatta. Vidare vände han på anklagelserna mot USA och frågade om det inte var omoraliskt av de franska och tyska regeringarna att diskutera saker som de inte vill att USA ska känna till.

Spionage mot Greenpeace, Amnesty och politiker

Som nämnts finns det också indikationer på att Echelon används för övervakning av ideella organisationer. Fred Stock, den tidigare medarbetaren på den kanadensiska underrättelseorganisationen CSE, säger exempelvis till Ekstra Bladet att miljöorganisationen Greenpeace stod under konstant bevakning:

"Baserat på de meddelanden jag såg var det väldigt tydligt att vi kunde följa Greenpeaces farkoster vart de än åkte. Och vi hade ständigt fullständig kännedom om deras exakta positioner. Det fanns alltid meddelanden om Greenpeace: om deras fartyg, var de gick i hamn, deras förmodade destinationer och planerade aktiviteter [...] Vi var noggrant och exakt informerade om deras tilltänkta planer – i förväg. Redan innan de gjort något. Greenpeace var ett mycket viktigt mål."

I samma tidningsartikel uppger Mads Christensen på Greenpeace i Danmark att han nyligen varit med om händelser som stöder misstanken att de utsatts för spionage. Han berättar hur de planerade fyra aktioner riktade mot fartyg lastade med genmanipulerade produkter, varav tre misslyckades, något han säger är ovanligt. "Det intressanta är att de tre misslyckade aktionerna alla var riktade mot amerikanska fartyg lastade med genetiskt manipulerade produkter från företaget Monsanto. Vid en av aktionerna greps våra aktivister i England redan innan de hunnit påbörja aktionen, och i de två andra fallen dirigerades fartygen om [...] [Den enda lyckade aktionen berörde] ett argentinskt fartyg, och det var lustigt att den enda framgångsrika aktionen var den som inte riktades

mot ett fartyg från USA", säger Mads Christensen. Vittnesmålet bevisar naturligtvis ingenting, det utgör bara en indikation.

Ett annat viktigt mål för Echelons övervakning är medborgarrättsorganisationen Amnesty International, enligt Fred Stock. Så här säger han till Ekstra Bladet:

> *"När jag arbetade för CSE såg jag oräkneliga rapporter om Amnesty International. De allra flesta av rapporterna var slutprodukter preparerade av NSA. NSA samlade in råa underrättelser från hela världen och använde dem i rapporterna som jag tog emot [...] Vissa av rapporterna handlade om ögonvittnen och samvetsfångar i fängelser runt om i världen. Men det fanns också rapporter om planerade kampanjer, och ibland fick vi rapporter med annan information om organisationen."*

Margaret Newsham, en annan avhoppad Echelon-medarbetare som omnämndes tidigare i kapitlet, stöder Stocks uppgifter:

> *"Vi övervakade vanliga människor, intressegrupper, företag, och sådant. För att sikta in sig på vissa subjekt behövde man bara koda in dem i en dator och skriva 'Amnesty International' eller 'Margaret Newsham', till exempel. Sedan kunde vi övervaka subjektet i fråga – medan de kommunicerade, märk väl."*

Newham berättar vidare om den dag i sitt arbete på den brittiska Echelonstationen Menwith Hill då hon insåg att verksamheten var moraliskt förkastlig:

> *"Jag satt med en av våra många "översättare". Han var expert på språk som ryska, kinesiska och japanska. Plötsligt frågade han mig om jag ville lyssna på en konversation som ägde rum i USA på ett kontor i senatsbyggnaden. Då hörde jag tydligt en amerikansk sydstatsdialekt som jag tyckte jag hade hört förut. 'Vem är det?' frågade jag översättaren som sa att det var den republikanske senatorn Strom Thurmond. 'Oh my gosh', tänkte jag. Vi spionerar inte bara på andra länder, utan också på våra egna medborgare. Det var då jag i sanning förstod att det vi höll på med inte hade något att göra med USA:s nationella säkerhetsintressen."*

Newsham underrättade en amerikansk kongressman om vad hon uppfattade som missförhållanden inom den underrättelseverksamhet hon deltog i, och längre fram vittnade hon i en hemligstämplad kongressutredning. Enligt tidningen New Statesman har avslöjandet lett till en rädsla att den övervakning av amerikanska medborgare som avslöjades under den s k Watergate-skandalen, och som stoppades efter president Nixons avgång, ska ha återupptagits.

Fred Stock bekräftar hur politiker hölls under luppen: "Vi visste var de olika politikerna befann sig, och vad de tänkte göra. Vi hade inget mindre än tillgång till deras personliga planer." På frågan om även europeiska politiker övervakades svarar Stock: "Absolut. Till och med statschefer. Baserat på de underrättelser jag såg visste vi vilka de tänkte träffa och vad de hade talat om. Det var ett fascinerande jobb. Vi hade ständig koll på händelser över hela världen."

Ett annat exempel har avslöjats av Mike Frost, anställd vid den kanadensiska underrättelsetjänsten åren 1972–92. I det amerikanska nyhetsprogrammet 60 minutes år 2000 sa han att den dåvarande brittiska premiärministern Margaret Thatcher en gång bad den kanadensiska säkerhetstjänsten CSE att använda Echelon för att snappa upp

kommunikationen för en av sina ministrar i regeringen, som hon misstänkte för bristande lojalitet. Frosts närmaste chef, Frank Bowman, reste till London för att under tre veckor vara behjälplig vid spionaget. Därefter fick Bowman order att lämna över banden till den engelska säkerhetstjänsten GCHQ. Frost menar att syftet med att ta in någon från Kanada var att den brittiska regeringen utan att ljuga skulle kunna neka till all inblanding.

En annan händelse som kretsar kring Margaret Thatcher har publicerats av den brittiska tidningen London Observer. Där berättar en tidigare anställd på den brittiska underrättelseorganisationen British Joint Intelligence Committe, Robin Robison, att Mrs Thatcher personligen beordrade uppsnappning av kommunikationen till och från tidningen Observers moderbolag Lonrho. Bakgrunden var att Observer under 1989 publicerade uppgifter om att mutor hade betalats ut till Thatchers son Mark i en stor vapenaffär mellan Storbritannien och Saudiarabien. Robison säger sig personligen ha levererat det uppsnappade materialet till Margaret Thatchers kontor.

Svensk surfare fastnade i Echelons nät?

Låt oss återvända till den kanadensiske avhopparen Mike Frost. Ett annat av hans avslöjanden ger en bild av hur bred och allomfattande övervakningen tycks vara. Även helt vanliga ”Svenssons” riskerar att råka illa ut. Frost berättar för tidningen Ekstra Bladet hur en kvinna blev inlagd i registret över misstänkta terrorister för att hon i telefonen berättade för en vän att hennes son hade ”bombat” i en skolpjäs (verbet ”bomb” på engelska betyder i teatersammanhang ”misslyckas”). ”Datorn spottade ut den konversationen. Analytikern var inte säker på vad konversationen handlade om, så för att vara på den säkra sidan listade han kvinnan”, säger Frost.

Ett annat (påstått) exempel på hur en ”vanlig” människa fastnat i Echelons nät kan hämtas från en artikel i den svenska samhällskritiska tidskriften Contra. Så här skrev man i juli 2001 (utdrag ur artikeln):

> *”En av våra läsare berättar att han via en sökmotor letat efter RAF, Rote Armee Fraktion, den tyska marxistiska terroriströrelsen som verkade på 1970-talet och som ofta går under namnet ’Baader-Meinhof-ligan’ efter de mest ökända skurkarna i ligan, Andreas Baader och Ulrike Meinhof. Vår läsare hade sin dator bakom en s k brandvägg och hade installerat ett program som varnar för alla ”attacker” mot datorn. Attacker var förhållandevis ovanliga, men efter sökningen på RAF visade det sig plötsligt att omvärlden var intresserad av vår läsares dator. Inte mindre än sju attacker gjordes mot brandväggen. Och inte från vilken omvärld som helst.*
>
> *Han följde upp de attacker som skedde mot brandväggen och kunde med programmet Neotrace spåra dem till den danska ön Anholt. Anholt, som ligger mitt i Kattegatt, mellan Sverige och Danmark, har cirka 150 invånare. De flesta livnär sig på jordbruk och turism, men det finns också en avskärmad väderstation. Det har påståtts att [...] Echelon ska ha en avlyssningsstation i anslutning till väderstationen på Anholt. Hur det förhåller sig med det vet vi inte, men vår läsares spår upphörde vid Anholt, där det var omöjligt att spåra attacken mot brandväggen vidare bakåt.*
>
> *En mer traditionell metod för att spåra attackerna gav resultatet att de kom från företaget Space and Naval Warfare Systems (Spawar) i Washington DC och San Diego (den amerikanska flottans högkvarter ligger i San*

Diego). Spawar sorterar i själva verket under amerikanska flottan. När vår läsare gjorde efterforskningar efter varifrån han utsatts för en attack blev han själv kontrollerad av Telia abuse (Telias kontroll av otillbörlig aktivitet på nätet!)"

Eftersom inga namn nämns är det svårt att bedöma uppgifternas trovärdighet. Man kan dock konstatera att ovanstående passar väl in i den helhetsbild av Echelons funktionssätt som andra källor gett.

Vilka resurser har egentligen Echelon?

Det har diskuterats hur heltäckande Echelons avlyssning egentligen är. På grund av verksamhetens extremt hemliga karaktär är det förstås omöjligt att skaffa sig ett säkert svar på den frågan. Det verkar dock stå klart att det i medier förekommit en del överdrivna uppgifter. Exempelvis anser man numera att det inte stämmer, som det sades för några år sedan, att all telefontrafik, e-post, fax och telex i Europa filtreras av Echelon.

Många källor har rapporterat om den oro underrättelsetjänster känt med anledning av den successiva övergången till nya och mer svåravlyssnade kommunikationskanaler. Det handlar bl a om fiberoptiska kablar (som inte läcker information, vilket elektriska kablar gör), digital mobiltelefoni (som skickar informationen söndertstyckad i datapaket istället för som en lättavlyssnad analog röst) och Internettrafik/e-post (som också styckar upp informationen på mängder av datapaket som dessutom kan gå helt olika vägar).

Enligt boken "Body of Secrets", där James Bamford försökt kartlägga NSA:s historik och verksamhet idag, har NSA efter viss möda funnit vägar att lösa dessa nya problem. Så här uttrycker sig enligt nämnda bok NSA:s vicedirektör för tjänster, Terry Thompson, i en strikt hemlig diskussion 1999 (som uppenbarligen läckt ut) med delar av NSA:s teknikerkår:

"De förutsägelser vi gjorde för fem, sex, åtta år sedan om ökande mängder kommunikation och vad det kommer att innebära för våra analytiker har alla besannats, till stor del tack vare det arbete som ni och andra utfört. Vi har kommit mycket längre nu när det gäller förmåga att skaffa tillgång till och samla in nätverksdata, fiberoptik, mobiltelefoninformation, alla de olika typer av kommunikation som vi riktar in oss på, och det resulterar i mycket material för våra analytiker. Våra verktyg är på gång okay. [...]"

Thompson berättar vidare, enligt "Body of Secrets", om hur NSA skaffar sig tillgång till den information som flyter genom Internet genom att rekrytera ledande tekniker från de (amerikanska) företag som tillverkar dataväxlar och liknande utrustning. Särskilt nämns leverantören Cisco, som med stor marginal är världsledande inom dataväxlar. Med hjälp av de rekryterade produktspecialisterna utför NSA så kallad "reverse engineering" (analys av hur en produkt är konstruerad), vilket ofta avslöjar produkternas svaga punkter och därmed ger uppslag till hur avlyssning bäst sker.

Traditionella elektriska kablar läcker elektromagnetisk strålning som relativt lätt kan snappas upp (genom "induktion"), medan fiberoptiska kablar inte gör det. Därför har den snabba övergången till fiberoptik skapat huvudbry hos underrättelsetjänster. Fiberoptik kan dock avlyssnas om en skarp böj skapas på fibern så att en smula ljus läcker ut. Detta är svårt att göra i praktiken, särskilt om kabeln ligger i havet på ett par

tusen meters djup. Enligt tidskriften Spectrum, utgiven av den internationella standardiseringsorganisationen IEEE, håller USA på att utrusta ubåten Jimmy Carter särskilt för detta ändamål. Ubåten, som nu ligger i hamn och förses med extrautrustning till ett värde av 887 miljoner dollar, ska enligt Spectrum vara färdig i mitten av 2005. Liknande uppgifter om Jimmy Carter har publicerats i tidningen Los Angeles Times. Det lär röra sig om den mest avancerade spionubåt som någonsin byggts.

Vidare har det sagts att Echelon innehåller funktioner för automatisk igenkänning av talade ord, så att telefonsamtal kan datorövervakas på jakt efter vissa nyckelord. På senare tid har dock många börjat tvivla på om NSA, trots ihärdiga försök, verkligen lyckats få en sådan funktion att fungera tillfredsställande. Däremot anses det korrekt att systemet redan idag kan söka efter ”röstavtyck”, så att en viss person kan upptäckas av datorer så snart vederbörande lyfter en telefonlur.

Samtidigt finns det källor som hävdar att strävandena att utveckla fungerande ordigenkänning faktiskt krönts med framgång. En forskargrupp vid University of Southern California, som till stor del finansieras av det amerikanska försvarshögkvarteret Pentagon, säger sig ha skapat det första maskinella systemet som kan känna igen talade ord bättre än en människa. Systemet, som går under benämningen ”Speaker Independent Speech Recognition System”, använder s k neurala nätverk som efterliknar den mänskliga hjärnans sätta att arbeta. Forskarna hävdar också att systemet kan uppfatta och tolka konversationer som förs i bakgrunden, exempelvis som en del av sorlet på ett cocktailparty.

En föreställning om vilken funktionalitet Echelon har avslöjades – kanske av misstag – av en viss Bruce McIndoe när han intervjuades av danska Ekstra Bladet. McIndoe var med och byggde upp Echelon, vilket han också bekräftar i intervjun, och har efter slutförandet av Echelons första version arbetat med en utökad version, Echelon II. År 1998 lämnade han detta arbete för att övergå till privat tjänst. På tidningens fråga om hur NSA ser på att han numera tillämpar samma teknologi i den privata sektorn som han förut arbetat med för myndigheternas räkning säger han så här: ”Mycket av den teknologi som utvecklats av NSA kommer förr eller senare att sprida sig till civilt liv. Det gäller saker som ordigenkänning, automatisk översättning, språkigenkänning, osv.”

Det framstår som uppenbart att i princip all kommunikation som passerar genom satelliter övervakas av Echelon, och som visats ovan finns indikationer på att även undervattenskablar och andra fiberoptiska kablar täcks in. Frågan är hur väl underrättelsetjänsterna bakom the UKUSA agreement lyckats täcka in andra kommunikationskanaler. Ett vanligt sätt att vidarebefordra elektronisk kommunikation inom ett land är via s k mikrovågslänkar, vilket innebär att radiovågor av mikrovågstyp sänds i en rak linje från en parabolantenn till en annan några mil längre bort, och sedan vidare till nästa, osv. Mikrovågslänkar kan förefalla svåra att avlyssna för en främmande makt, eftersom signalerna är mycket väl riktade och av fysikaliska skäl bara fortsätter i en linje rakt framåt, utan att följa jordens krökning. Skenet bedrar dock i detta fall. Det är känt att NSA redan på 1960-talet utvecklade en teknologi som faktiskt drar nytta av mikrovågornas rätlinjighet – de mikrovågor som passerar vid sidan om den mottagande antennen fortsätter ju ut i rymden, där lurande spionsatelliter tar emot dem.

Ett centralt problem för en spionageverksamhet av Echelons omfattning är naturligtvis den gigantiska mängden data som genereras. Detta kräver en mycket hårdhänt maskinell sållning på ett tidigt stadium, exempelvis sållning efter nyckelord, person eller organisation. Den ideala lösningen på sikt (ur underrättelsetjänsternas perspektiv) skulle väl vara om sållningen inte behövde göras av underrättelsetjänstens superdatorer utan kunde ske decentraliserat ute hos de avlyssnade, med användning av de avlyssna-

des egen utrustning. Då skulle plötsligt mängden data framstå som liten i förhållande till hårdvarans beräkningskapacitet. Denna övervakarens önskedröm skulle elegant kunna förverkligas med spionprogram och/eller bakdörrar i världens alla datorer – exempelvis dolt i operativsystemet.

Det bör understrykas att ovanstående resonemang kring vad Echelon kan och inte kan göra av naturliga skäl präglas av stor osäkerhet.

Kan man skydda sig mot Echelon?

Hur skyddar man sin information mot Echelons stora öron? Det är svårt, och det beror på vilken typ av kommunikation man ägnar sig åt.

Om det handlar om telefoni vet man för det första inte om den del av nätet som används täcks in av Echelon eller inte. Ju mer internationell kommunikationen blir, desto mer verkar sannolikheten öka för bevakning. En första mycket grundläggande försiktighetsåtgärd för företag och andra med hemlig information är att åtminstone aldrig avhandla topphemliga ärenden över en internationell uppkoppling.

Det kan också vara ett alternativ att skaffa utrustning för talförvrängning (”scrambler”), men sådan måste installeras i förväg på båda sidor och passar därför bäst vid regelbunden kommunikation med en och samma motpart. En scrambler kan visserligen knäckas av en underrättelsetjänst som verkligen vill det, men eftersom det kräver betydligt större resurser än att avlyssna ett vanligt telefonsamtal minskar rimligen sannolikheten väsentligt för att informationen läcker ut (om du inte är ett högprioriterat mål för någon underrättelsetjänst, förstås).

Om det handlar om icke talad kommunikation, såsom e-post, fax och telex, är situationen en annan. Här finns möjligheten att kryptera, och den bör användas. Om nu inga hemliga framsteg i kodknäckningsvetenskapen har gjorts på senare tid verkar det som om stark kryptering fortfarande i princip sätter stopp för snokar. Företag, myndigheter och andra borde kryptera sin kommunikation i mycket högre utsträckning än idag (det gäller egentligen privatpersoner också). Sedan gäller det ju att se till det inte är en ”riggad” krypteringsprodukt som används. Ett alternativ för den riktigt säkerhetsmedvetne är att kryptera två gånger, med olika krypteringsprodukter, helst från olika länder. Detta blir naturligtvis mer omständligt. Det tråkiga är att det finns en direkt koppling mellan graden av säkerhet i en kommunikation och hur krånglig den är.

En annan åtgärd som enkelt kan vidtas är att låta bli att använda de mest kritiska orden. Dessa kan ersättas med omskrivningar, eller förvrängas (exempelvis så att ”stridsflygplan” skrivs som ”str fly pln”). Denna åtgärd torde knappast garantera att meddelandet ifråga klarar sig från att fångas upp av Echelons filter, men rimligtvis ökar chansen (eftersom resurserna hos Echelon inte räcker till att köra samtliga meddelanden genom avancerade analysprogramvaror).

I de riktigt stora sammanhangen, såsom vid internationella upphandlingar av telekomutrustning eller stridsflygplan, kan det vara idé att överväga att helt hålla sig utanför den elektroniska världen. Ett papper i ett kuvert skickat med kurirpost kan inte ”avlyssnas” (åtminstone har det inte läckt ut några uppgifter om att så skulle kunna ske).

Även privatpersoner kan använda kryptering för all elektronisk kommunikation. Det tråkiga är att krypteringsprogramvaror ännu inte är riktigt så användarvänliga som de borde vara, vilket gör att många förmodligen väljer att avstå. I kapitel 23, Skyddsmedel mot snokande, går vi djupare i de här frågorna.

”Hemlig cyberpolis utan rätt för individen att försvara sig”

Echelon utgör inte bara ett hot mot stater, företag och organsationer, utan även mot individer. Människor kan bli svartlistade baserat på mycket osäkra indicier, utan möjlighet att rentvå sig. Så här skriver James Bamford i ”Body of Secrets”. Observera att detta skrevs före den 11 september:

> *”Det finns en mycket viktigare fråga: Det är huruvida Echelon i praktiken eliminerar skyddet för personlig integritet – som är en fundamental mänsklig rättighet. Några uppgifter ur en konversation som snappas upp i etern, kanske ryckta ur sitt sammanhang, kan feltolkas av en analytiker som sedan i hemlighet skickar den vidare till polismyndigheter och underrättelseorganisationer i hela världen. Den missvisande informationen lagras sedan i NSA:s gigantiska dataarkiv [...] Till skillnad från uppgifter om amerikanska medborgare, som inte får sparas mer än ett år, kan uppgifter om utlänningar sparas hur länge som helst. Outplånlig kan informationen klibba fast vid individen så länge han lever. Han får aldrig veta hur han hamnade på tullens svarta lista, vem som satte upp honom på den, varför han inte fick det där kontraktet – eller också kan något ännu värre hända.*
>
> *Några uppgifter från NSA eller CIA handlade om en egyptisk invandrare, Nasser Ahmed, som sökte politisk asyl i USA. Den hemliga informationen ledde till att han häktades; utan möjlighet att släppas fri mot borgen hölls han fängslad i ensamcell i mer än tre år i väntan på deportation. Trots att hans advokat, som själv en gång utsattes för illegal NSA-övervakning, kämpade i flera år fick han aldrig veta vilka ’hemliga bevis’ man hade mot honom eller hur USA hade fått tag på dem. I denna Kafka-liknande värld kunde han inte försvara sig mot anklagelserna, eftersom han inte fick reda på vilka de var; de var hemliga. Först efter att arab-amerikanska grupper lyckats mobilisera ett tillräckligt politiskt tryck mot Justitiedepartementet släppte man där ifrån sig en del av uppgifterna. Ahmed kunde då bemöta anklagelserna och slutligen återfå sin frihet. [...]*
>
> *Utan politisk och rättslig kontroll kan [Echelon] bli ett slags hemlig cyberpolis, utan domstolar, juryer eller någon rätt för individen att försvara sig.”*

Bakdörrar – förrädare i vanliga programvaror

”Med företagsledare på högsta nivå handlar det oftast om en vädjan till patriotismen. Med mellanchefer av den kommersiella sorten är det ’Gör det här så får ni förmånlig exportbehandling’. Till de riktigt tekniska människorna är det ’Varför gör ni inte det här?’ Och sedan inser man inte vad det är som föreslås förrän man ser ingenjörerna bli vita.”

Källa inom NSA till tidningen Baltimore Sun

Vi har i föregående kapitel diskuterat risken för att våra datorer smittas av spionprogram, dvs ovälkomna dolda program som i smyg sänder iväg information till någon annan. Kan den som noga kontrollerar att det enbart finns programvara från de stora och etablerade mjukvaruhusen installerad på sin dator eliminera spionagerisken? Det är inte helt säkert. Det finns något som heter ”bakdörrar”, vilket är ungefär vad det låter som: En i programmet inbyggd väg förbi alla säkerhetsspärrar, som är hemlig och osynlig för alla utom den som byggt in bakdörren. Detta låter förvisso som hämtat ur James Bonds värld. Som bekant förekommer det dock att verkligheten överträffar dikten, och det finns tecken som tyder på existensen av sådana bakdörrar, inbyggda på initiativ av mäktiga organisationer, även i mycket betrodda programvaror.

Den häpnadsväckande historien om Crypto AG

Den ryskfödde svenske kryptologen Boris Hagelin (1892–1983) konstruerade redan under andra världskriget en krypteringsmaskin som såldes i 140 000 exemplar till det amerikanska försvaret. Hagelin blev personlig vän med en annan ryskfödd kryptolog, William F Friedman, som då var den amerikanska arméns ledande kryptolog. Friedman blev senare special assistant till direktören för NSA.

År 1952 startade Hagelin i Schweiz företaget Crypto AG, som snabbt etablerade sig som världsledande inom krypteringsteknologi. Till en början utvecklade och sålde man mekaniska krypteringsmaskiner, men på 70talet gick man över till mjukvarubaserad kryptering. Företaget skaffade sig en position som mycket välrenommerat, och hade under det kalla krigets dagar hjälp av det faktum att man kom från ett neutralt land. För att säkerställa att ingen främmande makt hade manipulerat krypteringsutrustningen ville många köpa från ett företag i det alliansfria Schweiz. Crypto AG blev det mer eller mindre självklara valet för kryptering på allra högsta nivå, och har sedan 1950-talet haft cirka 120 nationer som kunder – nationer som använt företagets utrustning för

att kryptera diplomatiska, handelspolitiska och andra meddelanden som skickats mellan ambassader, departement, med mera, liksom topphemliga militära meddelanden. Många storföretag har också använt företagets utrustning när man skickat känslig teknisk och affärsmässig information via exempelvis telex, radio, fax och teletype (liksom på senare tid datornät).

Kort sagt kan man säga att större delen av världen under ett halvt sekel har använt Crypto AG:s utrustning för sin allra mest hemliga kommunikation. Och det verkar som om amerikanska NSA (National Security Agency) under hela denna tid kunnat ta del av meddelandena som om de varit skrivna i klartext. Enligt ett antal olika källor med hög trovärdighet har maskinerna, och längre fram mjukvaran, nämligen riggats så att den slumpmässiga engångsnyckel som krävs för att läsa meddelandet har bifogas med varje meddelande (men dolt, så att bara NSA kan hitta den). Det är ungefär samma sak som om en reservnyckel till kassaskåpet i en värdetransportbil av tillverkaren skulle ha gömts i motorrummet – förare och personal vet ingenting, men rånare som är i maskopi med tillverkaren kan gå direkt på nyckeln.

Mystiska besök från amerikanska ”tekniska konsulter”

Affären började rullas upp år 1992. Redan en dag innan kroppen efter den tidigare iranske premiärministern Shahpour Bakhtiar hittades skickade den iranska säkerhetstjänsten Vevak ett kodat meddelande till Irans diplomatiska representationer i London, Paris, Bonn och Genève med frågan ”Är Bakhtiar död?”. Iranierna förstod på brittiska och amerikanska tidningsartiklar att meddelandet avlyssnats, och leverantören av krypteringssystemet blev misstänkt. Försäljningsrepresentanten för Crypto AG i Iran sedan 13 år, Hans Buehler, greps och anklagades för spioneri. Han förhördes fem timmar om dagen under nio månader. Buehler blev aldrig torterad, men spändes fast på träbänkar och skrämdes med att han skulle bli misshandlad. ”Vid den tiden visste jag inte om att vår utrustning hade riggats, annars hade de med sina metoder fått mig att prata”, sa Buehler senare.

Crypto AG lyckades köpa hans frihet för 1 miljon dollar. Några veckor efter hans hemkomst blev han uppsagd från sin tjänst, och företaget krävde att han skulle betala tillbaka lösensumman. Det intressanta som hände då var att ett antal tidigare anställda vid Crypto AG kom till Buehlers försvar, och berättade hur de sett krypteringsutrustning bli manipulerad. En tidigare ingenjör på företaget sa:

> *”Jag har bevis på att kodmaskiner riggats. För 15 år sedan såg jag amerikanska och tyska ingenjörer fiffla med våra maskiner. Det tog lite tid innan jag var säker på manipulationerna. Bevisen: tekniska dokument [...] jag la dem i ett bankfack. Sedan informerade jag åklagarämbetet i Bern. Det var många samtal. Plötsligt bröts dessa kontakter och alltihop rann ut i sanden.”*

Tvisten mellan Buehler och Crypto AG gick till domstol. Några dagar innan de tidigare Crypto AG-medarbetarna skulle vittna löstes tvisten i godo, och det ingick i överenskommelsen att parterna inte får avslöja något om densamma.

Den amerikanska tidningen Baltimore Sun utges i samma område som NSA:s högkvarter ligger, och tidningen har i en serie artiklar 1995 granskat organisationens verksamhet. En av de tidigare Crypto AG-anställda som trätt fram är Juerg Spoerndli, anställd på företaget fram till 1994. Så här säger han, enligt Baltimore Sun:

”Först var jag idealistisk, men jag anpassade mig snabbt [...] Det nya målet var att hjälpa Storebror USA att se över axeln på de här länderna. Vi sa, ’Det är bättre att låta USA se vad de här diktatorerna gör’ [...] Men det är ändå en imperialistisk syn på världen. Jag tycker inte man ska göra affärer på det viset.”

Spoerndli berättar också att han hört från äldre ingenjörer på Crypto AG att det förekommit mystiska besök från amerikanska ”tekniska konsulter”. Han säger vidare, enligt Baltimore Sun, att han i slutet på 1970-talet ”under mystiska omständigheter blev beordrad att ändra krypteringsalgoritmerna” för att försvaga krypteringen.

En annan tidigare anställd, Ruedi Hug, är också kritisk. ”Jag känner mig lurad”, säger han. Ytterligare en tidigare anställd säger att man på Crypto AG var tvungen att skicka all utrustning till NSA och dess tyska motsvarighet för godkännande. En fjärde tidigare ingenjör säger att han hörde Boris Hagelins son, Boris Hagelin Jr, beklaga sig över att hans pappa tvingade honom att rigga maskinerna. När ingenjören konfronterade fadern med uppgifterna bekräftade han dessa, och motiverade det men en teori om behov av politiskt förmynderi. ”Han sa att olika länder behövde olika grad av säkerhet”, säger ingenjören som vill förbli anonym enligt Baltimore Sun.

Det verkar inte bara ha varit skurkstater som fått sina meddelanden lästa av NSA och deras samarbetspartners. Exempelvis sägs det att den hemliga brittiska underrättelseorganisationen GCHQ under de känsliga förhandlingarna mellan Storbritannien och Irland 1985 i klartext kunde läsa diplomatisk trafik som sändes krypterat mellan Irlands ambassad i London och det irländska utrikesdepartementet i Dublin. Enligt pressuppgifter hade Irland dessförinnan köpt krypteringsutrustning från Crypto AG för mer än 1 miljon irländska pund.

På motsvarande sätt kunde britterna under Falklandskriget mot Argentina i klartext ta del av argentinarnas meddelanden, som krypterats med utrustning från Crypto AG. Det sägs också att USA vid ett tillfälle krävde av Pakistan att landet skulle köpa krypteringsutrustning från Crypto AG och ingen annan för att landet skulle få amerikanska militära krediter.

Baltimore Sun har låtit en expert, Alan T Sherman, professor och krypteringsspecialist på University of Maryland, gå igenom de tekniska detaljerna i anklagelserna från tidigare ingenjörer på Crypto AG. Han säger att anklagelserna är trovärdiga.

Crypto AG tillbakavisar kategoriskt alla anklagelser. Trots att förtroendet för företaget fick sig en knäck när dessa uppgifter kom ut på 1990talet, och försäljningen rasade, har Crypto AG uppenbarligen lyckats klara krisen och finns kvar än idag. ”Total information security” är enligt webbplatsen deras mantra.

Vädjan till patriotismen

Crypto AG kanske inte är det enda fallet i sitt slag. Envisa uppgifter från olika källor hävdar att den amerikanska underrättelseorganisationen NSA ger bättre exportvillkor och andra förmåner till amerikanska företag om de låter NSA få en egen bakdörr till deras programvaror. NSA:s metoder lär variera, och både piska och morot lär användas. Så här säger en källa med lång erfarenhet inom området till The Baltimore Sun 1995: ”Med företagsledare på högsta nivå handlar det oftast om en vädjan till patriotismen. Med mellanchefer av den kommersiella sorten är det ’Gör det här så får ni förmånlig exportbehandling’. Till de riktigt tekniska människorna är det ’Varför gör ni inte det

här?' Och sedan inser man inte vad det är som föreslås förrän man ser ingenjörerna bli vita."

För några år sedan hävdes restriktionerna i sin tidigare form för amerikanska företag att exportera system för stark kryptering. Den ledande amerikanska IT-tidningen Computerworld skrev i en artikel strax före lagändringen att denna nyordning riskerade att skapa en situation där amerikanska myndigheter pressar amerikanska mjukvaruföretag att bygga in bakdörrar i sina produkter. Så här skrev tidningen i september 1999: "Även om de nya reglerna skulle eliminera det nuvarande licensförfarandet för starka krypteringsteknologier, skulle företag vara tvungna att genomgå ett engångsförfarande med en teknisk genomgång från en hittills icke avslöjad myndighet. Barry Steinhardt på American Civil Liberties Union, sa att han tror att detta blir ett tillfälle för FBI och NSA att tvinga företag att skapa säkerhetshål i deras krypteringsprodukter eller att avslöja affärshemligheter. Det skulle ge myndigheterna tillgång till data som säkrats med dessa företags produkter."

Så här skriver CNN på sin webbplats:

> *"Spöken från NSA:s högkvarter i Fort Meade har kört fram och tillbaka i Silicon Valley och gjort besök hos företag, alltifrån branschledare som Netscape Communications Corp. och Sun Microsystems, Inc. till start-ups som VPNet Technologies, Inc., för att kika på produkter som fortfarande är på ritbordet. NSA vill att mjukvaruföretagen ser till att alla produkter med stark kryptering erbjuder något sätt för myndigheterna att komma åt data [...] Det har gått så långt att inget företag [...] ens börjar utveckla en produkt innan man stämt av med Fort Meade. Det inkluderar till och med den förmodade regenten i mjukvaruuniversum, Microsoft Corp."*

Det är också intressant att citera den tidigare omnämnda hemligstämplade australiska rapport från 1997, beställd av Australiens regering, som läckt ut. Den heter "Review of Policy Relating to Encryption Technologies" och har utarbetats av Gerard Walsh, tidigare deputy director på underrättelseorganisationen Australian Security Intelligence Organisation (ASIO). I rapporten står bl a, enligt den brittiska tidningen Guardian:

> *"Att bygga in en permanent grupp kommandon som inte specificeras i programmet skrivet av tillverkaren, kan hjälpa till att skapa en fjärrkontroll (remote switching device) med förmåga att utfärda kommandon på begäran."*

En intressant indikation som stöder teorin om att bakdörrar existerar ges också av några uttalanden från 1999 av den amerikanske republikanske kongressledamoten Curt Weldon, som då också var ordförande för amerikanska Research Committee for National Security. Han nämnde i förbifarten i en paneldiskussion att under det första Irakkriget (1991) hade amerikanska officerare snabbare tillgång till Saddam Husseins order än de irakiska officerare för vilka orderna var ämnade, på grund av att USA knäckt den irakiska militärens koder. Weldon gav en antydan om hur det gått till. Enligt den amerikanska nyhetstjänsten Tech Law Journal sa han bland annat:

> *"Men poängen är att när [USA:s vice försvarsminister] John Hamre briefade mig, och gav mig tre nyckelpunkter i denna förändring, är det många obesvarade frågor. Han försäkrade mig att i diskussioner han haft med folk som Bill Gates och [dåvarande koncernchefen] Gerstner från IBM att det skulle vara, någon sorts, jag vet inte om det är en, outtalad möjlighet*

att få tillgång till system om vi behöver det. Nu vill jag veta om det är del av policyn, eller om det bara är något som vi blir försäkrade, som behöver sägas. Därför att, om det är någon slags tyst överenskommelse, skulle jag vilja veta vad det är. (...)

Men, jag är också, som senior ledamot av Security Committee, som ordförande i Research Committee, när jag ser att 47 miljarder dollar om året av våra skattepengar går till Pentagons IT-system, vill jag vara fullständigt säker på att när det gäller vår förmåga att hantera underrättelsetjänst utomlands, att ha informationsdominans utomlands, att kunna använda de slags verktyg som CIA och Försvarsdepartementet behöver i relationer med motståndare, att vi verkligen åstadkommer det genom den hör nya policyn. (...)

Och jag tycker att vi bör höra med CIA och NSA direkt, eftersom de är folket när det gäller att kunna bryta sig in i utländska motståndares system, både verkliga och potentiella motståndare."

När svenska riksdagen upptäckte krypteringsförsvagningen i Lotus Notes

År 1997 fick Sverige stor uppmärksamhet i världen när den svenska riksdagen upptäckte att det fanns något som liknade en bakdörr i Lotus Notes, ett program för e-post och annan kommunikation och dokumentutbyte. Vid den tiden användes Lotus Notes bl a av ett stort antal företag, riksdagens alla ledamöter, 15 000 anställda på Riksskatteverket och många svenska militära inrättningar. ”Jag visste inte om att våra Notesnycklar var deponerade, det var intressant att få reda på”, sa datasäkerhetschef Jan Karlsson vid Försvarshögkvarteret enligt en artikel i Svenska Dagbladet i november 1997.

Uppenbarligen levde köparna av Lotus Notes i tron att det program de skaffat använde sig av 64-bitars kryptering. Så var också fallet. Det var bara det att 24 av de 64 bitarna i nyckeln i hemlighet skickades med varje meddelande, i krypterad form så att bara amerikanska NSA kunde läsa ut dem. Det innebär att för NSA var krypteringen i praktiken bara 40-bitars, vilket gör den ungefär 16 miljoner gånger lättare att knäcka. Kraftfulla datorer som finns på storföretag och underrättelsetjänster kan knäcka 40-bitars kryptering på några sekunder eller minuter. Helt logiskt kallas de medskickade 24 bitarna i underrättelsevärlden för workfactor reduction field.

Lotus, ett dotterbolag till IBM, bekräftade krypteringsförsvagningen i exportversioner av Lotus Notes och sa att den var en följd av amerikanska exportrestriktioner. Man lovade dock att amerikanska myndigheter inte kommer att missbruka sina möjligheter. Det verkar inte som om alla i Sverige och övriga Europa känner sig lugnade av den försäkran. ”Handhar man känslig information som rör Sveriges intressen ska man inte lämna krypteringsnyckel till vare sig den amerikanska regeringen eller någon annan. Det måste vara grundinställningen”, sa dåvarande riksdagsdirektören Gunnar Grenfors i den tidigare citerade artikeln i Svenska Dagbladet.

Bakdörr i Windows?

År 1999 upptäcktes av en händelse något intressant i en säkerhetsuppdatering till operativsystemet Windows, närmare bestämt i Windows NT4 Service Pack 5. En kanaden-

sisk datasäkerhetsoch kryptologiexpert, Andrew Fernandes på företaget Cryptonym, hittade då en tidigare okänd extra ”nyckel” till Microsofts operativsystem Windows. Nyckeln, som man uppenbarligen glömt bort att dölja i uppdateringen, bar i klartext namnet NSA-KEY (på vissa ställen anges istället NSA_KEY).

Den som är i besittning av en sådan nyckel kan på distans via Internet införa ändringar i operativsystemet Windows utan datorägarens godkännande eller ens vetskap. Nyckelägaren kan också installera tilläggsprogram på datorn, likaså utan datorägarens vetskap. Därmed blir det också tekniskt möjligt för nyckelägaren att distansövervaka vad som görs på datorer försedda med Windows, och att hämta data från dessa. Vidare kan eventuella krypteringsprogram som användaren införskaffar från tredje part sättas ur spel av den som har denna nyckel.

Före avslöjandet trodde man att bara en (1) sådan nyckel fanns till Windows – den nyckel som Microsoft har för att kunna installera säkerhetsuppdateringar hos Windowsanvändare. Varför fanns det en nyckel till, och varför bar den namnet NSA-KEY? Andrew Fernandes hävdade att nyckeln är en bakdörr som medvetet byggts in i Windowsversionerna 95, 98, NT och 2000 för att ge amerikanska NSA full insyn i världens alla Windows-försedda datorer.

Enligt Microsoft är detta ”fullständigt fel”. Man hävdar bestämt att nyckeln ifråga är en Microsoft-nyckel, den delas inte med någon annan part, inte heller NSA. Namnet NSA-KEY var olyckligt valt, men förkortningen NSA syftar bara på att nyckeln uppfyller NSA:s kryptografiska krav på produkter med exportlicens, enligt Microsoft.

Enligt nyhetstjänsten Techweb säger Microsoft att nyckeln är en backup för den nyckel som normalt används av Microsoft, en back-up som skulle kunna behövas exempelvis i händelse av en naturkatastrof. Detta kommenteras av Gaaspar Bowden på den London-baserade organisationen Foundation for Information Policy Research (FIPR) på detta vis: ”Att bygga in en back-up-nyckel tjänar inget syfte om det inte finns någon metod för att återkalla den primära nyckeln. Det finns ingen återkallandemetod.”

En annan kommentar kommer från Simon Davies, generaldirektör på medborgarrättsorganisationen Privacy International. Han säger på Techwebs webbplats:

> *”Jag tror dem inte – vad är det för naturkatastrof de talar om? En meteor som förstör allting på jorden? Microsofts argument stämmer inte överens med deras arbetsrutiner – de skulle kunna förvara en enda nyckel på flera platser, det är en normal säkerhetsåtgärd.”*

År 2000 dök liknande uppgifter upp igen, den här gången i den franska nyhetstjänsten för underrättelsebranschen, Le Monde du Renseignement (Intelligence Online). De rapporterade att ett hemligstämplat dokument från underrättelsegrenen av det franska försvarsdepartementet, DAS, uppger att Microsoft utvecklar programvara som gör det möjligt för NSA att utföra internationell övervakning. Microsoft avfärdade uppgifterna som helt ogrundade.

En indikation som stöder antagandet om att det verkligen existerar ett nära samarbete mellan amerikanska exportföretag och amerikansk underrättelsetjänst är den omskrivna skandalen kring Kinas köp av tjänsteflygplan åt sin president år 2000. När planet, av typen Boeing 767, levererades upptäcktes mer än 20 dolda mikrofoner som kunde fjärrstyras från en satellit.

Öppen källkod enda garantin mot bakdörrar

Det bör noteras att bakdörrar kan ta sig många uttryck, och att de inte behöver vara uppenbara och vidöppna. Ofta kan de se ut som misstag begångna av programmerarna, om de skulle upptäckas. Metoder som kan användas, enligt säkerhetsexperter, är exempelvis att se till att en slumptalsgenerator inte är riktigt slumpmässig, eller att ”råka” skicka med en del av den hemliga nyckeln i utsända meddelanden.

Det enda riktigt säkra sättet att förvissa sig om att en programvara inte innehåller några bakdörrar anses vara att i detalj granska källkoden (dvs den programvarukod som skrivits i något programmeringsspråk före den s k kompileringen till maskinkod, ettor och nollor). Detta har gjort att intresset bland säkerhetsmedvetna kunder för s k ”open source”-programvara (dvs programvaror med källkoden publicerad på Internet) har ökat.

Denna utveckling sätter även tryck på traditionella mjukvaruhus. Bland annat tillkännagav Microsoft, länge en hårdnackad motståndare till öppen källkod, i början av 2003 ett program (Government Security Program) enligt vilket länders regeringar kan ingå ett avtal som ger dem möjlighet att se (men inte ändra) källkoden till Windows. Ryssland ingick tidigt ett sådant avtal med Microsoft, och ett 20-tal andra regeringar lär ligga i förhandlingar.

Innebär denna nya öppenhet från Microsofts sida att vi kan vara säkra på att ingen bakdörr i Windows existerar? Det är inte självklart. Enligt Government Security Program får regeringarna se källkoden men inte själv ”kompilera” den till användbar programvara, vilket rimligtvis betyder att en annan källlod än den granskade ligger till grund för de Windows-program som verkligen installeras på datorer. Granskning av källkod fungerar bara som säkerhetsgaranti om man också behärskar hela kedjan fram till färdig programvara.

En viktig slutsats av ovanstående resonemang är att teknologier som hanterar information – åtminstone i en del fall – är av strategisk karaktär. Man kan få intrycket att politiker och andra beslutsfattare i Sverige och övriga Europa inte fullt ut har förstått vikten av att behärska, inte bara köpa in, informationsteknologi. Information har blivit så fundamental på alla plan i vårt samhälle att IT inte kan avfärdas som något man upphandlar där det för dagen är billigast. I varje fall inte alla sorters IT. Den som behärskar världens IT-mässiga infrastruktur har ett kraftfullt maktredskap i sin hand. Mycket kraftfullt.