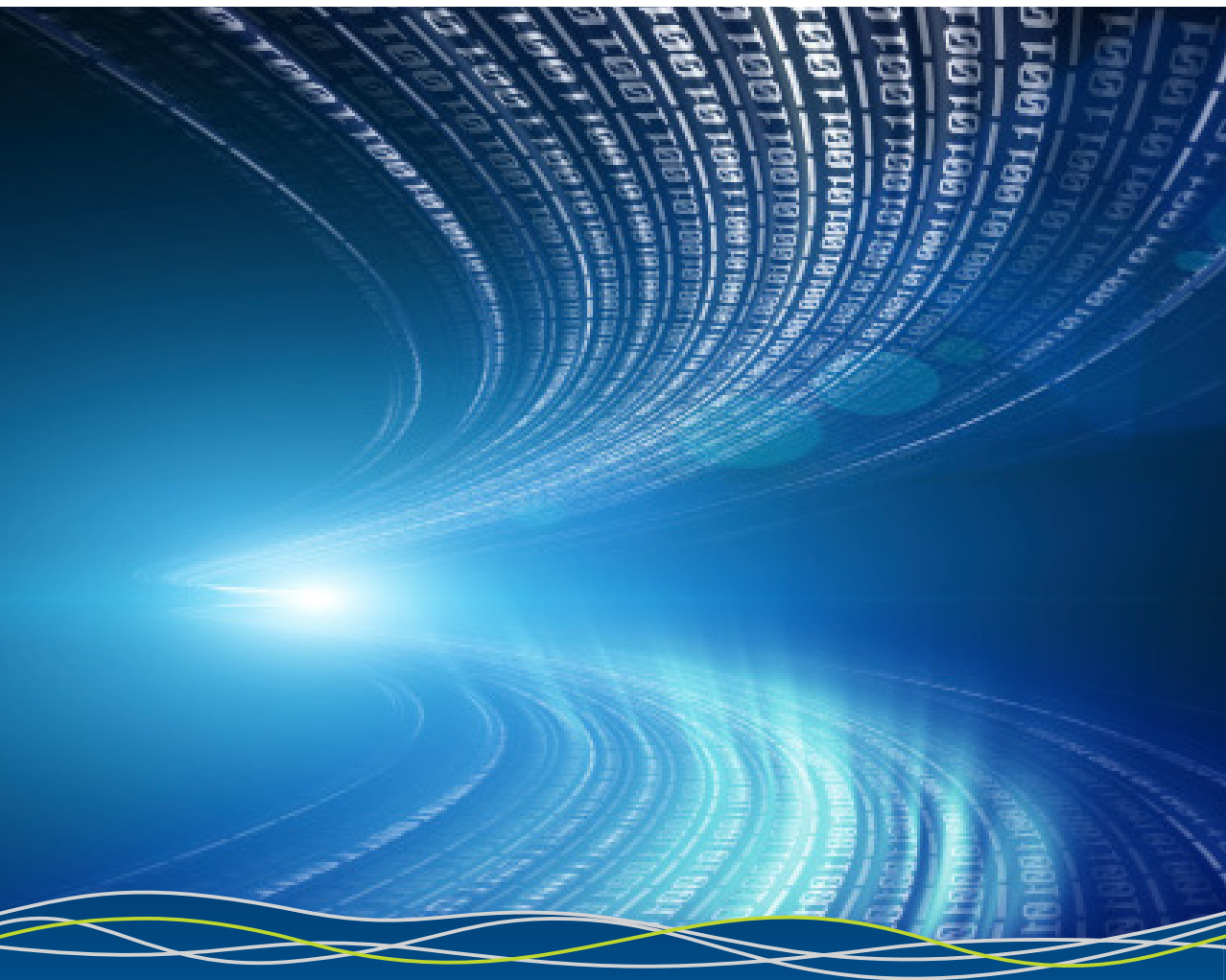


# Årsrapport 2012



FRA 70 år

# Generaldirektörens förord

Den 1 juli 2012 var det 70 år sedan vår myndighet bildades och vår verksamhet i dess nuvarande form inleddes. Vi vill därför, i samband med denna årsrapport, reflektera över vår verksamhet i går, i dag och i morgon.

När vår myndighet skapades pågick ett världskrig och den svenska regeringens målsättning var att hålla Sverige utanför kriget. Tack vare att matematikern och kryptologen Arne Beurling knäckte det viktiga tyska strategiska kryptot kunde regeringen få underrättelser om de tyska avsikterna i en tid då dessa behövdes som bäst. Tillgången till information som vi själva hade skaffat om vad som hände runt landets gränser hjälpte Sverige att hantera det svåra säkerhetspolitiska läget.

Under åren fram till i dag har det utrikes- och säkerhetspolitiska läget förändrats, men samma ambition har hela tiden gällt och gäller fortfarande för oss – att leverera underrättelser som bygger på en egen självständig inhämtning till våra uppdragsgivare till stöd för Sveriges utrikes-, säkerhets- och försvarspolitik. Därigenom bidrar såväl vi som de övriga försvarsunderrättelsemyndigheterna till Sveriges nationella integritet.

I denna årsrapport finns det en kort historik som beskriver viktiga punkter i vår historia. Det är en berättelse i tiden som sträcker sig från underrättelser mitt under brinnande världskrig, genom den tragiska händelsen med DC-3:an som

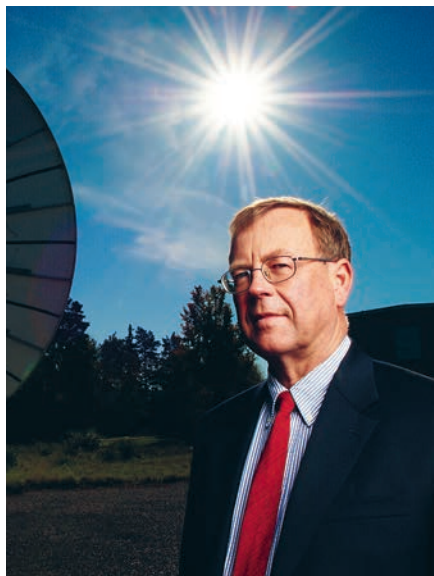


Foto: Johan Asp

sköts ner av sovjetiskt jaktflyg 1952, via de dramatiska skeendena under kalla kriget och in i dagens verklighet.

Denna verklighet präglas av företeelser som politisk oro och konflikter i områden av intresse för Sverige, alltmer avancerade IT-angrepp, internationell terrorism, högt tempo i den tekniska utvecklingen och Sveriges deltagande i internationella insatser.

Denna omvärld har varit vägledande i vårt arbete under 2012 när det gäller både underrättelseproduktionens viktigaste leveranser och det interna förändringsarbete som startades 2011 och som fortsatte under 2012.

Denna förändringsprocess, som bland annat innefattar ett kompetensväxlingsprogram och krav på ändrade arbetsmeto-

der inom underrättelseproduktionen, går ut på att bereda mark för de nya kompetenser som krävs för att möta morgondagens krav på en effektiv och ändamålsenlig underrättelse- och informationssäkerhetsorganisation.

Under det gångna året har utvecklingen av vår kabelinhämtning fortsatt och vårt stöd till Försvarmakten har utvecklats. På informationssäkerhetsområdet har myndigheten fortsatt att ge kvalificerat stöd till myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig i ett nationellt säkerhetsperspektiv. FRA har också hjälpt ett stort antal myndigheter och organisationer med säkra kommunikationslösningar.

Allvarliga IT-angrepp blir allt vanligare och de risker som detta för med sig för Sverige och svenska intressen blir allt tydligare. Vi har under året fortsatt arbetet med att anpassa organisationen för att på bästa sätt kunna stödja svenska myndigheter med att skydda känslig information. Dessa förändringar görs för att stärka vår samlade förmåga att möta den allvarliga utvecklingen inom området och för att tillsammans med andra myndigheter kunna bygga upp ett cyberförsvar för Sverige.

Trevlig läsning!

*Ingvar Åkesson,  
Generaldirektör, FRA*

## Innehåll

<b>Generaldirektörens förord</b>	<b>2</b>
<b>I går</b>	<b>4</b>
<b>I dag</b>	<b>8</b>
Organisation och verksamhet	8
Signalspaningsverksamhet	10
Informationssäkerhetsverksamhet och cyberförsvar	13
ÅR 2012	15
<b>I morgon</b>	<b>20</b>



Prov med teknisk signalspaning vid Torö 1948.

## I går

Mitt under andra världskriget, den 1 juli 1942, bildas den självständiga myndigheten Försvarsväsendets radioanstalt, sedermera Försvarets radioanstalt (FRA). Dessförinnan bedrevs verksamheten inom Försvarsstaben.

De viktigaste uppgifterna för signalspaningen under kriget är att förse den svenska regeringen med underrättelser om vilka planer de krigförande nationerna har och på så sätt stödja regeringens utrikes-, säkerhets- och försvarspolitik.

Tack vare matematikern Arne Beurlings insats med att lösa det strategiskt viktiga kryptosystem som Tyskland använder under kriget, den så kallade G-skrivaren,

kan signalspaningen under avgörande krigsår förse den svenska regeringen med betydelsefull information om tyska planer och avsikter för Nordeuropa under kriget.

Denna kunskap är oerhört värdefull i ett läge där osäkerheten är stor om Tysklands fortsatta krigsplanering och innebär mycket goda möjligheter att förvarna om ett eventuellt angrepp mot Sverige.

Andra världskriget tar slut och kalla



Foto: FRA



Foto: Tekniska museets arkiv

Trätorn för teknisk signalspaning 1948.

Den första svenskbbyggda datamaskinen Besk.

kriget tar vid. FRA blir en larmklocka för det svenska invasionsförsvaret med uppgift att förvarna regeringen och Försvarsmakten om läget skulle skärpas och behov av svensk beredskapshöjning skulle uppstå. Fokus blir på Östersjön och stormakter i närområdet.

Signalspaningen byggs ut med flygburen inhämtning. I samband med den tidiga utvecklingen av denna verksamhet skjuts en DC-3:a under ett signalspaningsuppdrag 1952 ner av sovjetiskt stridsflyg. Åtta personer finns ombord, varav fem från vår myndighet.

Att Sverige, genom FRA, bedriver underrättelseinhämtning genom signalspaning, särskilt från flygplan, är vid denna tid omgärdat av strängaste sekretess. Hanteringen av händelsen från såväl vår som andra aktörers sida leder till

decennier av hemlighållande som drabbar de anhöriga till de saknade besättningsmedlemmarna på ett sätt som vi har svårt att förlika oss med i dag.

Först 2003 hittas resterna av planet utanför Gotska Sandön och bärgas året därpå av Försvarsmakten. I dag finns en utställning på Flygvapenmuseet i Linköping med det som återstår av flygplanet och andra föremål som hittades på Östersjöns botten.

När den tekniska utvecklingen, som leder till dagens moderna datorer, tar fart under 1950-talet är våra medarbetare pionjärer i att utveckla de första maskinerna i Sverige för automatisk databehandling. År 1953 får FRA för första gången tillgång till datorkraft genom datorn Besk, vilket ökar vår förmåga att forcera krypterade meddelanden.

Det kalla kriget präglar vårt arbete.



Flygplanet Caravelle användes för signalspaning från 1970-talet till slutet av 1990-talet.

FRA:s signalspaning blir viktig för att följa Sovjetunionens ambitioner västerut. År 1956 lämnar vi underrättelser till den svenska regeringen om den dramatiska händelseutvecklingen i Ungern, då sovjetiska stridsvagnar rullar in i den ungerska huvudstaden för att slå ner upproret.

Under hela 1960-talet fortsätter vi att bevaka utvecklingen österut. Den viktiga funktionen av larmklocka vid planer på en förestående invasion är väletablerad och vi förser Sveriges regering kontinuerligt med uppgifter om läget i Sovjetunionen.

Under 1968 rapporterar FRA om trupp-sammandragningarna inför Warszawa-paktens inmarsch i Tjeckoslovakien som krossade den så kallade Pragvåren.

Under 1970-talet blir kommunikations-satelliter en central del i det internationella informationsutbytet. FRA utvecklar förmågan att inhämta satellitsignaler i takt med att behovet av underrättelser från uppdrags-givarnas sida ökar. De intressanta signalerna finns ännu huvudsakligen i militära radioförbindelser och andra kommu-

nikationskanaler som används specifikt av våra underrättelsemål.

Under 1980-talet ökar också efterfrågan på våra egna slutsatser kring det insamlade materialet allt mer. Detta resulterar i att vi anställer allt fler underrättelseanalytiker med kunskaper i exempelvis statsvetenskap och främmande språk – kunskaper som behövs för att sätta enskilda uppgifter i ett sammanhang i en underrättelserapport.

I och med 1990-talets ökande globalisering och de stora förändringarna i Öst-europa efter Berlin-murens fall 1989, som ledde till Sovjetunionens kollaps, inleds ett nytt kapitel i vår historia.

FRA följer händelserna i samband med upplösningen av Sovjetunionen och rapporterar bland annat om att stormningen av TV-tornet i Vilnius 1991 inte är ett spontant lokalt initiativ av de ryska trupperna på plats utan beordras av Moskva.

En viktig förändring är att Sverige nu deltar aktivt i internationella insatser, först i Bosnien och Kosovo och senare i Tchad, Afghanistan, Somalia och Libyen.

Detta ställer krav på FRA att utveckla sitt stöd till Försvarsmakten. Behovet av underrättelser från olika delar av världen där svensk trupp befinner sig eller dit eventuellt kan tänkas skickas ökar gradvis under 1990- och 2000-talen. Utbyggnaden av satellitkommunikationen går fort och satellittrafik står nu för en allt större del av vår inhämtning.

FRA har en lång erfarenhet av signalunderrättelseverksamhet riktad mot terrorism. Längre var denna verksamhet i huvudsak inriktad mot etablerade stater som understödde terroristverksamhet, men redan innan den 11 september 2001 inleds en omorientering mot organisationer som inte var direkt underställda något särskilt lands regering. Denna utveckling förstärks av naturliga skäl av händelserna i USA 2001.

Under 2000-talet flyttas alltmer av de internationella kommunikationerna från satelliter till fiberoptiska kablar. För att kunna fortsätta att leverera kvalificerade underrättelser till våra uppdragsgivare krävs en ny lagstiftning som gör det möjligt att inhämta den relevanta informationen oavsett den teknik som används.

Efter en lång politisk process och en omfattande medial diskussion stiftar riksdagen ett antal lagar, som både innebär en teknikneutral inhämtningsmöjlighet och som värnar den personliga integriteten. Lagarna innebär en omfattande reglering av vår signalspaning, med bland annat såväl tillståndshantering i domstol som extern kontroll och granskning.

Tidningsurklipp från den så kallade FRA-debatten.



# I dag

FRA är en civil myndighet under Försvarsdepartementet. Vi bidrar till att skydda Sverige och svenska intressen på två sätt: Vi ger våra uppdragsgivare unik information om viktiga utländska förhållanden genom att signalspana mot utländska företeelser till stöd för Sveriges utrikes-, säkerhets- och försvarspolitik. Vi arbetar för att stärka informationssäkerheten hos samhällsviktig verksamhet.

## Organisation och verksamhet

FRA är organiserat i fyra avdelningar: avdelningen för signalunderrättelser, avdelningen för informationssäkerhet, avdelningen för verksamhetsstöd och avdelningen för teknisk utveckling och

annat tekniskt stöd. Under 2012 inleddes ett arbete som syftar till att skapa goda förutsättningar för vår cyberverksamhet i dag och i framtiden. Detta arbete resulterade i beslut om att bilda en ny avdelning för cyberrelaterade frågor under 2013.

Utöver detta finns också ett ledningsstöd, som bland annat arbetar med verksamhetsplanering och informationsfrågor, samt ett antal specialistfunktioner, såsom till exempel en juridisk funktion och en säkerhetsfunktion.

Generaldirektören Ingvar Åkesson är myndighetschef. Överdirektör är Christina Malm.

Inom vår myndighet finns även ett integritetsskyddsråd med uppgift att fortlöpande följa de åtgärder som myndigheten vidtar för att säkerställa integritetsskyddet i signalspaningsverksamheten. Ledamöterna i rådet tillsätts av regeringen.







## Signalspaningsverksamhet

Signalspaningsverksamheten är en stor del av den svenska underrättelsetjänsten. Vår signalspaningsverksamhet syftar till att ge våra uppdragsgivare ett oberoende beslutsunderlag i frågor som rör svensk utrikes-, säkerhets-, och försvarspolitik.

Enligt en lagändring år 2012 får, förutom de tidigare uppdragsgivarna (regeringen, Regeringskansliet och Försvarsmakten), även Säkerhetspolisen och Rikskriminalpolisen från och med den 1 januari 2013 inrikta vår signalspaning.

All signalspaning sker på uppdrag av någon av dessa. All inhämtning kräver tillstånd av Försvarsunderrättelsedomstolen och är uteslutande riktad mot utländska förhållanden.

Det kan till exempel handla om

- Militär förmåga hos främmande länder
- Säkerhetsläget och aktörer i områden där det finns svensk trupp
- Läget vad avser mänskliga rättigheter i auktoritärt styrda länder
- Aktörer bakom IT-angrepp mot känsliga informationssystem
- Internationell terrorism
- Framställning och spridning av massförstörelsevapen

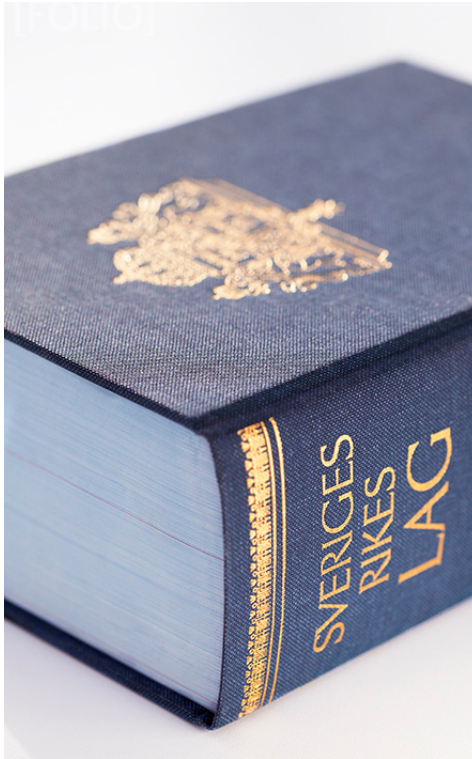
Signalspaningsverksamheten kan bestå antingen av spaning mot radarsignaler och signaler från navigeringsutrustning och vapensystem, eller av spaning mot civila

och militära signaler för kommunikation. Signalspaningen bedrivs i syfte att kartlägga de ändamål som anges i *ändamålskatalogen* i signalspaningslagen. Denna motsvarar i stort sett de områden som nämns ovan. Det är med andra ord dessa områden som är styrande för vår signalspaning.

Inom ramen för lagens ändamål ger regeringen FRA en årlig inriktning utifrån de underrättelsebehov som är aktuella. De övriga uppdragsgivarna kan sedan ge så kallade närmare inriktningar som är mer specifika. Dessa måste alltid rymmas inom ramen för regeringens inriktning.

Det är med utgångspunkt i regeringens årliga inriktning och de närmare inriktningarna som signalspaning kan genomföras.

All inhämtning vid signalspaning kräver tillstånd av Försvarsunderrättelsedomstolen. En tillståndsansökan innehåller bland annat en beskrivning av inhämtningsuppdraget och uppdragsgivarens underrättelsebehov samt vilka sökbegrepp eller kategorier av sökbegrepp som ska användas för uppdraget. Ansökan som rör kabelinhämtning ska dessutom ange vilka specifika



#### Ändamålskatalogen (2008:717)

1. yttre militära hot mot landet,
2. förutsättningar för svenskt deltagande i fredsfrämjande och humanitära internationella insatser eller hot mot säkerheten för svenska intressen vid genomförandet av sådana insatser,
3. strategiska förhållanden avseende internationell terrorism och annan grov gränsöverskridande brottslighet som kan hota väsentliga nationella intressen,
4. utveckling och spridning av massförstörelsevapen, krigsmateriel och produkter som avses i lagen (2000:1064) om kontroll av produkter med dubbla användningsområden och av tekniskt bistånd,
5. allvarliga yttre hot mot samhällets infrastrukturer,
6. konflikter utomlands med konsekvenser för internationell säkerhet,
7. främmande underrättelseverksamhet mot svenska intressen, eller
8. främmande makts agerande eller avsikter av väsentlig betydelse för svensk utrikes-, säkerhets- eller försvarspolitik.

signalbärare (fibrer i kabel) som uppdraget kräver.

Tillstånd kan ges för högst sex månader. Innan signalspaningen kan inledas kontrollerar Försvarsunderrättelsesdomstolen bland annat att uppdragsgivarens behov är i enlighet med ändamålen i lagen och att FRA:s inhämtning av eventuell integritetskänslig information står i proportion till behovet. Först därefter ges klartecken till FRA att inleda signalspaningen.

Resultatet av signalspaningen levereras till uppdragsgivarna och andra berörda myndigheter i form av underrättelse-rapporter. Rapporteringen utvärderas kontinuerligt och om rapporteringen ger

upphov till nya eller förändrade under-rättelsebehov formuleras en ny närmare inriktning av uppdragsgivaren. Statens inspektion för försvarsunderrättelseverksamheten (Siun) kontrollerar att vår signalspaning är i överensstämmelse med tillståndet och berörda författningar. Det är också Siun som ger oss den faktiska tillgången till trafik i kabel genom att koppla in de signalbärare som Försvarsunderrättelsesdomstolen beslutat att vi ska få tillgång till. En underrättelserapport skulle typiskt kunna innehålla formuleringar såsom:

*"Under perioden x mars till y april genomförde flygvapnet i landet X ett tiotal flygangrepp mot separatister i provinsen Z. Målområdet för insatserna var huvudsakligen gränsområdet mellan provinserna Z och W. Vid de flesta insatserna användes konventionella bomber, men vid två av angreppen bedöms klusterbomber ha använts och vid ett tillfälle precisionsstyrda vapen. Mycket få uppgifter om angreppen har förekommit i media."*

*"Ett stort antal viktiga datasystem inom såväl offentlig förvaltning som näringsliv i landet X är komprometterade genom systematiska dataintrång. Aktören bakom angreppen är sannolikt underrättelsetjänsten i land Y och syftet är att utvinna underrättelser. Områden som är värst drabbade är utrikesförvaltningen, försvaret och forskning och utveckling inom flyg- och rymdsektorn."*

*"Land X och land Y påbörjade under året ett omfattande underrättelse-samarbete. Personal från underrättelsetjänsten i Y har utbildats på kurser i X vid flera tillfällen. Samarbetet rör främst områdena terrorism, spionage och kontrapionage. Båda länderna är oroade över ambitionerna från land Z, och Y har dessutom en pågående gränskonflikt med Z."*

*"Under 2013 planerar raketforskningsinstitutet X i landet Z att öka personalstyrkan från 320 personer till 480 personer. Man planerar även inköp av utrustning för 210 miljoner dollar från landet Y. Ett problem uppges dock vara att få tag på tillräckligt kvalificerad personal, samt att man på grund av sanktionerna mot landet i många fall får vänta länge på beställd utrustning och materiel."*

Under 2012 har Siun utfört 15 granskningar hos oss. Inspektionsprotokollen ger sammantaget vid handen att vi bedrivit försvarsunderrättelseverksamhet inom ramen för regeringens inriktning, men innehåller också förslag på hur verksamheten kan förbättras i vissa avseenden.

Vi ser all kontroll och granskning som ett sätt att förbättra och utveckla verksamheten och implementerar löpande Siuns synpunkter och förslag i vår verksamhet på lämpligt sätt.



## Informationssäkerhetsverksamhet och cyberförsvar

Sverige behöver stärka informationssäkerheten inom samhällsviktig verksamhet på såväl administrativ som teknisk nivå. Antalet IT-angrepp ökar och de blir allt mer riktade och sofistikerade. Angriparna, som i allt högre grad är resursstarka och kunniga, har uttalade mål och syften med sina angrepp. Det kan till exempel handla om:

- Underrättelseinhämtning (statlig eller statsunderstödd)
- Ekonomisk brottslighet (elektronisk stöld)
- Industrispionage
- Sabotage/Förstörande angrepp

Vår myndighet har hög teknisk kompetens inom informationssäkerhetsområdet. Hos oss arbetar några av landets absolut skarpaste experter på området.

Experterna stödjer myndigheter och statligt ägda bolag inom området informationssäkerhet. Arbetet riktar in sig på verksamheter som hanterar information som är känslig i ett nationellt säkerhetsperspektiv.

Genom detta arbete bidrar vi till att stärka skyddet för samhällsviktig verksamhet. Konkret kan stödet handla till exempel om att testa en myndighets IT-system för att identifiera sårbarheter, att ge konkreta råd om hur informationssäkerheten kan förbättras och att förse myndigheter som hanterar känslig information med säkra kommunikationslösningar.

Verksamheten är utåtriktad och anpassad löpande till uppdragsgivarnas behov.



### **Synergier mellan signalspaning och informationssäkerhet**

Genom att utnyttja synergier mellan signalspaningsverksamheten och informations-säkerhetsverksamheten har vi en unik möjlighet att bidra till att Sveriges skydd mot avancerade IT-angrepp förstärks.

Via signalspaning följer vi angrepp och trender i det globala nätet. Vi kan se vilka angreppsmetoder som används, och kan också få en uppfattning om vilka länder som ligger bakom och varför. Denna kunskap kan vi använda i vårt informations-säkerhetsarbete för att stödja svenska myndigheter och statligt ägda bolag i Sverige.

Omvänt kan informationssäkerhets-experterna identifiera och analysera skadlig kod och se hur den fungerar, och med sina unika kunskaper bidra till förståelsen för hur angriparna verkar och agerar.

Under gynnsamma förhållanden kan ett angrepp spåras hela vägen mellan ett

antal olika länder som används som mellanstationer. På så sätt kan vi skapa oss en djupare förståelse för vad som sker och varför.

Tillsammans ger dessa kunskaper och förmågor en unik möjlighet för oss att, i nära samverkan med andra berörda myndigheter, bidra till uppbyggandet av ett svenskt cyberförsvar.

#### **FAKTARUTA**

Ett svenskt cyberförsvar syftar till att skydda landet och svenska intressen mot kvalificerade IT-relaterade hot och angrepp. Ett cyberförsvar utgörs av en kombination av förebyggande insatser, samverkan, samordning och operativa skyddsåtgärder.

FRA ska kunna verka inom hela detta område men ett nationellt cyberförsvar kan endast åstadkommas genom samordnade insatser från många olika myndigheter i Sverige.

# ÅR 2012

## Teknikneutral inhämtning

Vi rapporterar i dag underrättelser baserade på den teknikneutrala inhämtningen.

Kabelinhämtningen är etablerad inom signalspanningsverksamheten och bidrar till en höjd kvalitet i underrättelserapporteringen.

## Utvecklade former för samverkan med Försvarmakten

Vårt stöd till Försvarmakten består både av underrättelser om viktiga utländska förhållanden och av upprätthållandet och utvecklandet av det så kallade signalreferensbiblioteket (SRB), som Försvarmakten använder som underlag i de radarvarnare som finns i flygplan och på fartyg.

Vi ger också stöd till den yt- och luftlägesbevakning som Försvarmakten utför.

Under 2012 har vi utvecklat samarbetet med Försvarmakten på flera sätt. Nya samarbetsformer har skapat bättre förutsättningar för en effektivare samverkan både på central nivå och i konfliktområden, bland annat inom ramen för den pågående insatsen i Afghanistan. Vi har därmed bland annat snabbare kunnat producera och delge hotvarningar och annan tidskritisk rapportering till Försvarmakten under pågående operationer.

## Utveckling av cyberverksamheten

Antalet avancerade IT-angrepp och incidenter riktade mot samhällsviktig verksamhet i Sverige ökade i antal och i komplexitet under 2012. Vi har under året följt

ett stort antal angrepp globalt mellan andra länder, men också sett angrepp mot svenska mål. Det rör sig om svenska storföretag, universitet, högskolor och myndigheter varifrån känslig information förts ut.

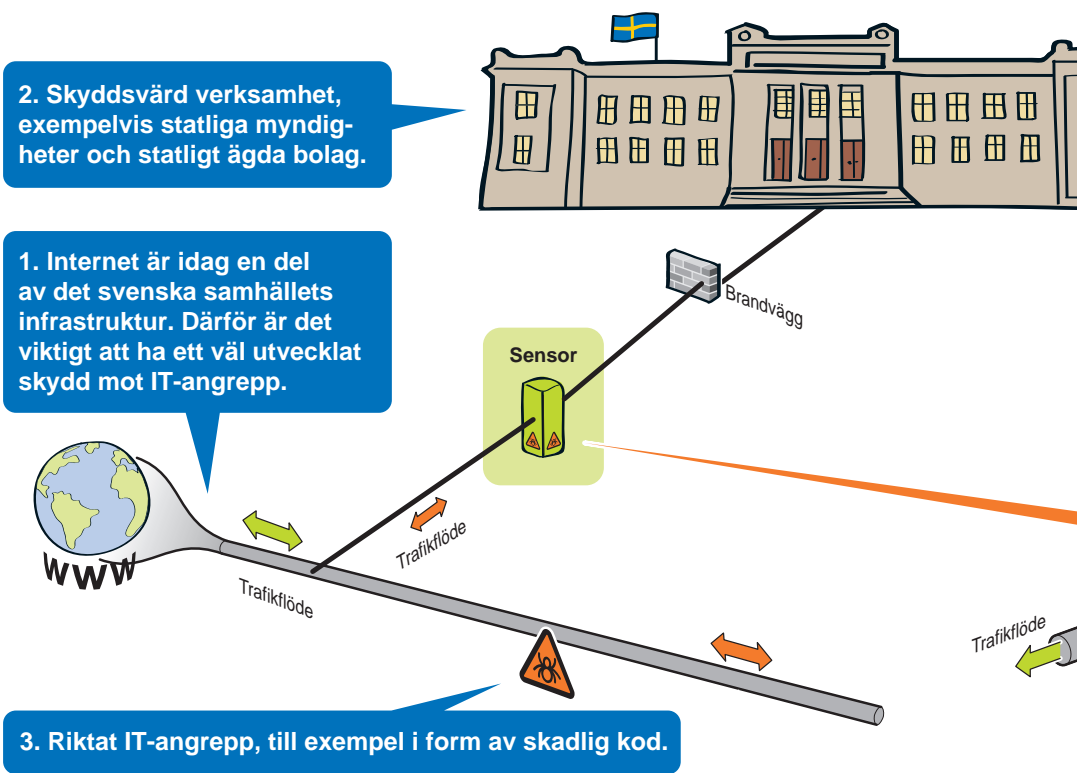
Angreppen utförs oftast av resursstarka aktörer, exempelvis andra länders underrättelsetjänster, och det sker bland annat genom så kallad skadlig kod (*malware*).

Till skillnad från de angrepp som uppmärksammats flitigt i medier under 2012, där angriparen vill synas, koncentrerar vi oss på angrepp som är *dolda*. Vid sådana angrepp vill aktörerna som ligger bakom dem undgå upptäckt och de ändrar också sina angreppsmetoder löpande. Ofta vet inte den som angrips att något har hänt, men vi kan vid gynnsamma förhållanden upptäcka spår av angrepp och analysera vad som skett – till exempel identifiera informationsförluster ur känsliga system.

Angreppen kan exempelvis ha som mål att stjäla värdefulla forskningsresultat som svenska forskningsinstitutioner och företag gjort stora investeringar i, och där stölderna därmed försämrar Sveriges framtida konkurrenskraft.

Under 2012 har vårt stöd i samband med den här typen av angrepp och incidenter ökat. Vi samarbetar med Säkerhetspolisen i dessa frågor.

Genom att analysera skadlig kod vid angrepp mot känslig verksamhet i Sverige och sedan jämföra med de signaturer vi har genom signalspanning globalt har vi också under 2012 kunnat identifiera vissa



TDV – ett tekniskt detekterings- och varningssystem för samhällsviktig verksamhet

aktörer bakom dessa angrepp. Det handlar uteslutande om stater eller statsunderstödda organisationer med stora resurser till sitt förfogande.

Under året har vi redovisat ett uppdrag från regeringen angående ett tekniskt detekterings- och varningssystem (TDV) som syftar till att öka informationssäkerheten inom samhällsviktig verksamhet genom att upptäcka, identifiera och varna för förekomst av IT-angrepp.

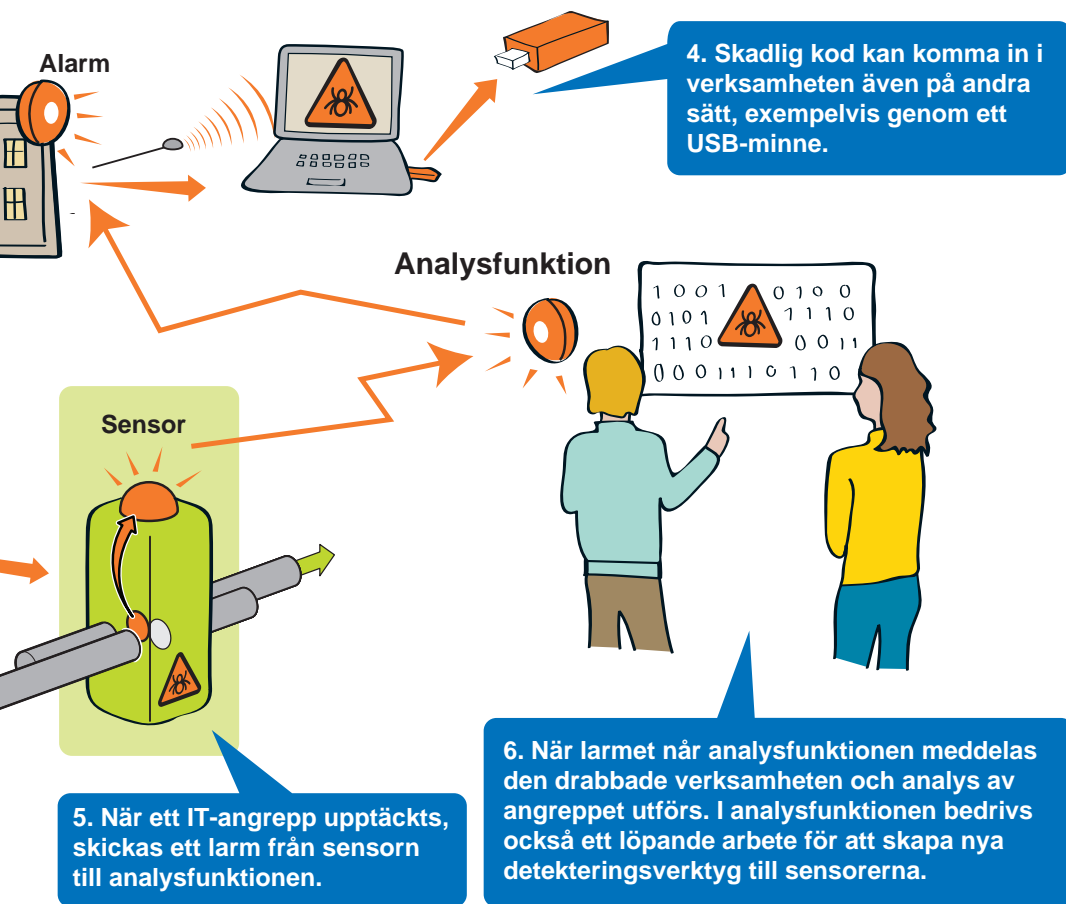
Dessutom redovisades en analys av begreppet cyberförsvar samt förslag på samverkansformer för hur ansvariga

myndigheter gemensamt kan skapa ett effektivt cyberförsvar.

I enlighet med uppdraget utvecklades bland annat en pilotversion av systemet som vi också testat hos en annan myndighet. Utvärderingen av pilotversionen visar att systemet fungerar som avsett och avancerade angrepp har kunnat identifieras med stöd av systemet hos denna myndighet.

I december 2012 etablerades en ny samverkansform kallad NSIT (Nationell Samverkan till skydd mot allvarliga IT-hot) mellan Säkerhetspolisen, Försvarsmakten och FRA. Syftet med NSIT, som





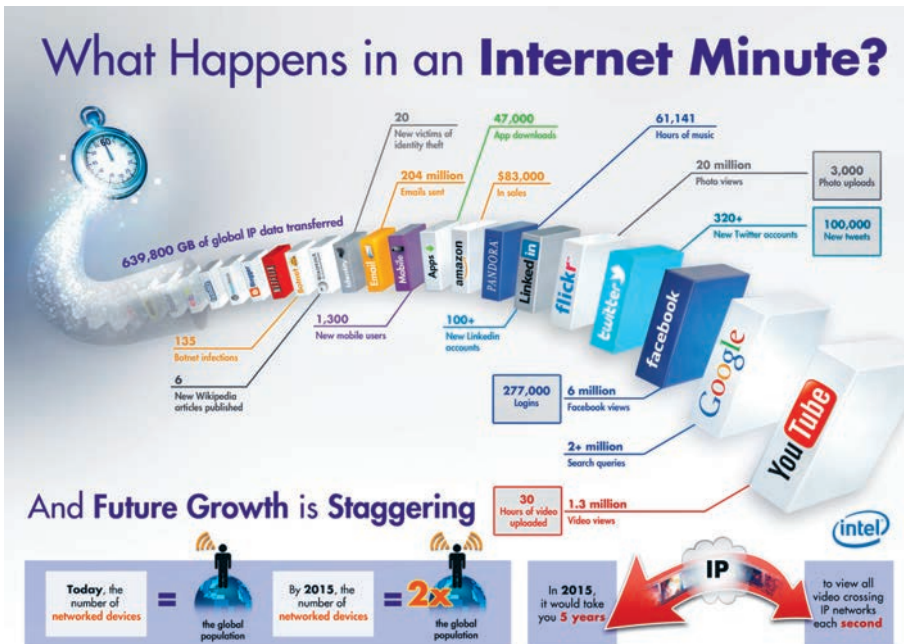
### Tekniskt detekterings- och varningssystem (TDV)

Avancerade IT-angrepp mot samhällsviktig verksamhet blir allt vanligare. Mot bakgrund av denna utveckling fick FRA två olika uppdrag av regeringen 2010–2011. Uppdragen handlade om hur informationssäkerheten i samhällsviktig verksamhet skulle kunna stärkas genom ett så kallat tekniskt detekterings- och varningssystem (TDV).

Det första uppdraget redovisades i mars 2011 och var främst en genomgång av hur ett TDV-system skulle kunna fungera rent tekniskt. I det andra uppdraget, som redovisades till regeringen i april 2012, belystes ytterligare aspekter av systemet. Bland annat togs en pilotversion av systemet fram och testades hos en annan myndighet.

### Nyttan av ett detekterings- och varningssystem

Systemet upptäcker olika former av IT-angrepp (exempelvis skadlig kod). Det som är avgörande för systemets funktion är de kvalificerade detekteringsverktyg och signaturer som används för att upptäcka IT-angrepp. Ett TDV-system är ett komplement till en verksamhets befintliga skydd, såsom brandväggar eller olika typer av antivirussystem. En god informationssäkerhet i grunden och ett aktivt arbete med att ständigt förbättra sitt skydd på olika plan är en förutsättning för att ett TDV-system ska göra största möjliga nytta i en verksamhet.



Den tekniska utvecklingen går i rasande tempo och innebär utmaningar för FRA att ständigt ligga i utvecklingens framkant.

drivs i ett pilotprojekt, är att utveckla samverkan mellan våra myndigheter så att vi tillsammans kan genomföra aktiviteter som försvårar för kvalificerade angripare att komma åt eller skada svenska skyddsvärda civila och militära resurser.

Genom vår kryptografiska funktion vid signalskyddsenheten i Sollefteå har dessutom ett stort antal svenska myndigheter, organisationer och företag som hanterar känslig och/eller hemlig information kunnat utbyta information elektroniskt på ett säkert sätt.

Den 1 juli 2012 fyllde myndigheten 70 år. Detta uppmärksammades med olika arrangemang under året, bland annat med en dag då media kunde besöka anläggningen på Lovön och också göra ett

besök i vårt museum. Dessutom arrangerades en fest för alla medarbetare, särskilda besöksdagar för anhöriga samt för uppdragsgivare och andra särskilt inbjudna.

Under året uppmärksammade vi att det var 60 år sedan, den 13 juni 1952, som sovjetiskt jaktflyg sköt ner en svensk DC-3:a under ett signalspaningsuppdrag öster om Gotland.

I samband med årsdagen av nedskjutningen reste vi en minnessten för de i tjänst omkomna inne på vårt område på Lovön.

Under 2012 har myndigheten tagit flera avgörande steg mot att bättre ta tillvara den unika synergien mellan informationssäkerhetsverksamheten, som arbetar

Så vass att du inte  
behöver prata om det?  
Bra, då är vi överens.

Just nu söker vi dig som gör det omöjliga möjligt.

[www.fra.se/jobb](http://www.fra.se/jobb)



med att stärka skyddet för samhällsviktig information och signalspaningsverksamheten, som följer IT-angrepp i det globala nätet. Organisationen kommer att anpassas efter detta behov under 2013.

Överlag präglades vår verksamhet under 2012 av fortsatt hög förändringstakt. Den enormt snabba tekniska utvecklingen innebär utmaningar för oss att följa den relevanta tekniken för våra underrättelseområden. Denna utveckling kommer att fortsätta under överskådlig framtid och innebära både hög investeringstakt och behov av nyrekryteringar.

Det omställningsarbete som inleddes under 2011, med syfte att frigöra resurser för nya tekniska investeringar som är nödvändiga för att möta utvecklingen, fortsatte under hela 2012.

En del i omställningen är ett kompetensväxlingsprogram som resulterade i att ett 20-tal medarbetare under 2012 valde att acceptera det erbjudande som vi gav om

att sluta i förtid. Denna åtgärd beredde vägen för ett stort antal nyrekryteringar inom relevanta kompetensområden.

För att möta denna utmaning i en tid då det är stor brist på duktiga tekniker och ingenjörer på arbetsmarknaden genomfördes två riktade rekryteringskampanjer under 2012. Dessa resulterade i att ett 20-tal tekniker med rätt kompetens kunde anställas.

#### Visste du att

- FRA stödjer Försvarmaktens internationella insatser. Stödet kan handla om utrustning, underrättelser och kan ske både inför, under och efter en insats.
- FRA samverkar med Säkerhetspolisen och Försvarmakten inom ramen för Nationellt Centrum för Terrorhotbedömning (NCT). NCT arbetar med långsiktiga strategiska analyser av terrorhotet mot Sverige och svenska intressen samt bevakar utvecklingen inom internationell terrorism.

# I morgon

En underrättelsetjänst måste alltid ligga steget före och försöka urskilja vilka trender i samtiden som verkar vara bärande. Den måste noga följa utvecklingen i de internationella frågor som är relevanta för svensk utrikes-, säkerhets- och försvarspolitik. Världen förändras och så också de företagsverksamheter som är av intresse för våra uppdragsgivare och därmed för Sverige som nation.

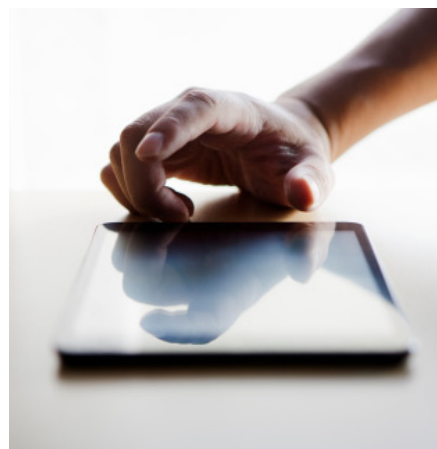
Den mycket snabba tekniska utveckling som vi sett under 2000-talets inledande decennium fortsätter sannolikt i allt högre takt. Nya innovativa produkter och tjänster byter ut varandra i ett hisnande tempo. Det som gäller i dag inom tekniken kan redan vara bortglömt i morgon.

Detta innebär allt större utmaningar för oss som organisation. Vi måste ständigt anpassa vårt arbetssätt och vår teknik till det som är relevant för våra underrättelseområden. Detta ställer ännu högre krav på en flexibel teknikorganisation.

Stödet till Försvarsmakten kommer under överskådlig framtid att vara ett fortsatt viktigt område för oss, men innebär krav på ökad flexibilitet och förmåga

att stödja flera parallella insatser med kortare varsel.

Framtiden för också med sig risker genom att företagsverksamheter såsom ökad globali-





sering, miljöförstöring eller politisk instabilitet i regioner av intresse för Sverige påverkar förutsättningarna för Sveriges utrikes-, säkerhets- och försvarspolitik. Regeringens behov av relevanta underättelser i sådana avseenden lär därför vara stort även i framtiden.

I ett nationellt informationssäkerhetsperspektiv medför den accelererande teknikutvecklingen och den ständigt växande floran av kommunikationslösningar nya risker. Sveriges växande beroende av en fungerande infrastruktur för kommunikation och av olika slags data-system fortsätter att skapa sårbarheter för samhället i stort och för samhällsviktig verksamhet i synnerhet.

IT-angrepp mot nationellt viktiga informationstillgångar kommer därför att vara ett fortsatt stort problem i ett nationellt sårbarhetsperspektiv.

Denna utveckling har inneburit att skydd mot och underrättelser kring IT-angrepp blivit en av de viktigaste delarna av verksamheten på FRA.

Vår samverkan med andra myndigheter på informationssäkerhetsområdet har fördjupats ytterligare, och i morgon har vi, tillsammans med flera andra myndigheter, etablerat ett effektivt svenskt cyberförsvar. Vi är fortsatt en underrättelse- och informationssäkerhetsmyndighet i tiden.



**COPYRIGHT**  
**FRA**

**FORMGIVNING**

Nowa Kommunikation, Stockholm, 2013



FRA | Box 301 | 161 26 Bromma | Tel 08-471 46 00 | [www.fra.se](http://www.fra.se)