Signalspanarna får viktiga roller på det elektroniska slagfältet

Signaljägaren utför sina bragder i det tysta

Syftet med militär signalspaning är att ge underlag för chefers beslut och att skapa informationsövertag för den egna sidan, skydda sina förband och neutralisera motståndarens vapen och verkansmöjligheter. Ytterst handlar det om att kunna använda sina resurser på det mest fördelaktiga sättet – genom kunskap om motståndaren, hans stridskrafter och avsikter. Perspektivet kan vara strategiskt, operativt eller taktiskt, det kan gälla långsiktig planering lika väl som duellsituationer på slagfältet.

Elektroniskt slagfält behöver spanare

Signalspaning är en otacksam disciplin av flera anledningar: Sekretessen hindrar god information utanför fackkretsen. Signalspaning syns inte, den ger varken ifrån sig vågskvalp eller ljudbangar. Den vinner inga snabba segrar i konventionella krigsspel eller på en krigsförbandsövning i Norrland. Efter verkliga krig förtigs den gärna i decennier. Signalspanarna själva vill hålla sina metoder hemliga och vilken historisk fältherre har velat vidgå att han hade signalspaningen att tacka för att han vann det stora slaget? På hemmaplan ser vi dock ett nytänkande i flera avseenden. Försvarsmaktsinrikning 2020 betonar underrättelsernas betydelse på framtidens elektroniska slagfält. För Jas prioriteras goda varnare och telemotmedel nu, och inte som något man kan hänga på i framtiden.

Militär signalspaning syns förvisso också mindre i fred än i krig. Möjligheterna är begränsade och resultaten mindre spektakulära. Men den teletekniska utvecklingen går med rasande fart och allt större informationsmängder till allt fler rörliga mottagare krävs för framtidens krig, liksom sofistikerade elektroniska medel för målinmätning och vapeninsatser. Detta talar entydigt till signalspaningens fortsatta och framtida nödvändighet.

Jan-Olof Grahn
är chef för avdelningen för militära underrättelser vid Försvarets radioanstalt, FRA

Signalspaningens huvudområden

I Sverige skiljer vi mellan kommunikationsspaning, *KOS*, och teknisk signalspaning, *TES*. Lite tillspetsat kan man säga att KOS i militära sammanhang används för att skapa bästa möjliga förutsättningar för striden – och TES för att vinna de enskilda duellerna när slaget väl börjat.

KOS riktar sig mot sådana radiosignaler som bär ett verbalt kommunikationsinnehåll mellan sändare och mottagare, dvs telefoni, telegrafi, fjärrskrift eller dataöverföring. KOS kan nedbrytas i *inhämtning, trafikbearbetning samt kryptoforcering*.

- Inhämtning av långvariga sändningar kan ske på klassiskt sätt, genom att en radiooperatör vrider på sin radiomottagare tills han eller hon hör något som erfarenhetsmässigt är intressant. Kortvariga eller komprimerade sändningar kräver automatiska spaningssystem som endera är bredbandiga eller snabbt scannar sig igenom stora frekvensområden.
- Trafikbearbetningen bringar ordning i det skenbara kaos som det inhämtade materialet erbjuder. Vem kommunicerar med vem och varför? De uppfångade radiosignalerna lägesbestäms och identifieras. Motståndarens organisation och stridsindelning klarläggs inklusive förbandens sammansättning, uppgifter och förmåga, gruppering och verksamhet, beredskap och avsikter. Slutligen ska trafikbearbetningen hjälpa inhämtningen med spaningsunderlättande hjälpmedel av skilda slag.

Lägesbestämning sker främst genom pejl, vilket för god precision kräver flera avlyssningsplatser lämpligt placerade i förhållande till den pejlade sändaren.

Identifiering av radiosändningar kan ske på ett antal av varandra oberoende sätt, som är avhängiga målet för uppmärksamheten. Anropssignaler, frekvensanvändning och trafikprocedur kan identifiera sambandscentralen, analys av signalernas modulation kan identifiera radiosändaren, analys av röst eller personlig stil kan identifiera sambandspersonalen och analys av själva meddelandena kan identifiera korrespondenten, dvs användaren av radiostationen.

Från fortlöpande identifiering av enskilda radiostationer kan bearbetningen rulla upp den bakomliggande signalorganisationen. Och eftersom denna oftast speglar den verkliga organisationen, har man därmed bestämt densamma. Motståndarens stridsindelning kan klargöras och från densamma kan information utläsas om vilka styrkor man har att göra med och var de är grupperade.

Från identitet och organisation är steget nära till verksamhet, förmåga och avsikter som de iakttagna förbanden uppvisar. Detta kan direkt eller indirekt framgå av den signalering som utväxlas, även utan forcering av kryptot. Direkt om det klart sägs ut, indirekt om man kan bygga upp indiciekedjor av olika slag genom att vissa verksamheter är kopplade till vissa uppträdanden.

- Att läsa motståndarens order och rapporter är naturligtvis det yttersta målet för signalspaningen. För att skydda sig mot detta har krypteringstekniken utvecklats snabbt, särskilt under senare år. Från användning av koder (en kodgrupp betyder en bokstav, ett ord eller en fras) och enkla chiffer (ett tecken ersätts normalt med ett annat), via meka-

niska chiffermaskiner över elektromekaniska till fullt elektroniska kryptoapparater och olika former av mjukvarukrypton för bruk i datorer. Kryptoforceringen har på motsvarande vis utvecklats och blivit alltmer datorstödd. De aktuella maskinerna eller algoritmerna kan därmed simuleras i datorer för att generera läsbar klartext när väl de beräkningsintensiva forceringsprogrammen rekonstruerat aktuella nyckelinställningar.

Kunskap om kryptoforcering är också en nödvändig förutsättning för att kunna konstruera goda egna krypton. Därför går dessa två discipliner helst hand i hand.

Teknisk signalspaning ,TES, riktar sig huvudsakligen mot signaler med andra syften än samband, främst radar och navigeringssystem. Teknisk signalspaning kan delas upp i operativa/taktiska respektive tekniska komponenter.

Operativ/taktisk TES syftar till att följa motståndarens rörelser och därigenom stödja den egna yt- och luftlägesbilden. Grunden är att olika signaler är kopplade till sina respektive plattformar. Har man hört en viss signal kan man ofta typbestämma målet och vet därmed vilket flygplan eller fartyg man har att göra med.

I sin enklaste form används sådant underlag i form av varnare som talar om för flygförare eller stridsledning på fartyg att ett visst hot har dykt upp inom det egna operationsområdet. Hotet kan vara en inkommande robot som omedelbart måste neutraliseras eller ett potentiellt mål för de egna vapensystemen.

Teknisk TES har som huvuduppgift att analysera de strålande delarna av motståndarens vapensystem och därmed lämna underlag för att bedöma deras prestanda och kunna anpassa egna vapen, motmedel eller taktik för att vinna dueller mot desamma. Teknisk TES lägger grunden för överlevnad på slagfältet.

Nära släktingar till signalspaning

Varje militär chef kräver ett bra beslutsunderlag för att lösa sin uppgift och för att skydda sitt förband. Taktisk signalspaning kan bidra till båda, men här finns en inneboende konflikt med sekretesskravet. Känslig signalspaningsinformation kan inte föras ut i stridslinjen på grund av risken att motståndare kommer över den. En lösning har varit att bryta ut mindre känsliga signalspaningsdelar för att direkt stödja stridande förband. I det sammanhanget tillkom begreppet *telekrigföring* (Electronic Warfare) som i Sverige tenderar att fokusera vid aktiva åtgärder som störning. Det är inte i samma utsträckning fallet i utlandet.

På liknande sätt kan begrepp som *ledningskrigföring och informationskrigföring*, vilka infördes under och efter Gulfkriget, ses som nya grenar på ett gemensamt träd. Många aspekter av dessa aktiviteter – t ex fysisk bekämpning – är mindre känsliga än signalspaning men samlingsbegreppen har blivit lystringsord. Detta hindrar inte att sekretessomgärdade signalspaningsmetoder och dito medel är avgörande för framgång.

- Telekrigföring (tyngdpunkt på TES) och televapen (tyngdpunkt på KOS) kan användas nära den taktiske chefen och under direkt kontroll av honom. I det första begreppet (eller snarare dess anglosaxiska motsvarighet Electronic Warfare) ligger alla aspekter av elektroniska dueller, i det senare självskydd och lokala beslutsunderlag – något som blivit ett viktig inslag i de senaste årens internationella insatser.
- Ledningskrigföring handlar om att med aktiva snarare än passiva metoder utnyttja, vilseleda eller förstöra motståndarens ledningssystem, något som givetvis förutsätter kunskap om desamma genom signalspaning för att kunna utföras. Informationskrigföring är ett än vidare begrepp för tillämpad signalspaning, och som inkluderar aktiv kommunikation med motståndarens datorer. ■

Churchills samtal med Roosevelt över Atlantkabeln knäcktes direkt av tyska experter

Organiserad radiospaning förekom redan före första världskriget, men det var först med kriget som den fullt ut skulle etableras hos samtliga deltagande parter. Tyskarna vann spektakulära framgångar genom sin systematiska avlyssning av rysk radiotrafik samt forcering av de koder som där användes. Den brittiska lösningen av det famösa Zimmermanntelegrammet 1917 bidrog starkt till USAs inträde i kriget kort därefter.

Under andra världskriget genomgick såväl de krigförande ländernas signalspaning som vår egen en våldsam expansion och utveckling. Lösningen av den tyska Enigma-maskinen hemlighölls nästan 30 år efter krigsslutet, men kom till allmänhetens kännedom 1974. Denna insyn i den tyska krigsmakten blev av avgörande betydelse på flera fronter och förkortade sannolikt kriget med flera år.

Andra framgångar för de allierade har kommit i skuggan av detta, men även mot Japan noterades goda resultat, såväl mot strategiska som taktiska kryptosystem. Tyskarna löste det första talkryptot som användes för Churchills samtal med Roosevelt över atlantkabeln – några timmar efter respektive samtal låg utskrift av dem på Hitlers bord.

För Sveriges del gav Arne Beurlings lösning av det tyska teleprinterchiffret för trafiken mellan Berlin och Norge en unik insyn i tyskarnas högsta ledning. Härigenom fick Sverige exempelvis förvarning om det tyska angreppet på Sovjetunionen i juni 1941. Regeringen kunde också fortlöpande inifrån läsa av de svensk-tyska relationerna, vilket gav den ett diplomatiskt trumfkort under de år vår neutralitetspolitik sattes på sina svåraste prov.

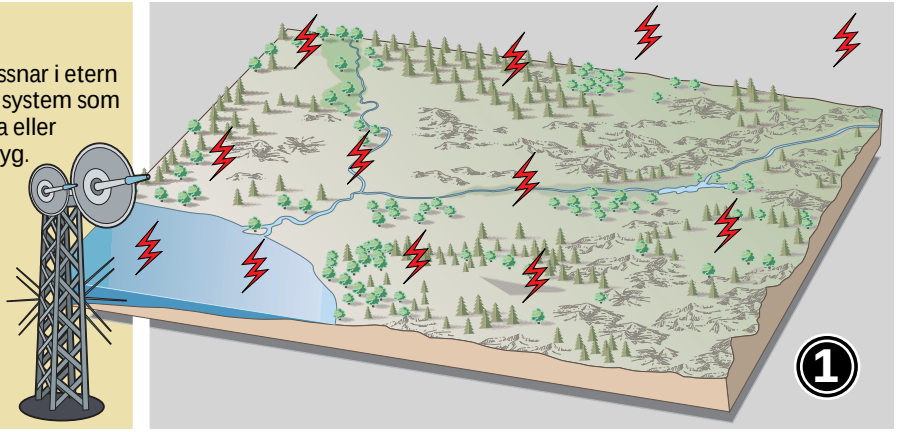
Efter andra världskriget har det varit relativt tyst om signalspaning. Men ett belysande tecken kanske är att de stora ländernas signalspaningsorganisationer gradvis växte till sig under det kalla kriget, och det är en rimlig gissning att den faktiska kapaciteten utvecklats än snabbare genom den ökade automatisering som blivit möjlig genom modern datateknik. Enligt öppna källor lär amerikanska National Security Agency omfatta över 20 000 man, en siffra som kan svälla till det dubbla om man räknar för NSA tjänstgörande militär personal och entrepenörer.

Från signal till underrättelse

Signalspaning syns inte. Den ger varken ifrån sig ljudbangar eller mullrande bogvågor. Ingen fältherre tackar signalspanarna för segern. Dessa bragder i det tysta kan förbli okända i decennier. På senare tid har dock insikten om signalspanarnas betydelse ökat. De kan fälla avgörandet på det framtida elektroniska slagfältet. Ett exempel på hur svenska signalspanare arbetar framgår av denna grafik.

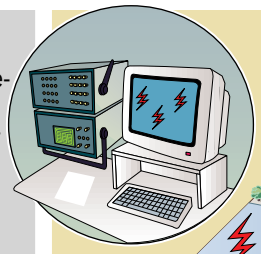
Inhämtning

Inhämtaren kan vara en radiooperatör som lyssnar i etern med hjälp av sin mottagare eller automatiska system som söker efter särskilda signaler, exempelvis korta eller komprimerade sådana. Pejl är ett viktigt verktyg.

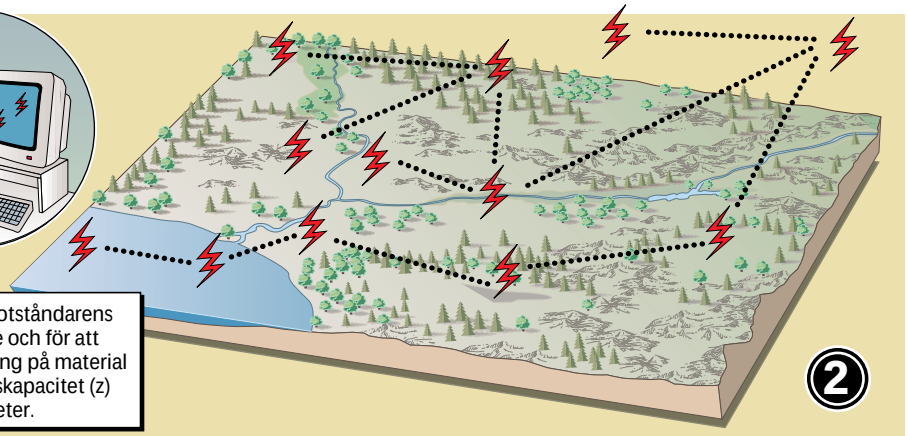


Bearbetning

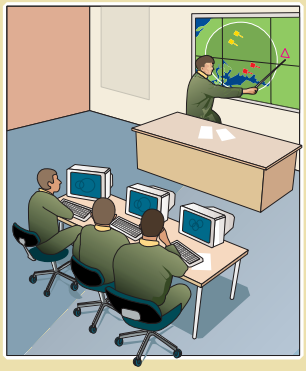
Med hjälp av avancerade metoder kringgås signalskydet och de olika sändarnas identitet klaras ut. Nu framträder signalorganisationen som speglar den militära organisationen med dess lydnadsförhållanden.



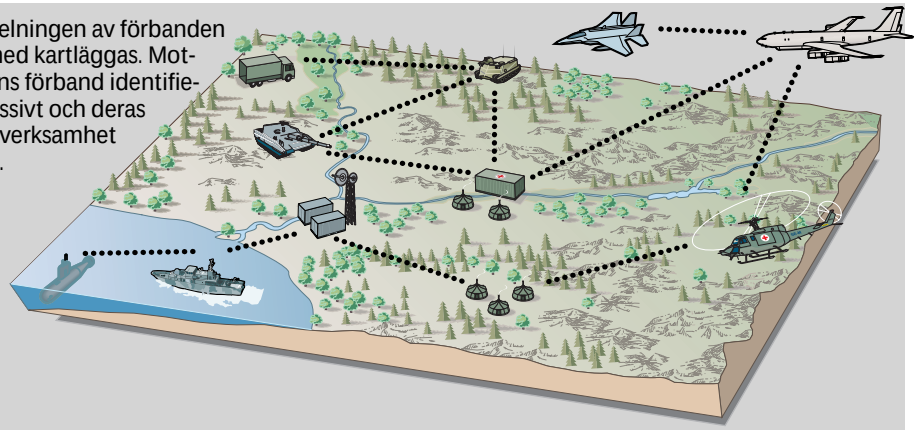
Signalspanarens finaste skalp är att direkt läsa motståndarens order och rapporter. Dessa är normalt krypterade och för att komma åt dem krävs att kryptona forceras. Tillgång på material (x) forceringskompetens (y) samt databeräkningskapacitet (z) är det som bestämmer radiospaningens möjligheter.



Bilden klarnar



Stridsindelningen av förbanden kan därmed kartläggas. Motståndarens förband identifieras successivt och deras läge och verksamhet klarläggs.



Hot/avsikt

När pusselbitarna successivt läggs ut ger den vidare analysen underrättelser om motståndarens förmåga och avsikter, t ex kraftsamlingsriktning. Detta kan gälla ett begränsat frontavsnitt eller en hel operationsriktning. Mycket hänger på analytikerns kunskaper och skarpsinne.

Snabbt växande globala nätverk förändrar signalspaningens tyngdpunkt

Bredbandsanalys av kommunikationsflöden kan bli ny uppgift för signalspanare

Foto: BJÖRN TÅNG, Telemuseum

Kapaciteten att överföra data ökar med en faktor tusen bara på tio år. En stor del av informationen går i IT-världens artärer, de fiberoptiska kablarna. Ett IT-angrepp mot Sverige kommer förmodligen i en sådan här kabel.

Precis som alla andra delar av totalförsvaret påverkas förstås signalspaningen av förändringarna i vår omvärld – i hotbilden och i tekniken. När det gäller signalspaning talar man i den internationella diskussionen främst om två betydelsefulla faktorer.

- En av dessa faktorer är förändrade underrättelsebehov. Offentliggjorda uppgifter ger en bild av att västvärldens signalspaningsorganisationer mindre fokuseras på sådana militära mål som dominerade under det kalla krigets dagar. I stället ägnar man sig relativt sett mer åt kris- och oroshärdar av andra slag världen över. Det för med sig många nyheter – intresset gäller andra geografiska områden, andra språkområden, annan kultur. Aktörerna behöver inte längre vara stater – de kan vara transnationella, t ex terroristorganisationer, drogsmuggling och storskalig ekonomisk brottslighet.
- Den andra stora faktorn är den oerhörda utvecklingen av tekniken. Världens telekommunikationer utvecklas snabbare för varje år. Den tillgängliga totala kapaciteten att överföra data – av alla slag – beräknas t ex öka med en faktor 1000 på drygt 10 år! Samtidigt blir utrustningen allt billigare, och allt mer tillgänglig både för stater och för andra. Framtidens signalspaning måste inriktas på att behärska de svårigheter som väntar, men också på att utnyttja de möjligheter som uppstår. Det är ett omfattande arbete, som redan pågår världen över.

Alltihop blir IT

Gränserna mellan olika slag av elektronik - datorer, TV, telefon, radio, radar osv – får allt mindre betydelse. Alltihop blir IT, informationsteknik. Drivande bakom utvecklingen är numera den civila sektorn snarare än den militära. Därmed blir också utvecklingen av civil IT styrande för militär IT. De militära systemen kommer därför i allt högre grad att överensstämma med de civila.

Hans Rehnvall
är informationsdirektör vid FOA och ansvarig utgivare för FOA-tidningen

Det gör att man kan förutse att civil utrustning och civila system i allt större grad kommer att användas i militära sammanhang. Det i sin tur leder till att gränsen mellan spaning mot civil och spaning mot militär kommunikation suddas ut. Med distribuerade databaser, dvs datornät där man från vilken punkt som helst kan hämta data från andra datorer i nätet – extremexemplet är förstås Internet – blir också gränsen mellan lagrade och kommunicerade data otydligare.

Trots att säkerhetslösningar med kryptering, brandväggar m m blir allt vanligare, så innebär själva takten i utvecklingen av nya produkter och versioner att det blir svårt att hålla systemen buggfria och täta mot signalspaning.

Klassisk signalspaning har varit baserad på lyssnande i etern. Etern har betraktats som fri, och allt som sänts ut i den som åtkomligt för spaning. En stark teknisk utveckling äger rum även för etermedia, men andra tekniker börjar få större betydelse. Dagens, och framtidens, viktigaste förbindelser, vid sidan av kommunikationssatelliterna, är de optiska kablarna. Med globala nätverk där optiska kablar får allt större betydelse förändras signalspaningens tyngdpunkt.

De flesta länder har regelverk som gör det möjligt för polisen att avlyssna enskilda teleadresser i landet. Reglerna innebär ett juridiskt förfarande, t ex godkännande av en domstol, och avser normalt en bestämd person eller ett bestämt telefonnummer. In-

kopplingen görs nära abonnenten. Dessa regelverk förändras nu utomlands för att medge teleavlyssning i en ny signalmiljö. Man kan t ex ”filtrera” fram uppgifter av ett bestämt slag, eller riktade mot en bestämt mottagare, ur ett stort dataflöde – som i ett knippe optiska kablar – i stället för att koppla in sig intill abonnenten.

Aktiv signalspaning

Signalspaning har traditionellt inneburit passivt lyssnande. Aktiv signalspaning är ett begrepp som används för att beteckna aktiva åtgärder för att möjliggöra signalspaning. Det kan tex innebära ”hacking” för att sätta krypteringen ur spel, för att tränga igenom en brandvägg eller för att styra ut datafiler på kommunikationsnät.

Aktiv signalspaning är ett område där arbete pågår i flera länder. Även i Sverige måste vi därför ta det på allvar, också från skyddssynpunkt. Hacking är ett hot både i civila och militära sammanhang. Hur stora dimensioner illasinnad, eller direkt kriminell, hacking redan har är svårt att bedöma – mycket tyder på att mörkertalet är mycket stort. En del i ett systematiskt skyddsarbete vore att ge signalspaningen ytterligare en uppgift, nämligen att upptäcka denna typ av attacker genom att bredbandigt analysera kommunikationsflödena.

Säkerhet och integritet

Signalspaningen kommer i framtiden att ha en vital betydelse för rättsvårdande myndigheter, för militären, för alla de underrättelse- och säkerhetstjänster som ska möta olika former av militära och icke-militära hot. Detta innebär en grannlaga avvägning mellan säkerhetsintressen å ena sidan och personlig integritet å den andra.

I demokratiska länder har man – eller söker man – lösningar som innebär att det finns en fristående och effektiv kontroll av underrättelsetjänsten. Samtidigt skärps tillämpningen i tillståndsgivningen så att den gäller precist avgränsade mål. För signalspaningen innebär det att allt som inte är uttryckligen tillåtet kastas – i huvudsak med automatik. Kopplat till detta vidgar man möjligheten till spaning mot breda informationsflöden, t ex för att upptäcka IT-angrepp eller rulla upp internationella terroristorganisationer. ■

Strävan att dölja visar vad som är intressant

Signalspanare ser vad motparten vill gömma

Johan Tunberger
är direktör vid Försvarets radioanstalt, FRA och var tidigare ledare för FOAs Teslagrupp

Signalspaning – många vet att den existerar, men bara invigda invigda vet vad det är. Samtidigt är signalspaningen, i Sverige representerad av Försvarets radioanstalt, den resursmässigt och personellt största grenen av underrättelsetjänsten i mer avancerade länder. Spänningen mellan storlek och slutenhet har medfört att signalspaning omges av en viss mystisk aura – och en mängd, oftast konspiratoriska gissningar som skjuter över, under och vid sidan av målet.

Signalspaning lever på en enda källa

Om agentverksamhet finns en uppsjö av böcker och filmer. I fråga om signalspaning händer det att historiska fakta kommer fram med 40–50 års fördröjning, men ”007or” saknas. Ett sent undantag från denna huvudregel är actionfilmen *Enemy of the State*, som skildrar amerikanska National Security Agency som en ondsint Big Brother med den samlade underrättelsetjänstens alla resurser till sitt förfogande – och en sagolik prylgarderob därutöver. Redan där blev det fel. Seriös signalspaning utmärks av att den är *single source*; det är uteslutande signaler som utgör råvaran i signalspaningskedjan – inhämtning, bearbetning och rapportering av underrättelser. I demokratiska stater finns därtill strikta regelverk och mekanismer för kontroll som sätter gränserna för vad signalspaningsorganisationerna får och inte får göra.

Öppna källor som nålen i höstacken

Vi talar i dag om informationsexplosionen. Sant är att det är alltmer möjligt att vaska fram underrättelser – beslutsrelevant information – genom öppna källor. Det kan dock vara som att leta efter nålen i höstacken. Och det är ofta svårt att avgöra vad som är korrekt information eller vad som är avsiktlig eller oavsiktlig desinformation.

Strävan att dölja viktig indikation

Fortfarande gäller att underrättelsemässigt intressanta aktörer oftast vill dölja vissa förhållanden och aktiviteter. Strävan att dölja är i själva verket en viktig indikation på att underrättelser finns att hämta. Det kan gälla fullt legitim, självklar militär sekretess; vem vill tex publicera data som gör det möjligt för en motståndare att förblinda ens egna radarsystem? Strävan att dölja eller vilseleda tenderar att öka ju mer sinistra avsikter en aktör har – det kan gälla en stat, en drogkartell eller andra som hotar grannstater eller egna befolkningsgrupper, en internationell säkerhetsordning och, ytterst, det samhälle och de värden vi vill värna.

Signalspaningens unika egenskap är att den kan avläsa vad en aktör reellt har för sig när han tror sig vara skyddad för motpartens insyn. I den flod av information som väller över oss kan det alltså vara vitalt att genom signalspaning kunna skåda in i hästens mun för att avläsa tex säkerhetshotande aktörers faktiska åtgärder eller egna uppfattningar om sin förmåga, sina planer och avsikter. Inte minst gäller detta i kris- eller spänningslägen då den allmänt tillgängliga informationen tryter och mängden desinformation ökar.

Hur långt FRAs förmåga sträcker sig och vilka metoder som används är och måste förbli förborgat – utan sträng sekretess skulle källorna sina. ■