ÅRSRAPPORT 2017

UMEEÄ OGKLÖ GRITN UTRKC RSTFI

EHIKO DVSTE AAREH NEPNS SETT

Innehåll

Generaldirektörens förord

Säkerhetspolitiska frågor står högt på dagordningen i svensk debatt sedan ett antal år tillbaka. 2017 kom att bli ett år när några av de hot och risker i omvärlden som mycket av samhällsdebatten handlat om blev påtagliga för oss i Sverige. I ett av dessa fall, terrorattacken på Drottninggatan i Stockholm i april, krävdes fem människoliv och ännu fler personer skadades.

Cyberangrepp som får konkreta konsekvenser för olika samhällsfunktioner är numera en del av vår vardagsverklighet, och behovet av att skydda känsliga uppgifter i myndigheters och företags IT-system har blivit alltmer uppenbart.

Den militära utvecklingen i vårt närområde påminner oss om att frågor om territoriell integritet och så kallade traditionella hot är lika aktuella i dag som tidigare i historien.

Tillsammans med Säkerhetspolisen och Försvarsmakten tillhör FRA de myndigheter som regeringen gett utökade uppgifter för att Sverige ska kunna möta dessa säkerhetsutmaningar, så att människorna i vårt land ska känna trygghet. Ytterligare resurser satsas på kontraterrorverksamheten. FRA och Säkerhetspolisen har också fått ett uppdrag att utöka stödet till statliga myndigheters förmåga att skydda sig emot och hantera allvarliga IT-angrepp. Sveriges digitala territorialförsvar stärks. Beslut har också fattats om att ersätta det nuvarande signalspaningsfartyget HMS Orion.

Samtidigt intensifierar vi och dessa två myndigheter vårt samarbete. Tillsammans gör vi Sverige säkrare.

FRA är en utpräglad kunskapsorganisation. Att ha spetskompetens på ett flertal områden är en förutsättning för att vi ska kunna fullfölja vårt uppdrag. Därför är frågan om kompetensförsörjning avgörande för oss när uppgifterna utökas.

Att kunna möta dagens och morgondagens rekryteringsbehov, bland ofta mycket efterfrågade kompetenser på arbetsmarknaden, är därför en prioriterad uppgift. Vår styrka är samtidigt att vi kan erbjuda stimulerande arbetsuppgifter på många områden. Och insikten om att man får ett uppdrag där man bidrar till Sveriges säkerhet och integritet.

Dag Hartelius
Generaldirektör

»2017 KOM ATT BLI ETT ÅR NÄR NÅGRA AV DE HOT OCH RISKER I OMVÄRLDEN SOM SAMHÄLLSDEBATTEN HANDLAT OM BLEV PÅTAGLIGA FÖR OSS I SVERIGE.«

Ytterligare ett år av osäkerhet och spänningar

2017 har varit ytterligare ett år av konflikter, osäkerheter och geopolitiska spänningar. Exempelvis konstaterar fredsforskningsinstitutet SIPRI att ”nästan alla stora globala indikatorer för fred och säkerhet gått i en negativ riktning”.

I närområdet har den höga nivån på militär aktivitet fortsatt under 2017. Östersjöområdet är i dag en brännpunkt för den ökade konfrontationen mellan Ryssland och västvärlden. Ryssland har genomfört övningen Zapad 2017, en av de största ryska militärövningarna sedan det kalla kriget, samtidigt som Nato har haft övningarna Sabre Strike och Baltops. Även Sverige har genomfört sin största militärövning på länge genom övningen Aurora.

Parallellt med fortsatta utmaningar inom EU, med en pågående besvärlig process kring Brexit och andra stora frågor, ökar behovet av effektiv europeisk samverkan inom säkerhetsområdet för att möta både övergripande geopolitiska utmaningar och specifika hot såsom internationell terrorism.

I Irak och Syrien fortsätter striderna mot Daesh, och även om Daesh försvagats betydligt syns ännu inget slut på det lidande som orsakas av det pågående syriska inbördeskriget. Kriget i Syrien har resulterat i en förflyttning av hälften av befolkningen – över 4,8 miljoner som internationella flyktingar och över 6,3 miljoner som internt fördrivna – samt över 400 000 döda.

Säkerhetspolisen uppgav 2017 att de står inför en historisk utmaning där antalet individer i de våldsbejakande extremistiska miljöerna i Sverige på några år ökat från hundratal till 3 000.

I Mali, där svenska styrkor deltar i en FN-operation, är situationen fortsatt osäker. Det har förekommit ett antal attacker mot de fredsbevarande styrkorna under 2017 och totalt under uppdraget har 146 FN-soldater dödats, vilket gör det till den dödligaste pågående FN-missionen. Hittills har dock den svenska styrkan inte drabbats av några dödsoffer.

På cyberområdet finns inga tecken på att hoten eller antalet angrepp kommer att minska. Under året har alltmer uppmärksamhet riktats mot de utmaningar som svenska myndigheter har att hantera gällande sin informationssäkerhet.

Försvarsberedningen konstaterar att ”en utvecklad förmåga på informations- och cybersäkerhetsområdet, inklusive en god underrättelseförmåga i den digitala miljön, ökar möjligheten att upprätthålla vår nationella suveränitet, aktivt bidra till att hantera händelser i närområdet och skydda kritisk infrastruktur.”

Mot bakgrund av de uppgifter som framkommit om påverkansoperationer riktade mot de franska och amerikanska valen har risken för liknande påverkan i samband med det kommande svenska valet 2018 alltmer diskuterats. Utan tvivel ställs demokratier inför stora utmaningar när nya möjligheter till antagonistisk påverkan öppnas genom den allmänna fragmentiseringen och digitaliseringen av medielandskapet.

Källor:
FOI: Strategisk utblick 7
SIPRI Yearbook 2017
Försvarsberedningens rapport 2017
Säkerhetspolisen: Pressmeddelande 2017-07-03

Texten baserar sig på öppna källor och ska inte ses som en del av FRA:s underrättelserapportering.

Underrättelser om omvärlden och skydd för svensk information

Underrättelser och cyberförsvar

FRA har som uppdrag att ta fram kvalificerad information om omvärlden för att kunna bidra till skyddet för Sveriges säkerhet och integritet. Dels behövs kunskap om omvärlden för att kunna skydda oss mot olika typer av hot, dels är tillförlitlig information om omvärlden en förutsättning för en självständig svensk utrikes- och säkerhetspolitik.

FRA arbetar även med att se till att vi i Sverige har ett bra skydd för vår egen skyddsvärda information – en viktig del i byggandet av ett svenskt cyberförsvar.

Kvalificerade underrättelser genom signalspaning

Signalspaningsverksamheten vid FRA är en del av den svenska underrättelsetjänsten. Den syftar till att ge ett oberoende beslutsunderlag i frågor som rör svensk utrikes-, säkerhets- och försvarspolitik.

Det kan till exempel handla om följande:

- Militär förmåga hos främmande länder
- Kvalificerade IT-angrepp från andra länder mot känsliga informationssystem
- Internationell terrorism.

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

De som får ge FRA signalspaningsuppdrag är förutom regeringen Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen inom Polismyndigheten (NOA). Oavsett uppdragsgivare handlar det alltid om att kartlägga utländska förhållanden.

FRA:s signalspaning är tydligt reglerad i lag. Regleringen innebär bland annat att FRA:s signalspaning måste ha tillstånd av Försvarsunderrättelsedomstolen och att verksamheten löpande granskas av Statens inspektion för försvarsunderrättelseverksamheten (Siun).

Spetskompetens ökar säkerheten

FRA har ett uppdrag att stärka informationssäkerheten inom samhällsviktig verksamhet. Bland medarbetarna finns spetskompetens inom teknisk informationssäkerhet. Dessutom kan signalspaningsförmågan ge en unik bild av utländska angripare och deras angreppsmetoder. Det gör att FRA har kvalificerad kunskap som kan användas i arbetet med att hjälpa andra myndigheter och statligt ägda bolag att stärka sin informationssäkerhet.

FRA genomför på uppdrag IT-säkerhetsgranskningar, ger råd till andra myndigheter, har varningssystem som kan upptäcka avancerade angrepp, och vi tillhandahåller säkra kommunikationslösningar.

Verksamhet 2017

Omfattande militär verksamhet i Östersjöområdet

Intresset från uppdragsgivarna för den säkerhetspolitiska utvecklingen i närområdet är fortsatt högt. Kraven på tidskritisk rapportering är i dag mer omfattande än på många år.

Under 2017 har den militära aktiviteten varit fortsatt hög i Östersjöområdet. Det är en viktig del av FRA:s signalspaningsverksamhet att följa den militära verksamheten i Sveriges närområde. Förutom övningar gäller det truppförflyttningar, materielförnyelser eller utveckling av nya vapensystem.

Under 2017 har flera större militära övningar ägt rum i Sveriges närområde. Bland annat har Ryssland genomfört övningen Zapad som är en av de största ryska övningarna sedan det kalla krigets slut.

En del av FRA:s spaning utgörs av så kallad teknisk signalspaning, där man spanar mot utländska radarsignaler och signaler från navigeringsutrustning och vapensystem. Denna information ger stöd till Försvarsmakten i att identifiera andra länders militära fartyg och flygplan. Den utgör även ett viktigt underlag för att kunna se till att varningssystem på svenska flygplan och fartyg fungerar så att de kan uppträda på ett effektivt sätt i en stridssituation. Dessutom ger informationen underlag för utveckling av taktik och utrustning för svenska militära plattformar i ett längre perspektiv.

Striderna i Mellanöstern fortsätter

FRA följer krig och konflikter i omvärlden, både i Sveriges närområde och längre bort. Det kan gälla utländsk inblandning i konflikter, interna maktförhållanden, spridningsrisker med mera.

Under 2017 har striderna i Mellanöstern fortsatt. FRA:s rapportering har bidragit till att hålla svenska beslutsfattare väl orienterade om utvecklingen i regionen.

Terrorism med tydliga kopplingar till Sverige och övriga Europa

Säkerhetspolisen är den viktigaste uppdragsgivaren för FRA när det gäller rapportering kring internationell terrorism. Uppdraget innefattar att följa internationella terrororganisationer och eventuella kopplingar till Sverige.

I samband med särskilda händelser i Sverige och övriga Europa har FRA arbetat intensivt med att stödja Säkerhetspolisen i deras arbete. Under 2017 har rapporteringen på kontraterrorområdet ökat påtagligt.

Likaså har samverkan mellan myndigheterna ytterligare intensifierats som en del av ett sammanhållet systemtänkande om det svenska kontraterrorarbetet. FRA, Säkerhetspolisen och Miltära underrättelse- och säkerhetstjänsten (Must) har arbetat inom flera delområden för att stärka myndigheternas samarbete. Inom ramen för samarbetsformen Nationellt centrum för terrorhotbedömning (NCT) underlättas och effektiviseras det praktiska arbetet som ett resultat av en genomförd utredning.

I kölvattnet på att Säkerhetspolisen tidigare fått förstärkta anslag har under 2017 beslut fattats om att även FRA och Must får utökade resurser kopplat till verksamheten inom området internationell terrorism.


Hemköp
Alla dagar 7-23
Ingång T-baneplan
KALL ÖL.
KLIMATSMART. FÖRSTÅS.
clas
SCORETT
stadium
31-9570

Försvarsmaktens insatser i utlandet får ökat skydd

FRA har fortsatt att ge stöd till svensk militär insatsverksamhet utomlands. De underrättelser som levereras bidrar till skyddet för svensk trupp, men även till bedömningar av utvecklingen i stort i det aktuella landet. De har också betydelse i planeringsskedet av en insats.

Främmande underrättelseverksamhet tar sig olika uttryck

Flera länder bedriver underrättelseverksamhet som riktas mot Sverige och svenska intressen. Den vanligaste formen av främmande underrättelseverksamhet utgörs i dag av avancerade IT-angrepp, även om mer traditionella metoder också förekommer. En del av den främmande underrättelseverksamheten mot Sverige gäller spionage som auktoritära regimer riktar mot flyktingar i Sverige.

Påverkansoperationer uppmärksammad risk

Hybridhot och påverkansoperationer har blivit en risk som vi i Sverige inte kan bortse ifrån. FRA har i sitt arbete kunnat konstatera olika former av försök till påverkan. Det gäller både utrikespolitik i stort, påverkan via internet och utländskt stöd till extrema rörelser i Europa. Påverkansoperationer kan ske både på mer traditionellt sätt, men även med inslag av cyberattacker för att komma åt information som kan användas för att påverka opinioner.

IT-angrepp mot Sverige sker hela tiden

FRA följer IT-angrepp i det globala nätet via signalspaningen, men även genom kunskaper från uppdrag hos myndigheter och statliga bolag. Under året har FRA upptäckt flera avancerade angrepp mot mål i Sverige. Vanliga mål i vårt land är forskning och utveckling, försvarsindustri, politiska organ och institutioner och myndigheter med samhällsviktiga uppdrag. Rapporteringen om specifika angrepp går i första hand till Säkerhetspolisen och Försvarsmakten för åtgärder.

Outsourcing skapar sårbarheter

En ny form av angrepp som upptäckts under året handlar om att angriparna tar sig in hos leverantörer av IT-tjänster för att via tjänsteleverantörerna komma åt information hos deras kunder. Kunderna – företag och myndigheter – har i dessa fall outsourcat verksamhet till tjänsteleverantörerna. Denna typ av angrepp är svår att upptäcka för slutmålet men också relativt kostnadseffektiv för angriparen. Ett tydligt exempel under året är det angrepp som kallats Cloud Hopper, där FRA hade en viktig roll i att upptäcka och utreda angreppet. Angreppet omfattade ett stort antal tjänsteleverantörer, såväl internationellt som i Sverige, och angriparna kom åt betydande mängder information hos kunderna.

Med anledning av Cloud Hopper tog FRA fram en åtgärdsplan som spreds till uppdragsgivare och andra inom branschen, med förslag på konkreta åtgärder för att motverka den här typen av angrepp.

Några av de åtgärder som rekommenderas i åtgärdsplanen är följande:

- Förbättra loggning och logganalys
- Skapa starkare autentiseringsmetoder
- Behålla egen personal för kravställning och styrning av IT-säkerhet
- Utvärdera noga vilka system som är lämpliga att läggas ut på entreprenad och vilka som bör skötas internt


'sql') {
'mail') {
'config') {
'fn') {
'Success click here'

Åtgärdsförslag som svar på regeringsuppdrag

Mot bakgrund av de kvalificerade angreppen mot outsourcingföretagen fick FRA tillsammans med Säkerhetspolisen ett uppdrag från regeringen. Detta uppdrag innebar att föreslå åtgärder för att stärka skyddet mot de allvarligaste cyberhoten hos de mest skyddsvärda verksamheterna i Sverige. Till de åtgärder som föreslogs av de två myndigheterna hör bland annat dessa:

- Starkare förebyggande skydd för de mest skyddsvärda verksamheterna
- Ökad förmåga till incidenthantering vid kvalificerade angrepp mot statlig verksamhet
- Förbättrad aggregerad lägesbild över IT-hot och sårbarheter
- Utveckling av långsiktig kompetensförsörjning

Fler varningssystem utplacerade

FRA har fortsatt att placera ut det tekniska detekterings- och varningssystem (TDV) som ska larma om angrepp hos skyddsvärda verksamheter. TDV är en ordinarie del av det stöd som FRA kan erbjuda till myndigheter och statliga bolag på begäran av dessa och i samråd med Säkerhetspolisen. Ett TDV-system utgör en förstärkning av skyddet och gör betydande nytta om den skyddade organisationen i övrigt arbetar systematiskt med sin informationssäkerhet och redan har en bra nivå på skyddet.

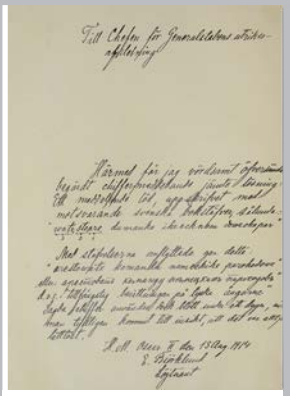
Nöjda signalskyddskunder

Inom ramen för sitt informationssäkerhetsuppdrag hjälper FRA andra myndigheter inom den civila delen av totalförsvaret med säkra kommunikationslösningar, så kallat signalskydd. Via kontoret i Sollefteå lämnar FRA stöd till signalskyddet i hela Sverige. En användarenkät som genomförts under året visar att FRA har mycket nöjda kunder inom signalskyddsverksamheten. Frågorna gällde bland annat leveranskvalitet, driftsättning, utbildning, bemötande, support och kompetens. Inom flera områden var kundnöjdheten 100 procent och den lägsta var 92 procent.

Samverkan nyckel till framgång

Många av de utländska företeelser som FRA följer är globala men har kopplingar till Sverige. Detta gör att betydelsen av samverkan såväl nationellt som internationellt är större än på länge. Exempel på områden där det nationella och internationella underrättelsesamarbetet vuxit i betydelse är internationell terrorism, bedömningar kring andra länders militära förmåga samt skydd mot allvarliga IT-angrepp.

FRA 75 år 1942–2017



1914

Den första svenska signalspaningen genomförs av flottan under första världskriget. Rapport om ryska Östersjöflottan från 1914.

30-talet

Kurser i kryptoforcering för ”lämpliga värnpliktiga studenter” genomförs.

1937

Den tyska kryptomaskinen ”G-skrivarens” krypto löses. Det forcerade materialet ger ett oerhört viktigt underlag när det gäller att hålla Sverige utanför kriget.

1939

En signaltjänstavdelning och en kryptoavdelning bildas inom Försvarsstaben. En inhämtningsstation inrättas året efter i Karlskrona.

Andra världskriget startar.

1940

1942

FRA avskiljs ur Försvarsstaben och blir en egen organisation och en självständig myndighet. Personalstyrkan var vid bildandet 384 personer. På bilden ses personal på 40-talet.

1943

Nya lokaler på Lovön blir inflyttningsklara.

1944

Operation Stella Polaris. En stor del av den finska signalspaningen flyr till Sverige av rädsla för en sovjetisk ockupation.

1945

Andra världskriget slutar.

1947

Val i Polen. FRA rapporterar om att resultatet förfalskats för att gynna kommunisterna. Det kalla kriget börjar, och därmed inser man att svensk signalspaning behövs även i fredstid.

1952

FRA börjar arbeta med datorer genom den första svenskbyggda datorn BESK.

Den svenska DC-3:an skjuts ner över internationellt vatten i Östersjön under ett signalspaningsuppdrag.

1953

FRA följer hur sovjetiska styrkor slår ner upproret i Ungern.

1956

FRA rapporterar om Warszawapaktens förberedelser för invasionen i Tjeckoslovakien.

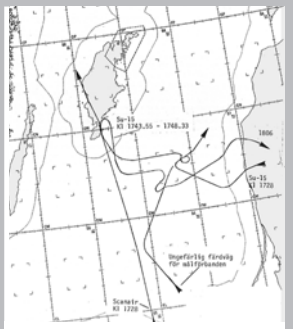
1968

Trafik från kommunikationssatelliter blir ett nytt arbetsområde.

70-talet

Berlinmuren faller.

1989

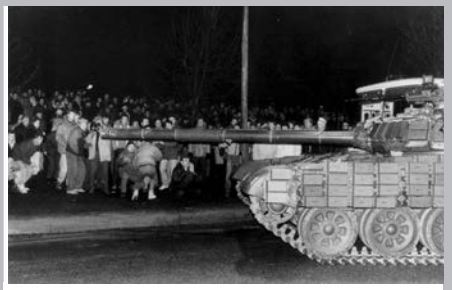


Intensivare kallt krig i Östersjön. FRA följer och rapporterar. I den så kallade Scanair-incidenten följer ett sovjetiskt jaktplan ett svenskt trafikflygplan in över Gotland.

80-talet

FRA börjar med IT-säkerhetsgranskningar.

1988



Sovjetiska trupper sätts in mot en folkmassa som försvarar TV-tornet i Vilnius, varvid fjorton människor dödas. FRA rapporterar om händelsen.

1991

Irak-kriget. FRA rapporterar om att man inte ser några tecken på att Irak kan framställa kärnvapen eller stödjer al-Qaida.

2001

FRA får särskilda uppgifter inom informationssäkerhetsområdet.

2003

FRA fyller 75 år.

2017

Debatten om den så kallade FRA-lagen startar.

2007

Ny signalspaningslag beslutas av riksdagen.

2008

Vad är signalspaning och underrättelser?

Vad är signalspaning?

Signalspaning går ut på att få fram information (underrättelser) ur elektroniska signaler. Signalspaning kan sägas ha existerat från mitten av 1800-talet, när man började med telegraftrafik, och från början av 1900-talet när det gäller radio.

Signalspaning kräver att man inhämtar intressanta signaler, antingen i radio eller i tråd eller på annat sätt. När man fått in signalerna gäller det att utvinna information ur dem. Det kan kräva olika typer av bearbetning, till exempel översättning från främmande språk, trafikbearbetning eller dekryptering.

Trafikbearbetning går ut på att genom sambandsmönster och geografiska lägen på sändare dra slutsatser ur signaltrafik, ofta utan att man kommer åt innehållet i trafiken.

Kryptering är när man döljer innehållet i ett meddelande genom att antingen ersätta ord med koder eller genom chiffrering, där varje tecken ändras enligt en matematisk beräkning.

Kryptering skedde från början manuellt med kodböcker och tabeller. Från 1920-talet utvecklades olika typer av krypteringsmaskiner som automatiskt kunde kryptera text man skrev in. Den mest kända av dessa är den tyska Enigma-maskinen.

Genom tålmodigt och krävande analysarbete går det ibland att få fram texten i ett krypterat meddelande, vilket kallas att forcera det.

Signalspaning kan även riktas mot signaler som inte används för kommunikation, till exempel mot radarsignaler. Ur sådana signaler kan man få fram information om radarns prestanda och även skilja på olika radartyper. Detta kallas i Sverige för teknisk signalspaning.

Vad är en underrättelse?

En underrättelse är information om politiska eller militära förhållanden som har utvunnits genom någon form av underrättelseverksamhet, till exempel signalspaning, bildanalys eller mänskliga källor. En underrättelse kan antingen ge underlag för ytterligare efterforskningar eller utgöra beslutsunderlag för praktiska åtgärder.

Exempel på underrättelser kan vara uppgifter om fiendens grupperingar inför en militär operation eller uppgifter om andra länders politiska beslutsfattande och avsikter. Underrättelser har ofta en viss grad av osäkerhet, man kan alltså inte vara helt säker på att de stämmer. Detta beror på att de handlar om förhållanden som en motståndare vill hålla hemliga och anstränger sig för att skydda. I underrättelserapporter uttrycks osäkerheten i termer av sannolik, trolig och möjlig, där sannolik betyder att man bedömt att det är minst 75 procent säkert att uppgiften stämmer, troligen mer än 40 procent och möjligen mindre än 40 procent.

Underrättelser är oftast färskvaror och förlorar sitt värde efter kortare eller längre tid. Ett exempel kan vara en rapport som säger att fienden ska anfalla på onsdag morgon. Den är naturligtvis toppintressant på måndag och tisdag, men ointressant vid lunchtid på onsdag.

Underrättelsetjänst omfattas oftast av sekretess. Om målen för underrättelseverksamheten får klart för sig vad man har fått reda på och hur man gjort det kommer de att ändra på sina rutiner. Då kan metoder som utvecklats med stora ansträngningar och kostnader gå förlorade.

Sverige behöver ett starkt cyberförsvar

Allvarligaste hotet är avancerade cyberangrepp från andra stater

Enheter som är uppkopplade till internet går att hacka sig in i. Det är bara en fråga om tid, kompetens och resurser. Bakom de mest avancerade angreppen står stater och statsunderstödda organisationer och de utgör de allvarligaste cyberhoten mot Sverige.

Skadlig kod stjäl information utan att upptäckas

Angrepp genomförs med hjälp av skadlig kod som har till uppgift att ta sig in i ett system och påverka det. Till skillnad mot överbelastningsattacker, som märks tydligt och skapar mycket uppmärksamhet, är den här typen av angrepp utformade för att inte upptäckas. Angriparna kan finnas i systemen under lång tid och stjäla lite information i taget för att varningssystemen inte ska reagera.

Angreppen hotar Sveriges säkerhet, demokrati och ekonomi

Syftet med angreppen kan till exempel vara att hitta information om Sveriges försvarsförmåga och vår planering i händelse av en uppblossande konflikt. Det kan också handla om att söka information i samband med en utrikespolitisk förhandling eller att stjäla patent, forskningsresultat eller industrihemligheter för att skapa ekonomiska fördelar för sitt eget land. Dessa angrepp kan alltså påverka Sveriges säkerhet, demokrati och ekonomi. Det är den här typen av angrepp – de mest avancerade angreppen mot Sveriges mest skyddsvärda verksamheter – som FRA fokuserar på att motverka.

FRA är en del av ett svenskt cyberförsvar

FRA:s förutsättningar för att bidra till ett starkt svenskt cyberförsvar är mycket goda tack vare den signalunderrättelseverksamhet som myndigheten bedrivit sedan starten för 75 år sedan och som i dag till stor del bedrivs i det globala nätet.

FRA har teknik och kunskap för att upptäcka och följa skadlig kod genom cyberrymden från de mest avancerade angriparna. Det är denna teknik och kunskap som innebär att FRA kan ge ett unikt bidrag till ett starkt cyberförsvar i Sverige.

Utökat operativt stöd

FRA har sedan länge arbetat med IT-säkerhetsanalyser för att hitta sårbarheter och sedan lämna en lista på rekommendationer. I dag kan man se att detta inte riktigt räcker. Hos många uppdragsgivare finns samma sårbarheter kvar när man genomför nästa säkerhetsanalys. FRA utvecklar därför i samarbete med Säkerhetspolisen möjligheten att kunna erbjuda ett mer kontinuerligt operativt stöd till dessa verksamheter.

Samlad rapportering om hot

En annan fråga handlar om den rapportering som beslutsfattare i Sverige får från olika myndigheter kring de angrepp som sker mot svenska mål. Denna rapportering sker i dag i ”stuprör” vilket ger en splittrad bild och ett sämre beslutsunderlag än om den hade samlats i en enda rapport. FRA arbetar tillsammans med Försvarsmakten och Säkerhetspolisen för att ta fram ett mer aggregerat underlag för beslut om olika skydds- och motåtgärder.

Avancerade varningssystem stoppar angrepp

FRA har placerat ut varningssystem (TDV – tekniskt detekterings- och varningssystem) som fungerar som ett avancerat intrångsdetekteringssystem hos ett antal myndigheter. Dessa system har som uppgift att fånga upp IT-angrepp och varna för pågående angreppsförsök. Information om angreppen skickas därefter tillbaka till FRA för analys som kan ge värdefull information om angriparen. Funktionaliteten i TDV-systemen utvecklas för närvarande för att även kunna stoppa pågående angrepp.

Stöd för att bygga upp aktiv förmåga

I syfte att förstärka möjligheter till motåtgärder i ett starkt cyberförsvar har regeringen gett FRA i uppdrag att stödja Försvarsmakten med att fortsätta analysera och utveckla förmågan att genomföra aktiva operationer i cybermiljön.

Ett cyberförsvar som försvarar den digitala territorialgränsen

Ur ett nationellt perspektiv behövs ett cyberförsvar som skyddar den digitala territorialgränsen. Utan detta riskerar ett land att utarmas ekonomiskt, politiskt och säkerhetsmässigt. Ett cyberförsvar består av tre delar som samverkar och förstärker varandra: kunskap om hoten, skyddsåtgärder och motåtgärder.

Fokus på central ledning och försvar

Den mest skyddsvärda verksamheten är ett lands centrala ledning, som till exempel departement och myndigheter. Även militär verksamhet och försvarsindustri är självklara mål för att ta reda på hur en nation skulle försvara sig vid ett angrepp. Andra viktiga mål för en främmande makt är kritisk infrastruktur som till exempel vatten- och elförsörjning, kommunikationer, sjukvård samt bankverksamhet.

Signalspaning ger kunskap om hoten

Signalspaning i det globala nätet är ett av de viktigaste sätten för att ta reda på hur angreppen ser ut och hur de fungerar. Förmågan att upptäcka och kartlägga de angripare som ligger bakom är central för ett nationellt cyberförsvar. Kunskapen om angreppen används för att bygga upp tekniken kring skydds- och motåtgärder.

Skyddsåtgärder

Skyddsåtgärderna måste hela tiden utvecklas för att möta hotutvecklingen och uppdragsgivarnas behov. Skyddsåtgärderna omfattar såväl tekniska tjänster som rådgivning och utbildning, men även säkra nätverk som tillhandahåller IT- och kommunikationstjänster med särskilda säkerhetskrav.

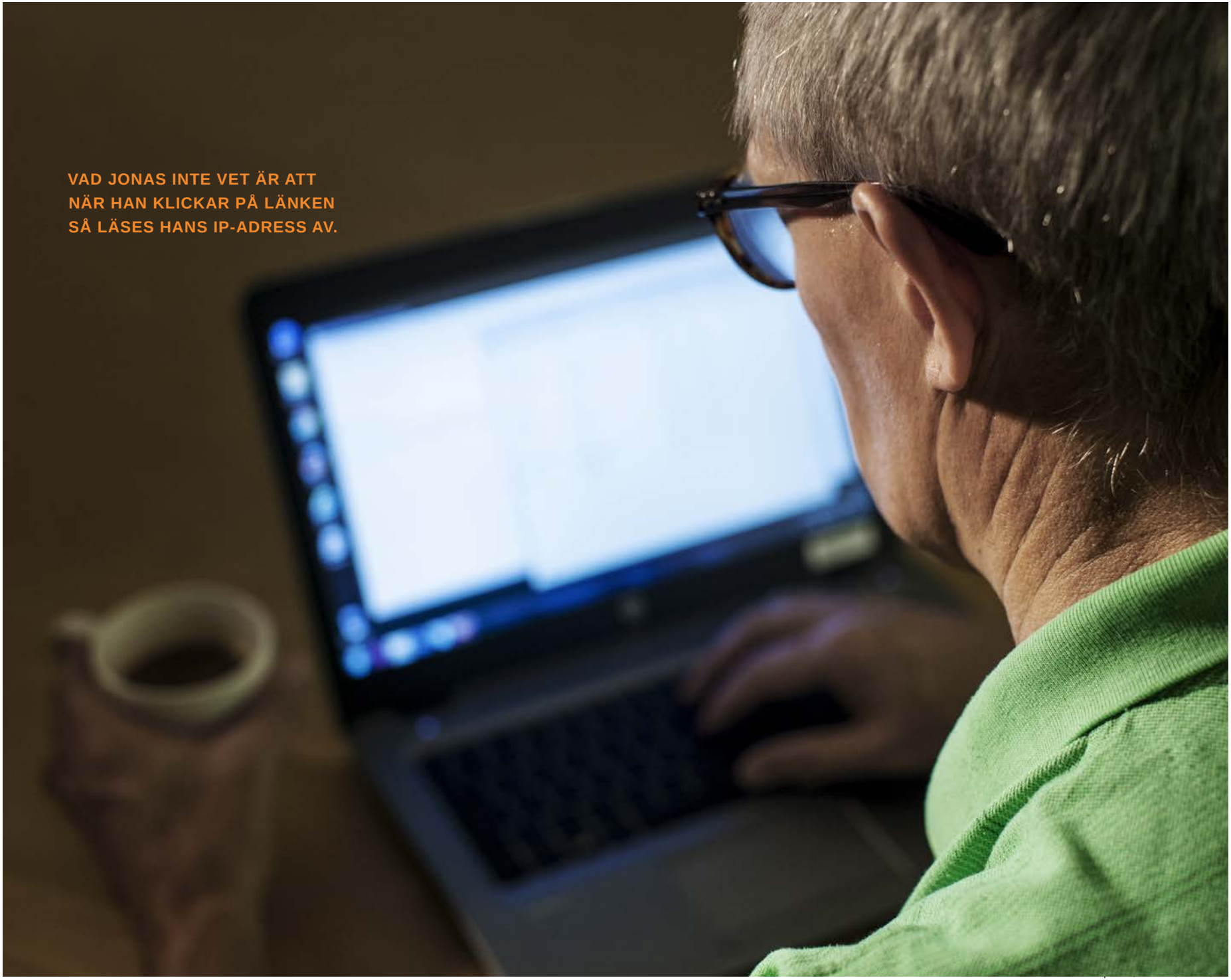
Några av de viktigaste åtgärderna för att förbättra Sveriges cyberförsvar är att öka medvetenheten och kunskapen om cybersäkerhet. Ofta finns det duktiga specialister i berörda verksamheter, men de får inte alltid gehör för sina synpunkter eller mandat att genomföra nödvändiga skyddsåtgärder.

Motåtgärder

Motåtgärder handlar om att upptäcka och stoppa pågående angrepp. Det kan också handla om att genom signalspaning spåra ett angrepp tillbaka till angriparen och på något sätt reagera på angreppet.

Kompetensförsörjningen avgörande

De kvalificerade rollerna inom cyberförsvaret kräver en kombination av kunskaper hos informationssäkerhetsexperter, underrättelseanalytiker och mjukvaruutvecklare. Framgångsrik kompetensförsörjning är avgörande för att FRA, Försvarsmakten och Säkerhetspolisen ska kunna lyckas med sina uppdrag inom området. Det krävs en komplex kombination av förmågor och metoder från samtliga tre myndigheter. Tillsammans utgör de grunden för ett cyberförsvar.


VAD JONAS INTE VET ÄR ATT
NÄR HAN KLICKAR PÅ LÄNKEN
SÅ LÄSES HANS IP-ADRESS AV.

Berättelsen om ett angrepp

Under våren 2017 rapporterades kring ett cyberangrepp som i media fick namnet Cloud Hopper. Här följer en fiktiv historia som baseras på samma tillvägagångssätt.

Jonas arbetar på AB Förenade IT-tjänster, ett företag som arbetar med att på uppdrag sköta andra företags och myndigheters IT-system. Oftast utförs tjänsterna via fjärruppkopplingar mot kundernas system.

När Jonas kommer in på kontoret på morgonen med en kaffe i handen har han ett trettiotal mejl i sin inbox. Han skrollar snabbt igenom dem och skummar innehållet. De flesta kastar han direkt men det är några som han sparar. Fyra från kunder som han ansvarar för att sköta IT-miljön åt, och ett som handlar om en intressant konferens i Amsterdam.

Han öppnar mejlet om konferensen medan han tar en kaka ur en burk på skrivbordet. Han klickar på länken i mejlet och hamnar på en webbsajt med konferensinformation som han tittar igenom. Det verkar lovande, så han laddar ned ett konferensprogram och stänger sedan ned sin webbläsare.

Vad Jonas inte vet är att när han klickar på länken så läses hans IP-adress av. Den bedöms som intressant vilket gör att han nu skickas till en annan sajt med samma information som den med konferensinformationen. Därifrån infekteras hans dator med skadlig kod.

Jonas har nu druckit upp sitt kaffe och börjar jobba med sina kunduppdrag. Som ansvarig för nätverksunderhåll kopplar han upp sig med en fjärranslutning som systemadministratör mot en svensk myndighets nätverk. I dag ska han installera ny nätverksprogramvara hos kunden, men samtidigt som han gör det läser den skadliga koden av uppgifterna kring hans administratörskonto. När Jonas loggar ut finns uppgifterna lagrade hos angriparen.

Nu kan angriparen använda administratörskontot för att ta sig allt djupare in i myndighetens nätverk. Under de följande sex månaderna söker angriparna systematiskt efter information om ny teknologi och patent. Allt som bedöms intressant komprimeras och skickas, bit för bit för att inte väcka någon uppmärksamhet, tillbaka genom Jonas uppkoppling och vidare till angriparen. Där sammanställs informationen och blir grunden till en egen högteknologisk industri i angriparens hemland. Den konkurrerar nu på världsmarknaden med svenska företag med betydligt lägre priser, eftersom de sparat in på egen forskning och utveckling.

Alla namn och verksamheter är påhittade.

Ett nära samarbete ger bättre resultat

Nära samarbete och förståelse för varandras uppgifter och behov ger ökad nytta. Tillsammans kan vi motverka olika typer av hot så att Sverige blir säkrare.

– Hotbilden mot Sverige och svenska intressen ser annorlunda ut än den gjorde för några år sen. Aldrig tidigare har Säkerhetspolisen haft en mer komplicerad uppgift. Vi har ett nytt normalläge och hotbilden är alltmer komplex och berör flera av våra verksamhetsområden. Ett nära samarbete med FRA och Must är en förutsättning för att hålla Sverige säkrare.

Anders Thornberg
Generaldirektör Säkerhetspolisen

– Samarbetet mellan Must, FRA och Säkerhetspolisen har utvecklats och fördjupats de senaste åren. Detta har gynnat ömsesidig förståelse, gett ökad kunskap om komplexa förhållanden och bidragit till ökad nytta för Sverige. Tillsammans har vi hjälpt till att motverka olika typer av hot, bland annat på terror- och cyberområdet.

Gunnar Karlson
Chef för Militära underrättelse- och säkerhetstjänsten, Must

– Inom våra respektive uppdrag arbetar FRA, Säkerhetspolisen och Must i stor utsträckning med likartade frågor, men med olika förmågor, för Sveriges säkerhet och integritet. Genom en nära daglig samverkan och en god förståelse för varandras förutsättningar ökar vi effektiviteten i arbetet samtidigt som vi höjer kvaliteten på våra samlade resultat.

Dag Hartelius
Generaldirektör FRA

»ÄVEN OM DEN DETALJERADE ANALYSEN NUMERA SKER PÅ DATORN SÅ LYSSNAR JAG ALLTID PÅ VARJE SIGNAL. DET ÄR LITE SOM ATT LYSSNA PÅ MUSIK.«

PETER, SIGNALSPANARE

Spaning på hög nivå

Peter har jobbat på FRA i 40 år, varav de senaste 33 åren som spanare på signalspaningsflygplan. Peter har mer än 14 000 flygtimmar och har följt utvecklingen i närområdet från första parkett.

Hur kom du till FRA?

– Jag var intresserad av telegrafi redan som tonåring. I handelsflottan behövs radiotelegrafister, och jag ville se ”den vida världen” så jag sökte mig till sjöbefälsskolan i Härnösand.

– När jag var färdig var det jättesvårt med jobb. Det var oljekris, kaos i branschen. Jag minns hur tavlorna på anrika rederier plockades ner från skolans väggar, en efter en. Det var deprimerande. Då tänkte jag att jag gjort ett brutalt smalt yrkesval, vart skulle jag ta vägen?

– Via en kompis fick jag höra att FRA sökte telegrafister. Jag hade inte den blekaste aning om vad FRA var, men lyckades luska ut en adress. Jag skrev ett brev och fick komma till FRA för att göra tester, bland annat ett telegrafiprov. På den vägen är det.

Hur var det på den tiden?

– Allt var väldigt hemligt, men man vande sig snabbt. Det var bara så det var. Jag fick först en anställning på Gotland. Det var under det kalla kriget, så där satt jag och var mitt i händelserna och den spänning som det var då.

Vad gör en signalspanare ombord på ett flygplan?

– Vi spanar i första hand mot radarsignaler. Det handlar, förr som nu, om att hålla koll på signalmiljön i omgivningen. Även om den detaljerade analysen numera sker på datorn, så lyssnar jag alltid på varje signal. Det är lite som att lyssna på musik. Antingen känner man igen låten direkt, eller också påminner den om något annat liknande. Ibland hör man att de modifierat något, då kanske vi har stött på en signal där en parameter ändrats. Som att någon mixtrat i Queens ”The show must go on” och ändrat några toner.

Hur många signaler känner du igen?

– Har aldrig räknat, men många är det i alla fall. De flesta kan jag placera direkt i en viss kategori, men kanske inte i rätt fack. Det händer att en yngre kollega frågar om en signal och jag kan säga på rak arm att det är den och den roboten i den och den staden.

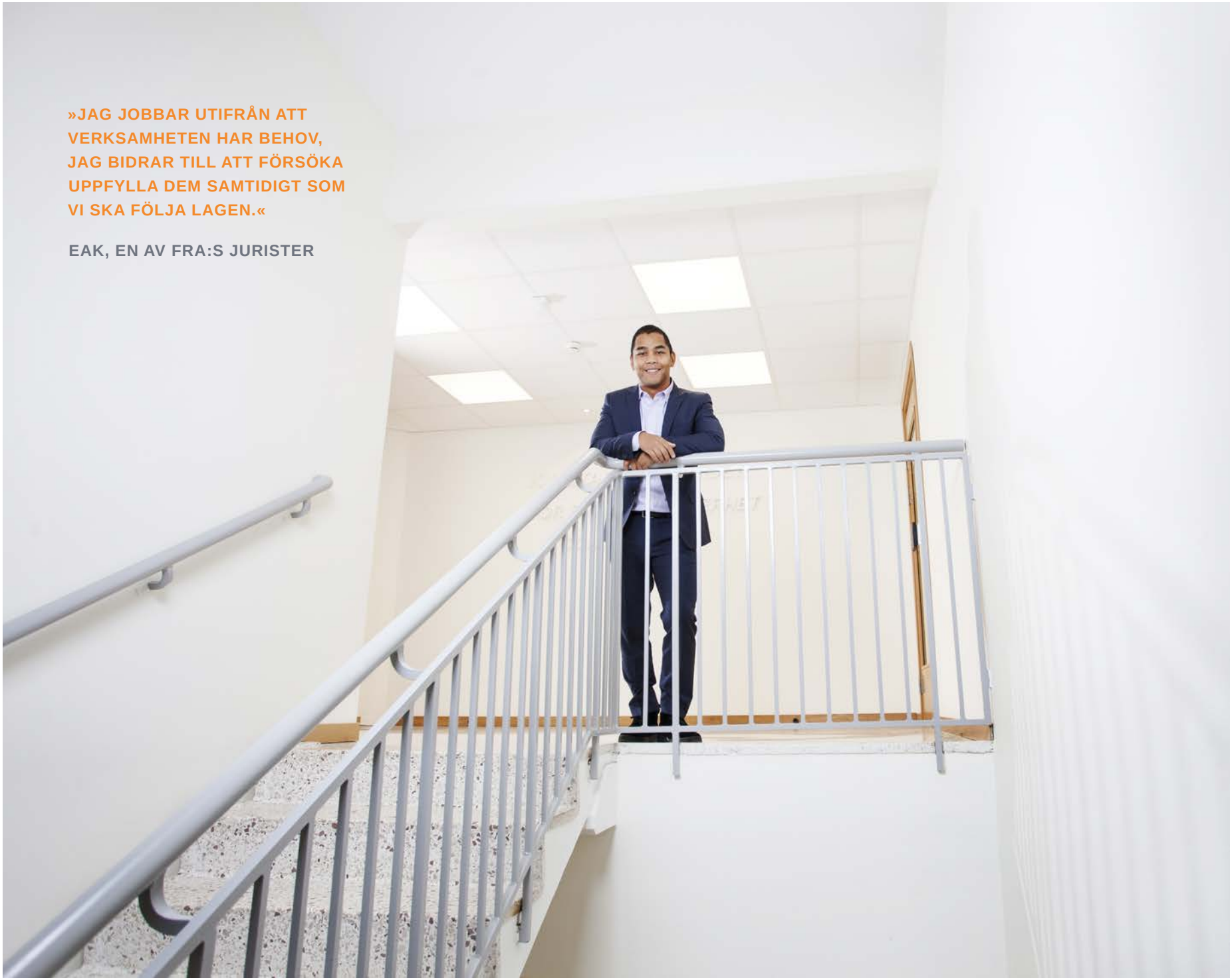
Hur tänker du kring riskerna?

– Försvarsmakten flyger planet och de är jätteproffsiga, så allmänt sett är jag helt trygg. Det är inget man tänker på när man är uppe, då skulle man ju bli knäpp. Däremot blir jag fortfarande illa berörd när jag tänker på besättningen på DC-3:an som sköts ned, och deras anhöriga.

– Ett starkt minne är minnesstunden ute på havet för anhöriga när vraket hade bärgats. Vi flög över platsen precis när de anhöriga kastade sina kransar i havet, vi i mitten och två Viggenplan på varje sida.

Vad är roligast på jobbet?

– När vi stöter på nya typer av signaler. Ibland är vi ju ute på internationella uppdrag, och då är signalmiljön helt ny. För en signalspanare blir sånt lite julafton.



»JAG JOBBAR UTIFRÅN ATT VERKSAMHETEN HAR BEHOV, JAG BIDRAR TILL ATT FÖRSÖKA UPPFYLLA DEM SAMTIDIGT SOM VI SKA FÖLJA LAGEN.«

EAK, EN AV FRA:S JURISTER

Mer än bara rätt eller fel

Eak är en av FRA:s jurister. Såväl valet av juristyrket som FRA som arbetsgivare är något av en slump. Men Eak har inte ångrat något av det.

Hur fastnade du för juridiken?

– I ärlighetens namn, det gjorde jag inte. Jag har alltid varit intresserad av idrott och ville bli gympalärare. Men min SYO-konsulent tyckte att jag hade så bra betyg att jag även skulle titta på andra möjligheter *(skratt)*. Jag frågade vad man kunde tänka sig då och hon sa: ”nåja, till exempel jurist”. Så jag sökte och kom in. Det var verkligen en slump.

Hur hamnade du på FRA?

– Efter en tid på Förvaltningsrätten i Växjö och Kammarrätten i Stockholm ville jag testa annat. Jag har mycket fart och fläkt i mig, eftersom jag hade bakgrund i det förvaltningsjuridiska var det naturligt att söka jobb på en statlig myndighet.

Förvaltningsrätt låter inte så där jättespännande?

– Jo, det är det! Förvaltningsrätt rör relationen mellan staten och den enskilde. På domstolarna handlade arbetet mycket om ”rätt” eller ”fel”. På en myndighet handlar det mer om vilka förutsättningar det finns för att ta vissa beslut eller göra på ett visst sätt. Inom signalspaning finns inte heller lika mycket praxis eller andra rättskällor att luta sig mot, det gör det mer spännande för en jurist.

Ibland beskrivs jurister som lite fyrkantiga, känner du igen dig i det?

– Vi jurister kan nog ibland betraktas som lite av stoppklossar eller petmajor. Men jag jobbar utifrån att verksamheten har behov, jag bidrar till att försöka uppfylla dem samtidigt som vi ska följa lagen.

Vad gör en jurist på FRA?

– Massor med olika saker. Vi hanterar allt-ifrån enklare utlämnandeärenden – alltså där man begär ut allmänna handlingar från oss – till mer komplexa rättsutredningar. Vi granskar olika dokument och deltar som juridiskt stöd i olika samarbeten och förhandlingar. Sen är det ofta verksamheten, ibland tillsammans med chefsjuristen, som slutligen fattar beslut i de frågor som vi hanterar.

Vad gör du en helt vanlig dag?

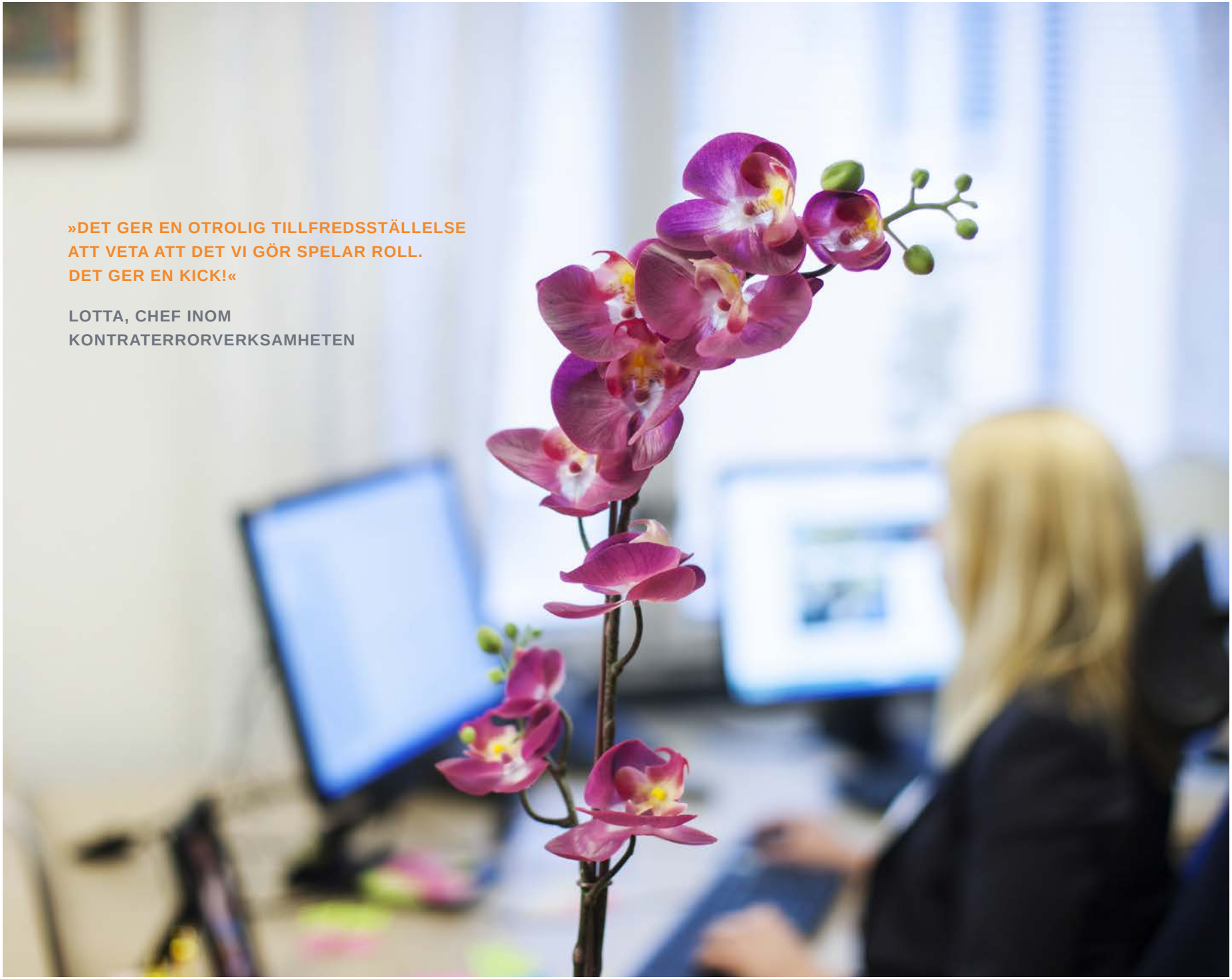
– I dag började jag dagen med att läsa på inför ett remissyttrande. Sen var jag med på ett samverkansmöte med Säkerhetspolisen och Försvarsmakten om terrorlagstiftningen. Efter lunch deltog jag i verksamhetsplanering för min avdelning. Nu ska jag få iväg ett svar på ett utlämnandeärende och sen tänkte jag avsluta dagen på gymmet.

Vad är mindre roligt?

– Ärenden som är slentrian, när det är bara ren administration. Men det är en del av jobbet.

Vad är det bästa med att jobba på FRA?

– Att jag har så intressanta arbetsuppgifter, samtidigt som jag faktiskt kan ha ett privatliv. När jag jämför med mina kurskamrater på andra jobb är det många som jobbar på tok för mycket. Det är också kul att få jobba med många olika typer av människor med olika bakgrund. Att bara arbeta med andra jurister vore tråkigt i längden!



»DET GER EN OTROLIG TILLFREDSSTÄLLELSE ATT VETA ATT DET VI GÖR SPELAR ROLL. DET GER EN KICK!«

LOTTA, CHEF INOM KONTRATERRORVERKSAMHETEN

Här skapas pusselbitar till hotbilden

Lotta är statsvetare och chef inom FRA:s kontraterrorverksamhet. Hon har tidigare arbetat på Militära underrättelse- och säkerhetstjänsten, Must.

Hur blir man chef inom FRA:s kontraterrorverksamhet?

– Jag har alltid varit intresserad av det som sker ute i världen. Det första ordet jag lärde mig skriva var Sydafrika, fast felstavat förstås. Sen har jag sökt mig till utbildningar och jobb med internationell dimension. Efter ett par år utomlands, bland annat i Afrika, fick jag jobb på Must. Efter åtta år där fick jag ett tips om det här jobbet på FRA.

Vad gör du på dagarna?

– Det är allt från verksamhetsutveckling och personalfrågor till ledningsgruppsmöten men förstås också en del operativa frågor. Sen vill jag läsa underrättelserapporter, det är ju det som är outputen, men har inte alltid tid. Då går jag runt i korridoren för att inte hamna för långt bort från verksamheten och hetluften.

Vad består själva jobbet av?

– Mycket handlar om att svara på de frågor som Säkerhetspolisen ställer. Vad händer med den och den terrorgruppen, hur finansieras verksamheten, vilka svenska kopplingar finns det? Vi kan se en del som det kan vara svårt för Säkerhetspolisen att få information om, till exempel i länder där polisiärt samarbete är svårt att få till.

Ser ni om jag skriver ”bomb” i ett mejl?

– Nej, så går det verkligen inte till. Vi följer inte saker på måfå eller spanar på alla, det har vi varken rätt att göra eller resurser till.

Vad säger du till vänner och bekanta om det du gör?

– Inte mycket. Min närmsta krets vet var jag jobbar, men inte med vad.

Vad tycker du om filmer och tv-serier som Homeland?

– Många tv-serier är rätt så överdrivna, även om jag känner igen mig. Sen retar jag mig på vissa detaljer. Som att de pratar om jobbet på sin mobil mitt i stan, det är ju inte så man gör. Men jag gillar Falsk identitet, Fauda – och faktiskt även Game of Thrones.

Kan du säga något om vad ert arbete bidragit till?

– Jag kan inte prata om konkreta fall. Men det ger en otrolig tillfredsställelse att veta att det vi gör spelar roll. Det blir skarpt för oss som jobbar med det, nästan varje vecka faktiskt. Det ger en kick!

Hur påverkar det ert arbete om det sker ett terrordåd i Sverige?

– Vid sådana händelser jobbar vi dygnet runt. Då är det inte så lätt för medarbetarna att gå hem och säga tack för i dag. Många vill sitta kvar av lojalitet och ansvarskänsla. Jag kan inte säga mer men jag vet att det vi gör i sådana fall är viktigt.


75

KUNSKAP OM UTLANDET
– FÖR SVERIGES SÄKERHET OCH INTEGRITET

Utgivare: FRA | Grafisk form: Sinfo Yra | Foto: Björn Tesch, Erik de Castro/Reuters, Sergei Grits/AP, Jonathan Nackstrand/AFP, TT, EPA, Kari Kuuka/TT, AFP, Jerome Delay/AP, Peo Werngren, iStock | Tryck: Åtta45 2018