FRA

Årsrapport 2010

Innehåll

Förord

Den här årsrapporten är den första i sitt slag. Vår verksamhet omfattas av hög sekretess som gör det svårt att berätta i detalj vad vi gör och varför. Vi tycker ändå att det är viktigt att försöka tillhandahålla så mycket information till allmänheten som möjligt.

Innehållet i FRA:s underrättelserapporter har varierat under årens lopp. Världen såg mycket annorlunda ut när myndigheten bildades mitt under brinnande krig 1942. Mycket har hänt sedan dess – kalla kriget är slut, hotbilden har förändrats och förutsättningarna för Sveriges utrikes-, säkerhets- och försvarspolitik har kommit att radikalt förändras i och med Sveriges inträde i EU, vårt deltagande i internationella insatser och andra omvärldsförändringar.

En tydlig trend är att avancerade IT-angrepp ökar. Under 2010 ökade antalet incidenter mot samhällskritisk verksamhet och kritisk infrastruktur kraftigt. Bland annat förekommer systematisk underrättelseinhämtning. Aktörerna bakom sådana angrepp är ofta stater eller statsunderstödda aktörer med stora resurser.

För FRA var 2010 det första helåret med den omfattande lagstiftning som numera präglar vår verksamhet och som innebär att vi har möjlighet att bedriva signalspaning i kabel som passarar rikets gräns. Inhämtningen av kabelburen trafik är igång, och vi har under 2010 producerat de första underrättelserapporterna baserade på denna inhämtningsmetod.

Ett stort arbete har lagts ner på att tillmötesgå de krav och frågor som vi under året fått från både tillfälliga granskningsinstanser och från Statens inspektion för försvarsunderrättelseverksamheten, som sedan 1 december 2009 är det permanenta granskningsorganet. Vi har också etablerat rutiner för de ansökningar till Försvarsunderrättelsedomstolen som enligt lagen måste beviljas innan inhämtning kan ske.

Parallellt pågår arbetet med att anpassa oss efter den föränderliga omvärlden. För FRA handlar det om att ligga i den tekniska utvecklingens framkant och om att använda våra resurser så att vi kan svara upp mot de krav våra uppdragsgivare ställer på oss. Framtiden för med sig många tuffa utmaningar. De utmaningarna tar vi oss an med beslutsamhet för att bidra till att skydda Sverige och svenska intressen, i dag och i framtiden.

Ingvar Åkesson
FRA:s generaldirektör

Uppdrag, organisation och personal

FRA (Försvarets radioanstalt) är en civil myndighet. Vår uppgift är att ge våra uppdragsgivare unik information om viktiga utländska förhållanden genom signalspaning mot specifik internationell kommunikation. Vår uppgift är också att hjälpa samhällsviktiga verksamheter att skydda sin IT-miljö.

Våra medarbetare

På FRA arbetar cirka 700 personer. De flesta finns på huvudkontoret på Lovön utanför Stockholm. Av våra anställda är 26 procent kvinnor. Bland myndighetens chefer och ledare uppgick andelen kvinnor till 40 procent.

Våra yrkeskategorier

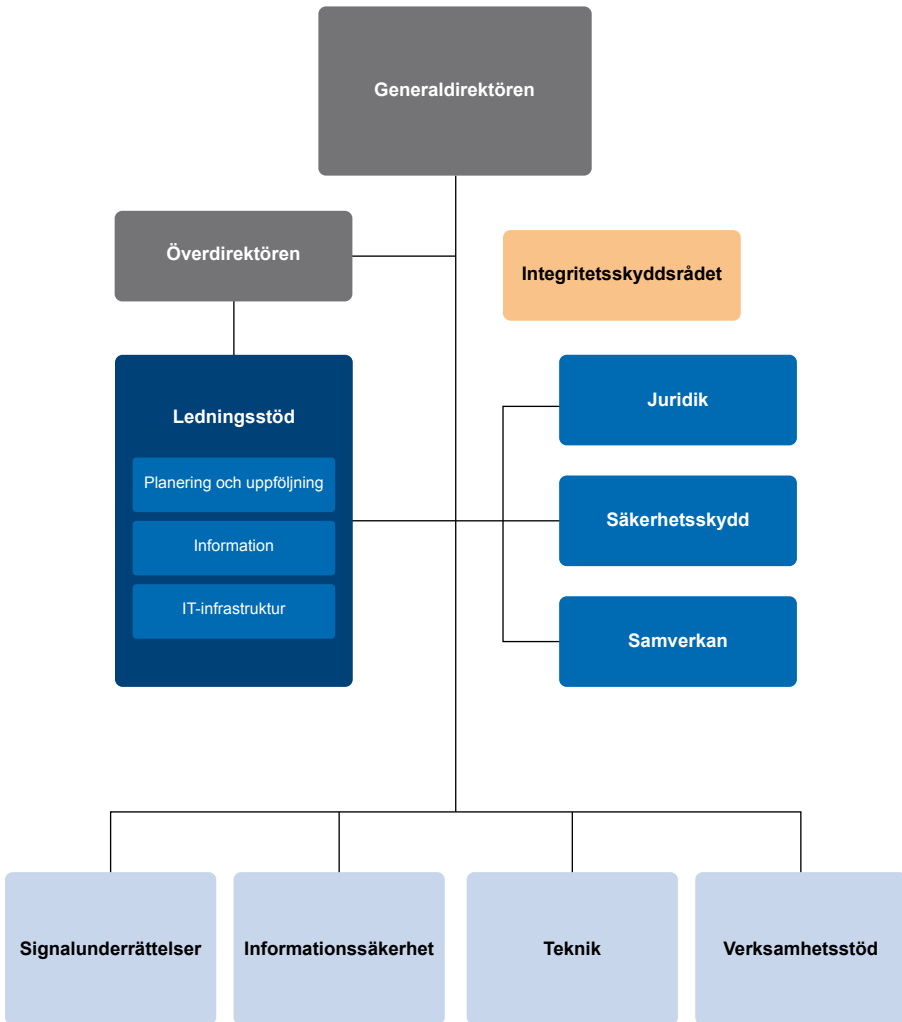
För att vår verksamhet ska fungera krävs många olika kompetenser. Det behövs bland annat civilingenjörer som arbetar med utveckling och drift av tekniska system och medarbetare med kunskaper i radiokommunikation och telekom.

Bearbetning och underrättelseanalys kräver matematiker, personer med statsvetenskaplig eller naturvetenskaplig examen samt lingvister. I arbetet med informationssäkerhet behövs bland annat dataforensiker och experter inom reverse engineering.

Dessutom finns det bland våra anställda HR-specialister, handläggare för upphandlingsfrågor, arkivarier, ekonomer och jurister, samt personal med kunskaper om säkerhetsskydd.

En **dataforensiker** utvinner digital information ur IT-system för att säkra spår och dokumentera eventuella IT-relaterade brott.

Reverse engineering innebär i det här sammanhanget att utifrån en skadlig kod ta reda på hur den är konstruerad, och få kunskap om vilka beståndsdelar den består av och hur de fungerar.



FRA:s organisation.

Två verksamhetsområden

FRA har två verksamhetsområden: signalunderrättelser, där vi producerar rapporter baserade på signalspaning, och informationssäkerhet, där vi stödjer myndigheter och statligt ägda bolag i deras informationssäkerhetsarbete.

Signalunderrättelser

Signalunderrättelseverksamheten består av två delar; kommunikationsspaning och teknisk signalspaning. Inhämtning bedrivs från stationer på olika platser i Sverige och från flygplan och fartyg.

Kommunikationsspaningen riktas mot civila och militära radiosignaler som till exempel telefoni, telegrafi och dataöverföringar, samt numera även mot viss kabeltrafik som passerar rikets gräns. Inhämtade signaler bearbetas, analyseras och resulterar sedan i rapporter som sänds till uppdragsgivarna.

Den tekniska signalspaningen riktas primärt mot signaler som inte innehåller kommunikation, främst från radar-, navigerings- och vapenrelaterade system.

Vad får FRA:s signalspaning användas till?

All signalspaning sker mot utländska förhållanden till stöd för svensk utrikes-, säkerhets- och försvarspolitik.

Signalspaning i försvarsunderrättelseverksamheten får enligt lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, endast ske i syfte att kartlägga

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.

Utifrån denna lagstiftning ger regeringen en årlig inriktning till FRA. Den är mer specifik men måste ligga inom ramarna för de områden som nämns ovan.

Informationssäkerhet

FRA har hög teknisk kompetens inom informationssäkerhetsområdet. Det krävs för att kunna stödja de statliga myndigheter och statligt ägda bolag som hanterar information som bedöms vara känslig från sårbarhetssynpunkt eller i ett säkerhets- eller försvarspolitiskt avseende.

Verksamheten innebär i praktiken att vi

- stödjer insatser vid nationella kriser med IT-inslag
- medverkar till identifieringen av inblandade aktörer vid IT-relaterade hot mot samhällsviktiga system
- genomför IT-säkerhetsanalyser
- levererar kryptosystem
- ger annat tekniskt stöd.

För att kunna ge relevant stöd inom informationssäkerhetsområdet genomför FRA studier för att ligga i takt med teknikutvecklingen.

De tjänster som FRA:s avdelning för informationssäkerhet levererar till uppdragsgivarna behovsanpassas löpande. För närvarande består de av bland annat penetrationstester, dataforensiska utredningar och källkodsanalyser.

Underrättelser och integritet

Att integritetsskyddsfrågor har en naturlig plats på FRA kunde Datainspektionen rapportera i december 2010 när dess uppdrag att granska vår verksamhet ur ett integritetsskydds-perspektiv avslutats. Rapporten belyser samtidigt svårigheterna som balansgången mellan effektiva underrättelser och hänsyn till den personliga integriteten innebär.

För att kunna rapportera relevanta underrättelser i rätt tid behöver FRA tillgång till information. En del av underrättelsearbetet handlar om att identifiera mellan vilka informationsbärare informationen kommuniceras. Med dagens förutsättningar innebär det i ökad utsträckning utmaningar med hänsyn till den personliga integriteten.

Signalspaning har i Sverige bedrivits sedan 1900-talets början. Länge var målen i huvudsak militära och trafiken gick till största delen i etern eftersom det dominerande kommunikationssättet var radio.

I dag är situationen annorlunda. Militära sändningar blandas med civila och privata i det globala telenätet, vilket ställer höga krav på att FRA kan sortera och urskilja trafik. Men fortfarande är angreppssättet i grund och botten detsamma, nämligen att vi riktar oss mot information som kommuniceras till eller från en informationsbärare, exempelvis ett robotsystem, en general eller en terrorist. I de två senare fallen är informationsbärarna fysiska personer, vilket ställer krav på oss hur vi hanterar uppgifterna.

Lagstiftningen som gäller vår verksamhet är omfattande. Bland annat har genomgripande ändringar i den nya signalspaningslagen och ändringar i närliggande lagar påverkat oss. Under 2010 har vi anpassat oss till de nya förutsättningar som denna lagstiftning inneburit.

Integritet och relevans

Att värna den personliga integriteten i signalunderrättelseverksamhet hänger nära samman med förmågan att urskilja den trafik som är relevant, sådan som vi för uppdraget bör inhämta och som vi enligt gällande tillstånd får inhämta. I denna trafik kan inhemsk kommunikation i undantagsfall förekomma. Sådan kommunikation måste passera utan att vi kan ta del av den. FRA har utvecklat tekniska metoder och ett tydligt regelverk för denna hantering.

Under 2010 genomgick FRA en omfattande extern kontroll och granskning (läs mer om detta på sidan 10). Datainspektionen (DI) rapporterade sina resultat i december och konstaterar i sin sammanfattning att intrycket av vad man sett är positivt. DI fann också att FRA:s personuppgiftsbehandling sker för de syften som riksdagen och regeringen har bestämt.

FRA har tagit hänsyn till förbättringsförslag från DI, både av de slutsatser som presenteras i DI:s rapport och löpande i den dialog som fördes i samband med DI:s kontroller under 2010.

Ny lagstiftning kräver anpassning

De senaste årens lagändringar har medfört en ökad reglering av FRA:s signalunderrättelseverksamhet. År 2010 var det första hela kalenderår då vi arbetat utifrån dessa nya förutsättningar.

Tillstånds- och granskningsorgan

Ett antal tillstånds-, kontroll- och granskningsorgan har verkat bland annat för att ge ökad insyn i, och kontroll av, hur vi hanterar bland annat integritetsfrågan. Två av dem är permanenta.

Försvarsunderrättelsedomstolen

Sedan den 1 december 2009 ansöker FRA om tillstånd för signalspaning hos Försvarsunderrättelsedomstolen. Ansökningarna är alltid baserade på uppdragsgivarnas underrättelsebehov. Domstolen prövar våra ansökningar utifrån de krav lagstiftningen ställer.

Statens inspektion för Försvarsunderrättelseverksamheten (Siun)

Siun utvecklades ur det tidigare kontrollorganet Försvarets underrättelsenämnd, men har ett tydligare och mer utvidgat mandat att bedriva kontrollverksamhet gentemot bland andra FRA. Siun ger dessutom FRA tillgång till trafik i kabel via de signalbärare som Försvarsunderrättelsedomstolen beslutar om.

Utöver dessa organs uppgifter, gav regeringen två tidsbegränsade uppdrag: ett till Datainspektionen och ett till en parlamentarisk kommitté.

Datainspektionen (DI)

DI fick i uppdrag att kontrollera hur FRA hanterar personuppgifter i samband med signalspaning. Det inleddes i maj 2009 och avslutades den 7 december 2010. Rapporten finns på www.datainspektionen.se.

Signalspaningskommittén

Kommittén påbörjade i september 2009 sitt uppdrag att följa FRA:s signalspaning ur ett integritetsskyddsperspektiv. Upp-

draget redovisades den 8 februari 2011. Betänkandet Uppföljning av signalspaningslagen (SOU 2011:13) finns på www.regeringen.se.

På FRA finns dessutom ett integritetsskyddsråd som utsetts av regeringen för att följa hur vi, genom interna föreskrifter och rutiner, säkerställer att den personliga integriteten skyddas.

Insyn i verksamheten

För att kunna utföra sina uppdrag, har granskningsorganen genomfört ett stort antal besök på FRA, både för att få kunskap om hur signalunderrättelseverksamheten fungerar och för att genomföra regelrätta kontroller och inspektioner.

Under årets första månader anordnade vi ett flertal informationstillfällen för att ge Försvarsunderrättelsedomstolen och kontroll- och granskningsmyndigheterna kunskap om hur arbetet med att ta fram underrättelser ur elektromagnetiska signaler går till.

Sammantaget har kontroll- och granskningsorganen besökt oss i genomsnitt två gånger i veckan under året.

Vi har också visat granskningsorganen hur vi har anpassat arbetssätt, metoder och tekniska system i enlighet med de nya lagarna och förordningarna.

Tillstånd krävs för signalspaning

År 2010 var det första hela året med de nya kraven på tillstånd för all signalspaning. FRA har under året anpassat verksamheten till de nya förutsättningarna.

För att få inhämta trafik måste FRA söka tillstånd hos Försvarsunderrättelsedomstolen. Ansökningarna utgår från den inriktning som redan finns. Inför domstolen redogör vi noggrant för hur vi avser att gå till väga för att utföra inhämtningsuppdraget.

En ansökan innehåller bland annat följande:

- syftet med inhämtningen
- om informationens värde klart överstiger det eventuella integritetsintrånget
- uppgifter om de sökbegrepp eller kategorier av sökbegrepp som vi avser att använda
- vilken eller vilka signalbärare vi behöver få tillgång till, om spaningen ska ske i kabel.

Tillstånd för varje uppdrag får beviljas för högst sex månader.

Statens inspektion för försvarsunderrättelseverksamheten (Siun) ger oss sedan access till den eller de signalbärare som omfattas av tillståndet.

Avgränsning av trafik

Signalspaningsuppdragen styr vilken trafik som är relevant att inhämta. Genom väl utarbetade och exakta sökbegrepp avgränsar vi den trafik vi har tillstånd att ta del av. Vi gör detta med en automatisk urvalsprocess som så långt som möjligt sorterar bort den irrelevanta trafiken (läs mer på sidan 9).

Mer om signalspaning i kabel finns att läsa på www.fra.se.

Vad finns i en kabel?

- En kabel innehåller fiberoptiska trådar. Det är i dessa trådar signalerna går. En tråd brukar kallas för signalbärare.
- Antalet signalbärare per kabel kan variera, men det vanligaste är att en kabel innehåller ett hundratal signalbärare.
- Varje signalbärare rymmer i sin tur hundratalet olika våglängder, eller frekvenser.
- I en och samma frekvens passerar i normalfallet information som omfattar 10 gigabit per sekund.
- På ett dygn motsvarar trafikmängden, för varje frekvens, cirka 23 000 fulla DVD-skivor, som om man staplade dem skulle nå en höjd av 27 meter.

Foto: Johan Alp, Alp Images

Ökat stöd till Försvarsmakten

Försvarsmakten är sedan länge en av FRA:s viktigaste uppdragsgivare. Det gäller såväl kommunikationsspaning som den tekniska signalspaningen och rör både tekniskt stöd, underrättelserapportering och utbildning.

Uppdragen åt Försvarsmakten handlar i huvudsak om följande områden:

- stöd i samband med internationella insatser
- produktion av signaler till det så kallade signalreferensbiblioteket (SRB)
- stöd till Försvarsmaktens yt- och luftlägesbevakning
- underrättelser om viktiga utländska förhållanden av betydelse för Försvarsmakten samt
- utbildningsinsatser och teknikstöd

Stödet till Försvarsmakten i samband med internationella insatser har blivit en allt viktigare uppgift för FRA. Stödet kan handla om underrättelser, utrustning och olika typer av specialkompetenser inför, under och efter en insats.

Stödet till Försvarsmaktens yt- och luftlägesbevakning är fortsatt en viktig uppgift liksom produktionen av signaler till signalreferensbibilioteket, som ger underlag till JAS 39 Gripens varnings- och motmedelsystem.

Inom ramen för våra utbildningsinsatser har under förra året specialistofficerare för första gången examinerats av FRA inom området signalspaning.

Signalreferensbiblioteket

- Signalreferensbiblioteket är en databas som innehåller en beskrivning av elektromagnetisk energi som sänds ut i atmosfären genom olika tekniska utrustningar.
- FRA ansvarar för att förse signalreferensbiblioteket med information om dessa signaler.
- Försvarsmakten använder referensbiblioteket som underlag för att skapa specialbibliotek till de radarvarnare som finns i olika flygplan och fartyg.
- Med hjälp av biblioteket kan radarvarnare beskriva och identifiera signaler från främmande mål.

IT-relaterade hot och angrepp

FRA har under 2010 noterat en ökning av IT-relaterade hot och angrepp mot viktiga informationssystem i Sverige och svenska intressen. Antalet myndigheter som efterfrågat stöd från FRA i sitt informationssäkerhetsarbete har också ökat under 2010.

Många myndigheter är i dag mer medvetna om de problem som bristfällig informationssäkerhet kan medföra. FRA:s informationssäkerhetsexperter har under 2010 allt oftare använts för att hantera pågående incidenter och angrepp.

Det vi ser i dag är att angreppen ökar, både i antal och i omfattning. Men framförallt ser vi mer sofistikerade angrepp i form av skadlig kod. Beteendet har dock förändrats: utvecklingen går mot att angreppen inte ska upptäckas.

Genom att en angripare använder sig av skadlig kod som är dold, försvåras arbetet med att skydda informationssystem eftersom det ofta är mycket svårt att upptäcka att man är utsatt för angrepp. I många fall upptäcks inte angrepp förrän det är för sent.

IT-relaterade hot

Dagens och framförallt morgondagens IT-hot kommer från resursstarka och kunniga aktörer som har ett uttalat mål och syfte med sina angrepp. Det växande beroendet av internetbaserade kommunikationsverktyg har ökat sårbarheten gentemot insiders, hackare och spioner.

Aktörerna är framförallt intresserade av att skaffa sig information om statshemligheter, företagshemligheter, forskningsresultat samt information som kan kopplas till ett lands vetenskapliga utveckling och internationella samarbete.

Datoriseringstakten och den ökande exponeringen på internet förväntas bidra till en ökad hotbild för alla delar i samhället. Myndigheter och andra organ i samhällskritiska sektorer kan förväntas bli särskilt utsatta för IT-angrepp.

Hotbilden beror även på händelser i omvärlden och på hur Sverige och svenska medborgare agerar i olika sammanhang. Till exempel kan svensk närvaro i internationella konflikter uppfattas som stötande av vissa grupper. Förändringar av hotbilden kan komma att ske mycket snabbt.

Informationssäkerhet handlar också om Sveriges integritet

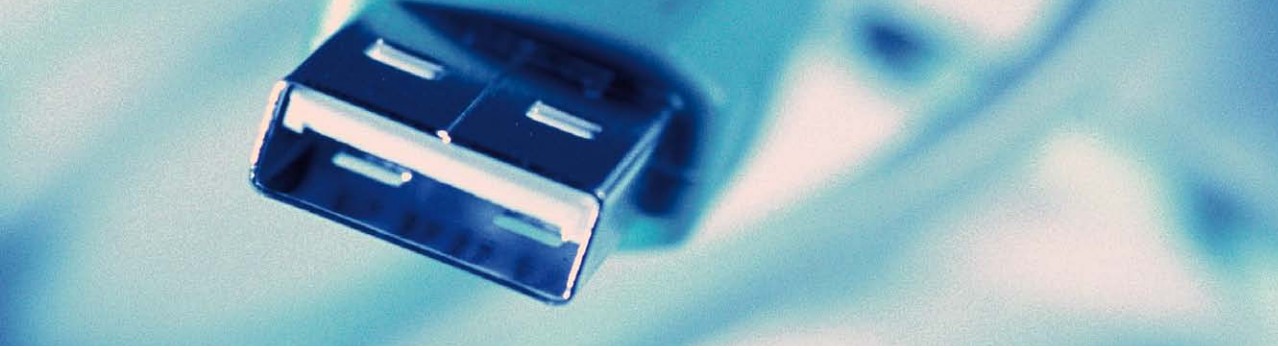
Säkerhet kring information och IT-system i samhället handlar inte bara om att bygga ett effektiv skydd mot angrepp. Det handlar även om att förhindra att datorer i Sverige infekteras för att i sin tur användas som plattform för angrepp mot andra länders system.

FRA har under 2010 kunnat se hur viktiga informationssystem i Sverige är föremål för allt fler angrepp som har systematisk underrättelseinhämtning som syfte. Landets digitala nätverk, vårt ”IT-territorium”, är ytterligare ett territorium där vår integritet kan kränkas.

Tekniskt system för att upptäcka hot i realtid

I april 2010 fick FRA i uppdrag av regeringen att ta fram ett förslag på ett system som kan upptäcka pågående IT-angrepp och larma drabbad verksamhet. Ett sådant tekniskt detekterings- och varningssystem är ett steg mot ett nationellt cyberförsvar. Arbetet med uppdraget pågick under 2010 och vi lämnade vårt förslag 1 mars 2011.

Du kan läsa mer om vårt förslag på www.fra.se.



Statens resurs för teknisk informationssäkerhet

FRA har under 2010 genomfört föreläsningar och förevisningar om informationssäkerhet på mässor, konferenser och utbildningar i större omfattning än tidigare.

För att bidra till en hög nivå på informationssäkerheten i samhället har FRA genomfört 35 föreläsningar och demonstrationer för myndigheter och organisationer. Föreläsningarna har främst avsett hot och risker, skyddsåtgärder samt statens roll och uppgifter inom området.

Under året har vi för första gången hållit en avancerad utbildning för ett tjugotal IT-tekniker från myndigheter och organisationer inom offentlig sektor. Innehållet, effektiva åtgärder för att säkra Windowsnätverk, bygger på våra erfarenheter av genomförda informationssäkerhetsanalyser.

FRA har också på olika sätt medverkat till att kurserna Informationssäkerhet för chefer och Chief Information Assurance Officer har kunnat genomföras i Försvarshögskolans regi.

Inom informationssäkerhetsområdet hjälper också FRA svenska myndigheter som hanterar känslig information med utbildning i signalskydd och säker kommunikation. Under 2010 har antalet myndigheter som FRA stödjer på detta sätt ökat.

Ökad nationell samverkan

FRA:s nationella samverkan intensifierades under 2010 genom att myndigheten bidrog med expertstöd inom ramen för utvecklingsarbetet inom samverkansgruppen SAMFI.

SAMFI (Samverkansgruppen för informationssäkerhet) är ett forum för samverkan och informationsutbyte mellan myndigheter med särskilda uppgifter inom området informationssäkerhet.

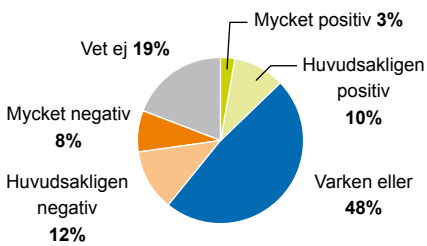
I SAMFI ingår Försvarsmakten, Försvarets materielverk, FRA, Post- och telestyrelsen, Rikspolisstyrelsen och Myndigheten för samhällsskydd och beredskap.

Allmänhetens bild av FRA

FRA är en välkänd myndighet och majoriteten är neutral i sin uppfattning om oss. 20 procent är dock uttalat negativa. Detta framkommer i en opinionsundersökning från Synovate om allmänhetens kännedom, attityder och förtroende när det gäller myndigheten.

Som ett led i vårt arbete att öka kunskapen om vår verksamhet genomfördes för första gången en opinionsundersökning under sommaren 2010. Totalt tillfrågades 1 014 personer mellan 16 och 80 år om kännedom, attityd och förtroende för FRA.

Cirka 85 procent säger sig känna till myndigheten. Vad gäller attityd och förtroende uppger 13 procent att de är positivt inställda till myndigheten. 20 procent är negativa och resten, två tredjedelar, är neutrala (48 procent svarar ”varken eller” och 19 procent ”vet ej”).



Undersökningen visar att äldre, från 60 år och uppåt, är mer positiva medan yngre män är de som är mest negativa.

Bland de negativa omdömena anger de flesta som skäl för sin inställning rädslan för övervakning på internet och oron för att vår verksamhet skulle vara inriktad på att stoppa illegal fildelning. En del anger också att de känner oro för att verksamheten bedrivs utan insyn och kontroll.

Resultatet pekar på att vi bättre behöver förklara att signalspaningen riktas mot utländska förhållanden som till exempel säkerheten i samband med stöd till internationella insatser, kartläggning av IT-angrepp mot Sverige eller spridning av massförstörelsevapen.

Vi behöver dessutom bättre informera om att det finns en omfattande extern kontroll och granskning av vår verksamhet.

FORMGIVNING
Enestedt & Co, Stockholm, 2011

FRA | Box 301 | 161 26 Bromma | Tel 08-471 46 00 | www.fra.se