ÅRSRAPPORT 2018

ÄTVVFVWWÅTYVYBYÅZMWASVRR

Innehåll

Nationell säkerhet i flera dimensioner

Den som under de senaste tre–fyra decennierna har arbetat med att följa och förstå utvecklingen i omvärlden konstaterar nog i likhet med mig att detta på flera sätt har blivit allt svårare. Visserligen var en del av omvärlden under det kalla kriget sluten och delvis svåråtkomlig, men hotbilden var samtidigt mer eller mindre konstant och handlade framför allt om traditionell militär säkerhet.

Idag är de militära frågorna åter mycket påtagliga med en tillförsel av allt mer avancerad materiel och ökad övningsverksamhet i Sveriges omedelbara närområde. Behovet av att kunna följa denna utveckling är stort och stigande.

Planering och utförande av terrorattacker fortsätter sedan några år tillbaka att vara en realitet i Europa och Sverige med tragiska konsekvenser i form av döda och skadade. Att förutse och förhindra dessa är en central fråga för underrättelse- och säkerhetsmyndigheterna.

Avancerade cyberattacker från statliga angripare i andra länder är numera en del av vardagen och syftar bland annat till att stjäla information som har betydelse för Sveriges säkerhet, eller till att stjäla det som utgör en grundbult för vårt välstånd – vårt kunnande och våra innovationer. Att kunna se dessa angrepp och att bygga ett effektivt skydd mot dem är en nationell säkerhetsfråga.

Den nationella säkerheten handlar med andra ord numera om flera dimensioner samtidigt som händelseutvecklingen i alla dessa dimensioner går långt snabbare än under det kalla kriget, en trend som har fortsatt att förstärkas under 2018. Detta är FRA:s huvudsakliga arbetsfält och vi löser uppgifterna i nära samverkan med i första hand Försvarsmakten och Säkerhetspolisen, men också med Polisen och MSB.

Under 2018 har detta praktiska vardagssamarbete fördjupats ytterligare på flera områden. Också de diskussioner om det framtida cyberförsvaret som pågår pekar på att en mer integrerad myndighetssamverkan behövs på detta område.

En effektiv och nära samverkan med både nationella och internationella samarbetspartners utgör idag en helt avgörande förutsättning för att upptäcka, följa och motverka allvarliga hot mot vår säkerhet. Ensam är inte stark. Det är tillsammans som vi skapar trygghet för Sverige.

Vårt uppdrag för Sveriges säkerhet och integritet återspeglas mycket tydligt i våra medarbetares höga motivation.

Det är också en betydelsefull faktor för att vi fortsätter att kunna rekrytera spetskompetens på en mycket konkurrensutsatt arbetsmarknad. I en osäkrare omvärld blir uppgiften att bidra till vår nationella säkerhet allt viktigare.

Dag Hartelius
Generaldirektör


»DEN NATIONELLA SÄKERHETEN HANDLAR NUMERA OM FLERA DIMENSIONER, OCH HÄNDELSEUTVECKLINGEN I ALLA DESSA DIMENSIONER GÅR LÅNGT SNABBARE ÄN FÖRR.«

Övningen Trident Juncture.

Året som gått

I allt väsentligt har 2018 präglats av en fortsättning av de trender vi sett under senare år. Den militära aktiviteten i Sveriges närområde har legat kvar på en hög nivå. Rysslands tillförsel av mer avancerad materiel och ett mer offensivt uppträdande har föranlett Nato att visa sin beslutsamhet till försvar. Natoövningen Trident Juncture, där även Sverige deltog, ägde rum i området kring Norska havet under oktober–november och var Natos största övning sedan kalla kriget.

En betydande friktionsyta mellan Ryssland och väst utgörs också av det ryska agerandet gentemot Ukraina alltsedan annekteringen av Krim 2014. I slutet av året eskalerade denna konflikt ytterligare med anledning av Rysslands agerande mot ukrainska fartyg och avspärrningen av Kertj-sundet.

Cyberattacker utförda av de mest kvalificerade statsaktörerna fortsätter att öka i både omfattning och sofistikeringsgrad och väcker samtidigt växande uppmärksamhet. Under 2018 utpekades Ryssland publikt för att ha använt den skadliga koden *NotPetya* mot Ukraina och med ännu vidare globala konsekvenser för viktiga samhällsfunktioner. Det brittiska nationella cybersäkerhetscentret NCSC offentliggjorde också tekniska uppgifter om sådan skadlig kod som handlar om förberedelser för cyberangrepp. World Economic Forums *Global Risk Report 2018* pekar ut cyberattacker som årets tredje mest sannolika globala risk efter extremt väder och naturkatastrofer.

Chefen för Säkerhetspolisen, Klas Friberg, uppgav i en intervju under 2018 att främmande underrättelseverksamhet mot Sverige utgör ett allt större hot och han pekade i sammanhanget ut Ryssland, Kina och Iran som särskilt aktiva. På den internationella arenan har inte minst mordförsöket i Storbritannien på Sergej Skripal och hans dotter samt den av nederländska myndigheter avslöjade operationen mot Organisationen för förbud mot kemiska vapen (OPCW) kommit att uppmärksammas.

Parallellt med konflikter av mer traditionellt slag växer också insikterna om olika former av gråzonskonflikter där påverkansoperationer, psykologisk krigföring och falska nyheter är betydande inslag. Senast i oktober släppte Twitter uppgifter om tio miljoner tweetar som härrörde från ryska och iranska så kallade trollfabriker, där den ryska operationen var den mest omfattande. Också frågor om utländska fastighetsköp och investeringar har börjat få ökat utrymme i den säkerhetspolitiska debatten i flera länder.

Den internationella terrorismen utgör ett fortsatt hot, även mot Sverige. Attacker med dödlig utgång har under 2018 utförts både i och utanför Europa.

Johan Olsson, operativ chef på Säkerhetspolisen, nämner i en intervju i Ekot att terrorism nästan alltid har haft ganska starka inslag av att man går över nationsgränser, men just nu är den trenden väldigt tydlig. Vi har hundratals personer i Sverige som har stridit för IS utomlands.

Texten på denna sida är baserad på öppna källor och inte på signalspaningsunderlag.

Kertjsundet november 2018.

Underrättelser och cyberförsvar

FRA skyddar Sverige och svenska intressen

FRA bidrar till att skydda Sverige och svenska intressen. Det gör vi på två sätt: Vi ger information om utländska förhållanden till våra uppdragsgivare och vi bidrar till att stärka informationssäkerheten hos samhällsviktig verksamhet.

Signalspaning mot utlandet ger unik information till stöd för Sveriges utrikes-, säkerhets- och försvarspolitik. FRA:s signalspaning är en betydelsefull del av Sveriges underrättelsetjänst och syftar till att ge kunskap, förvarning och djupare insikter i händelser och förhållanden i omvärlden.

Rapportering

Några exempel på ämnen för rapportering som grundar sig på FRA:s signalspaning är:

- Militära förhållanden i närområdet och militär förmåga hos andra länder.
- Internationell terrorism och eventuella hot mot Sverige.
- Avancerade IT-angrepp mot viktiga svenska informationssystem.
- Främmande underrättelseverksamhet mot Sverige.

De som kan inrikta FRA:s signalspaning är regeringen, Regeringskansliet, Försvarsmakten, Säkerhetspolisen och Nationella operativa avdelningen inom polisen. Signalspaningen måste alltid riktas mot utländska förhållanden.

Svensk signalspaning regleras tydligt i lag. Regleringen innebär bland annat att signalspaning kräver tillstånd av Försvarsunderrättelsedomstolen och att verksamheten löpande granskas av Siun (Statens inspektion för försvarsunderrättelseverksamheten).

Cyberförsvar

FRA har även uppgiften att vara statens resurs för teknisk informationssäkerhet. Det innebär att vi lämnar stöd till andra myndigheter och statliga bolag för att stärka deras förmåga att stå emot IT-angrepp. Genom kombinationen av tekniskt kunnande om angrepp och angreppsmetoder och vår signalspaning mot angripare som ligger bakom avancerade angrepp kan vi bidra med unika kompetenser till Sveriges cyberförsvar. Cyberförsvar är dock ingenting en myndighet kan göra ensam. Samverkan mellan olika myndigheter är nyckeln till framgång. Genom ett nära samarbete med främst Säkerhetspolisen, Försvarsmakten och MSB, bidrar vi till att göra Sverige säkrare.

Rättsliga frågor

Den svenska signalspaningslagstiftningen har i internationella jämförelser lyfts fram som något av en förebild. I juni 2018 kom ett utslag från Europadomstolen som slår fast att den svenska signalspaningslagen motsvarar Europakonventionens krav.

Idag avbryter FRA sin rapportering när en förundersökning inleds i ett ärende. Säkerhetspolisens och Polisens möjligheter att få underrättelseinformation via FRA:s signalspaning riskerar därför att minska när det kriminaliserade området inom terrorverksamhet utökas. Mot bakgrund av detta träffade sex av riksdagspartierna i juni 2017 en överenskommelse om åtgärder mot terrorism som syftar till att polisen fortsatt ska kunna få tillgång till nödvändig underrättelseinformation från FRA. Under 2018 presenterades ett förslag om hur signalspaningsrapportering till polisen i underrättelsesyfte ska kunna möjliggöras parallellt med en pågående förundersökning. Förslaget bereds nu i Regeringskansliet.

Terrorattentat i Melbourne 2018.

Verksamhet 2018

Terrorism

Den internationella terrorismen är ett allvarligt hot såväl globalt som i Europa och Sverige. Till skillnad från tidigare, när det främst förekom stöd och finansiering av terrorverksamhet från individer i Sverige, finns det nu en reell risk för attentat på svensk mark. FRA lämnar stöd till Säkerhetspolisen genom att rapportera om utvecklingen inom internationell terrorism i allmänhet och eventuella kopplingar till Sverige i synnerhet. Under året har detta arbete intensifierats och FRA har fått ökade anslag på detta område för att bättre kunna svara upp mot Säkerhetspolisens behov av stöd.

FRA:s rapportering till Säkerhetspolisen sker såväl löpande som i samband med särskilda händelser. Vid särskilda händelser kan FRA arbeta extra intensivt för att ge ett fullgott och unikt stöd till Säkerhetspolisen.

Närområdet

FRA har under året lämnat dagligt stöd till Försvarsmakten med rapportering om militär verksamhet i närområdet och rörelser av militära fartyg och flygplan i närheten av Sverige.

Rapporteringen kan omfatta till exempel truppförflyttningar och övningsverksamhet. FRA har även kunnat rapportera om förnyelse av militär materiel och utplacering av nya vapensystem i närområdet.

Svenska militära insatser utomlands

Ett annat område där FRA har lämnat stöd till Försvarsmakten är svenska militära insatser i utlandet. Stödet från FRA kan gälla utrustning, specialkompetens eller underrättelser och kan ges både inför, under och efter en insats.

Typiska underrättelser som rapporteras i anslutning till svensk militär insatsverksamhet utomlands ger information om aktuell hotbild mot den svenska truppen och bedömningar av utvecklingen i det aktuella landet.

Varnarbibliotek för svenska militära flygplan och fartyg

Inom området teknisk signalspaning samlar FRA in parametrar och annan data om utländska militära radarsystem. Dessa data används bland annat som underlag för varningssystem i svenska militära fartyg och flygplan i det så kallade signalreferensbiblioteket. Informationen bidrar även till förmågan att följa rörelser av utländska militära fartyg och flygplan i närområdet, och därmed även att hävda Sveriges territoriella integritet.

Kemiska stridsmedel

Forskning och utveckling samt användning av kemiska stridsmedel har varit en högaktuell fråga under det senaste året. FRA har kunnat bidra med relevant rapportering på detta område till våra uppdragsgivare.

Konflikter utomlands

Under året har ett antal kriser och konflikter fortsatt i omvärlden. FRA har kunnat rapportera unik information om pågående konflikter, bland annat i Mellanöstern.

Främmande underrättelseverksamhet

Flera länder bedriver underrättelseverksamhet riktad mot Sverige och utgör därmed ett säkerhetshot. Denna form av hot har fått större uppmärksamhet under 2018. FRA har kunnat rapportera om mål och metoder för främmande underrättelseverksamhet riktad mot Sverige och svenska intressen.


flickr
Sign Up
Instagram
Welcome to Facebook - Lo
Polska | LinkedIn
LinkedIn
facebo
Google Play
Google play
Twitter
Twitter, Inc. (US)
YouTube
YouTube

Påverkansoperationer

Påverkansoperationer av olika slag och försök att styra eller förleda media från främmande makt förekommer i dag i bred omfattning, bland annat i form av vilseledande nyhetsförmedling och så kallade nättroll. FRA har kunnat rapportera om hur denna verksamhet styrs och organiseras samt detaljer om tillvägagångssätt.

Stöd till att säkra valet

I samband med riksdagsvalet arbetade FRA tillsammans med bland andra Säkerhetspolisen och MSB och bidrog till arbetet med att säkra det svenska valet mot yttre påverkan i form av IT-attacker och andra typer av påverkansoperationer. Mot bakgrund av hotet från påverkansoperationer i allmänhet och händelserna i de amerikanska och franska valen i synnerhet fanns anledning att befara att påverkansoperationer kunde förekomma.

IT-angrepp

Hoten från avancerade IT-angrepp har varit en högaktuell fråga även under 2018. FRA har kunnat rapportera detaljer om tillvägagångssätt hos kvalificerade angripare vid angrepp både mot mål i Sverige och mot andra länder.

Man kan numera hos svenska myndigheter och statliga bolag se en väsentligt ökad medvetenhet om risken för IT-angrepp och vikten av informationssäkerhetsfrågor. Detta har i sin tur ökat efterfrågan på stöd från FRA inom informationssäkerhetsområdet. Det gäller både behov av lösningar för att myndigheter ska kunna kommunicera säkert med varandra, samt förfrågningar om IT-säkerhetsanalyser och andra former av stöd. Under året har FRA genomfört IT-säkerhetsgranskningar och lämnat stöd till uppbyggnaden av ett antal samhällsviktiga system.

Varningssystem

TDV-systemet, ett varningssystem som utvecklats av FRA och som syftar till att larma om pågående IT-angrepp, är en ordinarie del av det stöd som FRA kan erbjuda sina uppdragsgivare inom informationssäkerhetsområdet. Systemet har under 2018 installerats på ett antal ytterligare myndigheter och statligt ägda bolag. Till följd av denna utbyggnad har även FRA stärkt sin förmåga att analysera och bearbeta den ökade mängden indata. Systemet har under året kunnat upptäcka flera avancerade intrångsförsök från kvalificerade angripare mot svenska mål.

På FRA pågår nu ett arbete med att vidareutveckla TDV-systemet med tillvaratagande av de erfarenheter och resultat man hittills vunnit. Avsikten är att systemet inte bara ska kunna larma för angrepp utan även automatiskt kunna avbryta pågående angrepp.

Nytt signalspaningsfartyg

Fartygsburen signalspaning

Fartygsburen signalspaning är viktig för att kunna inhämta intressanta signaler som inte skulle kunna uppfångas från fastlandet. Ett fartyg kan ligga närmare källan till signalerna och därmed inhämta svagare signaler än vad som är möjligt från land. Samarbetet mellan FRA:s signalspaning och de visuella observationer som marinen gör från bryggan är också unikt för fartygsburen inhämtning. Jämfört med signalspaningsflygplan, som också är en kvalificerad signalspaningsresurs och rör sig över stora områden på kort tid, har ett signalspaningsfartyg större uthållighet och kan bevaka längre förlopp över tid. Det huvudsakliga operationsområdet för den fartygsburna signalspaningen är sydöstra Östersjön.

Det nuvarande signalspaningsfartyget HMS Orion har blivit ålderstiget, och ett ersättningsfartyg är nu under byggnad. I mars 2018 skars de första plåtbitarna ut till det nya fartyget på varvet Nauta i Gdynia i Polen. Detta har föregåtts av en lång period av förarbeten med kravställning där FRA, Försvarsmakten, Försvarets materielverk och Saab Kockums samt Nauta deltagit.

Samtidigt som varvet i Polen började bygga fartyget inleddes en hög aktivitet på FRA med tekniska förberedelser. Det gäller bland annat upphandling av antenner och annan teknik samt förberedelser för installation av signalspaningsutrusning till det nya fartyget.

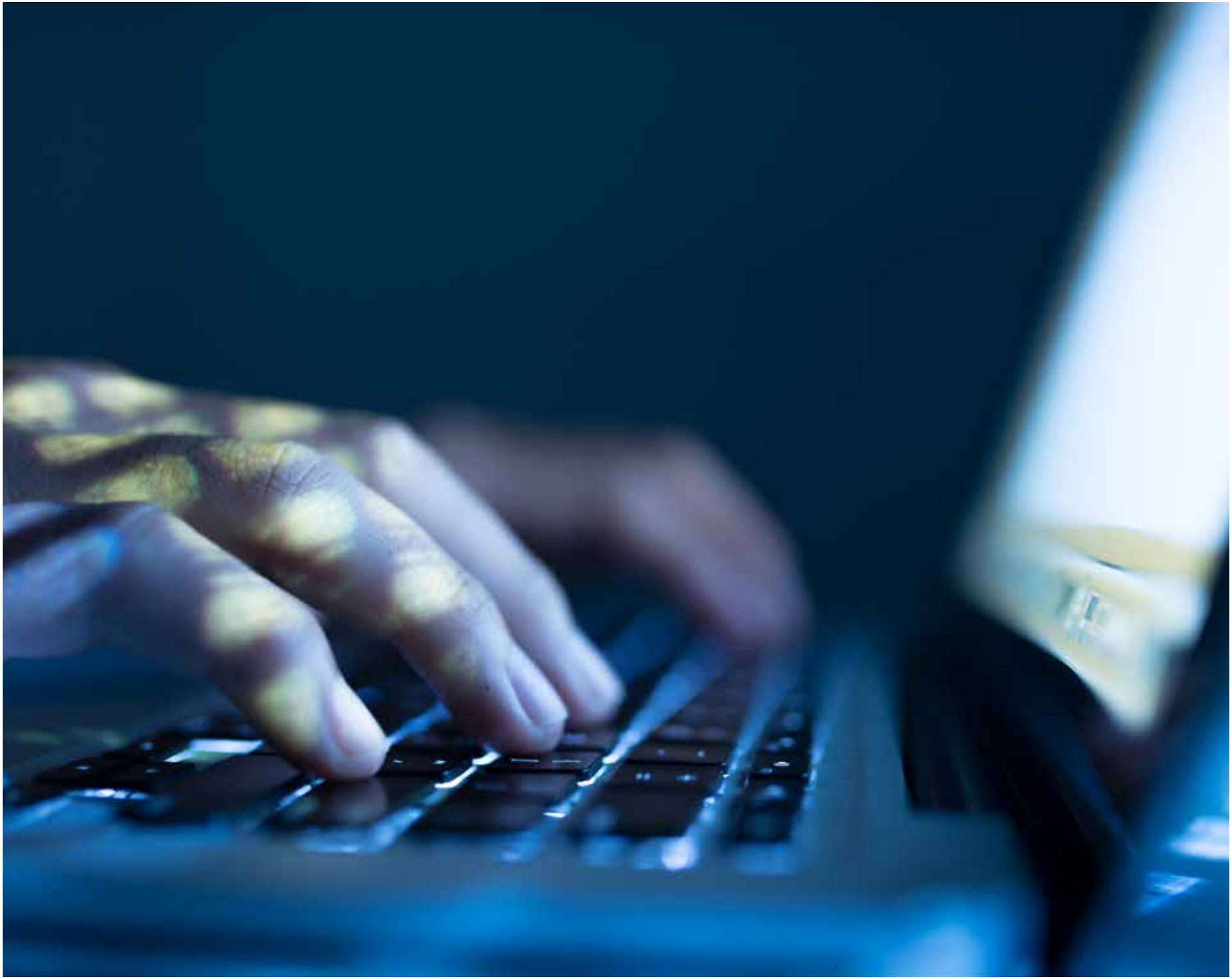
Kölsträckning

15 juni 2018 var en milstolpe i projektet då kölsträckningsceremonin av fartyget skedde på varvet i Polen med deltagande från FRA i form av generaldirektör Dag Hartelius.

Under hösten fortsatte bygget i Polen och våren 2019 ska sjösättning ske och varvet kommer att göra fartyget klart för leverans. Då görs hela inredningen och nödvändiga sjötester innan hon går till Karlskrona, dit hon enligt plan ska ankomma senare under året. När fartyget kommit till Karlskrona kommer installation av signalspaningsutrustningen att påbörjas.

Viktiga teknikprojekt

Under kommande år kommer teknikavdelningen på FRA att arbeta med flera olika projekt för att ta fram signalspaningssystemen till det nya fartyget. Nya förmågor utvecklas samtidigt som det sker en modernisering av redan befintliga förmågor.



Cyberattacker mot Sverige – hur ser de ut?

Cyberangrepp från andra stater största hotet

Med internet har världen fått ett verktyg för omedelbar global kommunikation. Denna positiva utveckling har dock även medfört möjligheten att lika globalt göra intrång i andras nätverk. Under 2018 har frågan om IT-angrepp och hur Sverige bör organisera sitt cyberförsvar diskuterats i olika sammanhang. Tillsammans med andra berörda myndigheter har FRA under året pekat på möjligheterna till ett fördjupat myndighetssamarbete för att stärka det svenska cyberförsvaret.

Skadlig kod med tydliga syften

Sådana cyberattacker som organiseras av stater syftar oftast till att komma över information. Exempelvis vill de attackerande staterna få reda på strategierna bakom Sveriges utrikespolitik, vårt samhälles sårbarheter samt kartlägga Sveriges totalförsvar. Det kan också handla om förberedelser för senare angrepp och störningar.

Många företag och lärosäten har sina servrar fulla med forskningsresultat, utvecklingsprojekt och patentansökningar. Dessa representerar enorma värden för den stat som vill gå genvägar i sin egen näringslivs- och teknikutveckling. I praktiken kan det innebära att de företag som utvecklat ny teknik konkurreras ut av sina egna lösningar, realiserade av företag i de länder som ägnar sig åt företagsspionerі på nätet. Inte minst för ett utrikeshandelsberoende land som Sverige är det viktigt att vara en säker marknadsplats.

Att skaffa sig otillbörligt tillträde till de nätverk som styr samhällsviktig verksamhet kan också göras med målet att vid ett senare tillfälle störa eller slå ut samhällsviktiga funktioner.

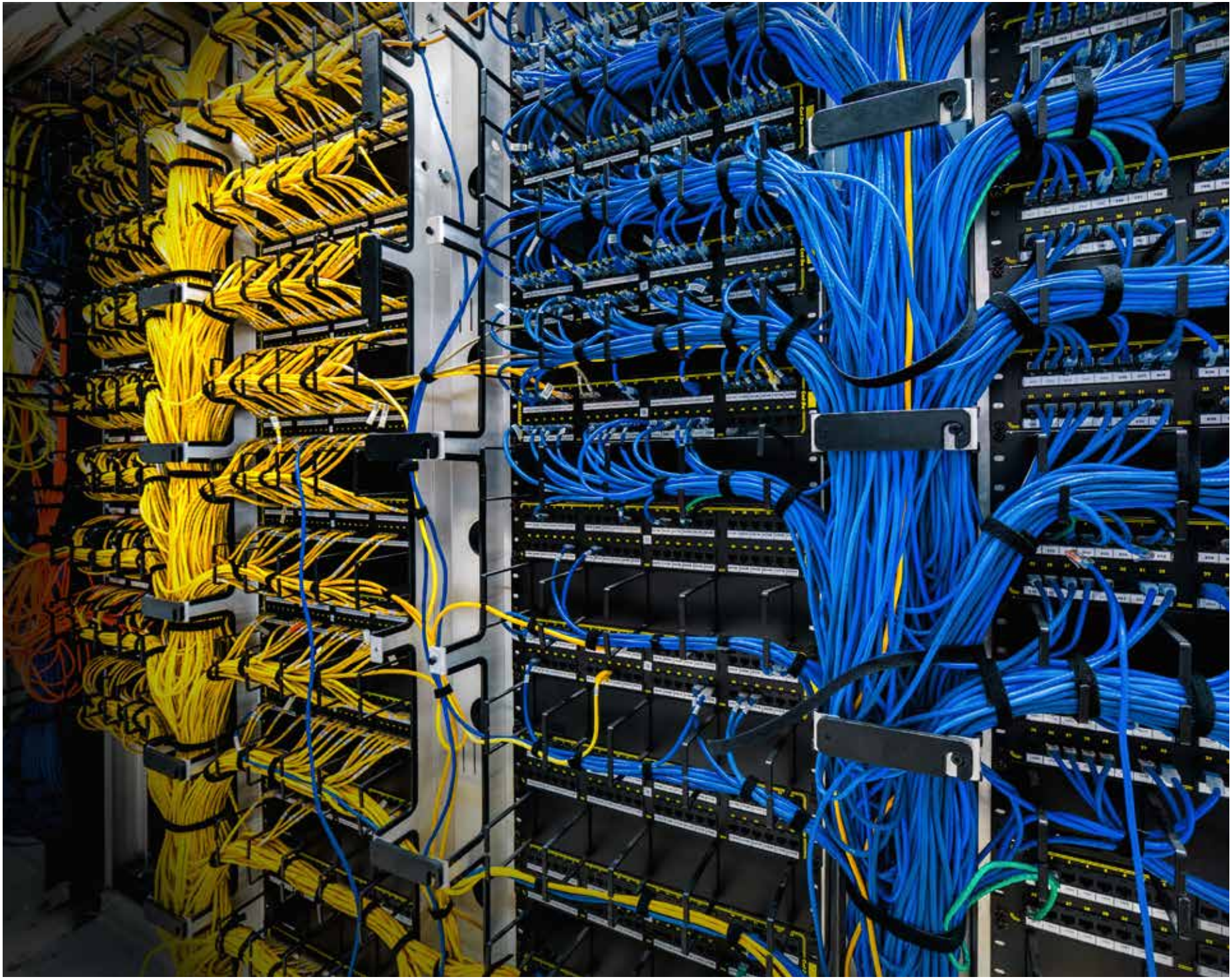
Statliga cyberattacker pågår ständigt och ökar

FRA ser ett stort antal aktiviteter från angripare i andra länder som är avsedda att gå runt de säkerhetssystem som ska skydda oss från informationsförluster och sabotage. Dessa pågår ständigt. Vi ser också konkreta exempel på intrångsförsök från utlandet mot viktiga svenska system där de som genomfört intrången troligen lyckats i sitt uppsåt att stjäla information.

Antalet statsunderstödda cyberangrepp ökar fortlöpande och angriparnas metoder utvecklas. Skadlig kod blir allt mer sofistikerad.

Skadlig kod i e-post

De sätt som utländska stater försöker hacka svenska samhällsviktiga system på är många. Ett av de vanligaste tillvägagångssätten för en angripare att få tillträde till svenska samhällsviktiga system är att skicka e-postmeddelanden med skadlig kod till anställda eller till deras anhöriga. Dessa e-postmeddelanden blir allt mer sofistikerade och väcker många gånger ingen misstanke ens hos den vaksamme. Andra sätt kan vara att gå via nätbaserade tjänster för medborgarna eller att placera ut skadlig kod hos outsourcingföretag eller tredjepartsleverantörer.



Mot ett svenskt cyberförsvar

Förbättring är möjlig och nödvändig

Trots att de statligt stödda cyberangreppen ökar i omfattning, och dessutom blir allt mer avancerade, bör vi inte misströsta när det gäller våra möjligheter att agera. Genom anpassade system, kompetent personal och förmåga att hantera attacker kan informationssäkerheten höjas. Det kräver dock ett bra, nära och långsiktigt samarbete på alla nivåer.

Omfattande verksamhet

Under de senaste åren har bristen på informationssäkerhet i enskilda fall kommit att ådra sig stort allmänt intresse. Det är angeläget att understryka både den stora omfattningen av de statsunderstödda cyberangreppen och det hot mot vårt samhälle, vårt välstånd och mot allas vår integritet som dessa innebär.

När inte ens en hög tröskel räcker

Alla enheter som är kopplade till internet går att hacka sig in i. Det är ytterst en fråga om huruvida den som vill vinna tillträde förfogar över den tid, kompetens och de resurser som krävs. I vissa fall har system som aldrig varit avsedda att kopplas till internet kopplats upp i efterhand utan att säkerheten anpassats för detta. Vissa system bör över huvud taget inte vara uppkopplade till det globala nätet.

Samverkan grunden för effektivt cyberförsvar

Under 2018 har FRA som bidrag till debatten om hur Sveriges framtida cyberförsvar ska se ut betonat vikten av fördjupad samverkan mellan myndigheter och mellan myndigheter och privata företag, exempelvis i form av ett nationellt cybersäkerhetscenter. FRA har intensifierat sitt samarbete med Säkerhetspolisen, Försvarsmakten och MSB. Till de frågor som myndigheterna för närvarande tittar på hör behovet av olika förmågor för en sammanhängande helhet, organisatoriska aspekter och offentlig-privat samverkan. Kompetensförsörjningen på området är också avgörande för våra möjligheter att på sikt utveckla ett cyberförsvar som klarar att möta hoten.

Ett samlat beslutsunderlag

Rapporteringen till beslutsfattare skulle kunna utgöra ett bättre samlat underlag än idag. Under 2018 har FRA tillsammans med Försvarsmakten och Säkerhetspolisen byggt upp en mer aggregerad rapportering. Detta arbete fortsätter.

Vad gör FRA inom Sveriges cyberförsvar?

Kopplingen underrättelser och informationssäkerhet i Sverige

FRA har två huvuduppgifter inom cyberförsvaret. Myndigheten ska dels utföra signalspaning mot utländska förhållanden, däribland cyberhot som kommer från utländska stater, dels stödja myndigheter och statligt ägda bolag i deras informationssäkerhetsarbete.

1. Vi ser cyberattacker på internet

Genom signalspaningen kan vi se hur vissa stater angriper mål i sin omvärld. Vi ser vilka typer av mål de angriper och vilka angreppsmetoder de har utvecklat. FRA använder den kunskapen för att undersöka om samma skadliga kod riktas mot samhällsviktig verksamhet i Sverige.

2. Genom kännedom om attacker mot Sverige får vi än mer kunskap om angreppen

Fördelarna med kombinationen av uppgifter går också omvänd väg. Genom att söka ursprunget till skadlig kod vi funnit i Sverige kan FRA rapportera om hur främmande stater agerar i det globala nätet.

Mot den bakgrunden behöver ett effektivt svenskt cyberförsvar även bygga på underrättelseinhämtning om vad som sker i det globala nätet.

TDV på fler myndigheter

FRA har utvecklat ett tekniskt detekterings- och varningssystem (TDV) som fungerar som en sorts avancerat virusskydd. Systemet finns utplacerat hos svenska myndigheter och statliga bolag och kan varna för pågående angrepp. Under 2018 har FRA placerat ut ett antal nya TDV hos uppdragsgivare.

TDV utvecklas löpande. Systemet ska i framtiden förutom att varna för angrepp också kunna stoppa pågående angrepp.

FRA bistår myndigheter och statliga bolag

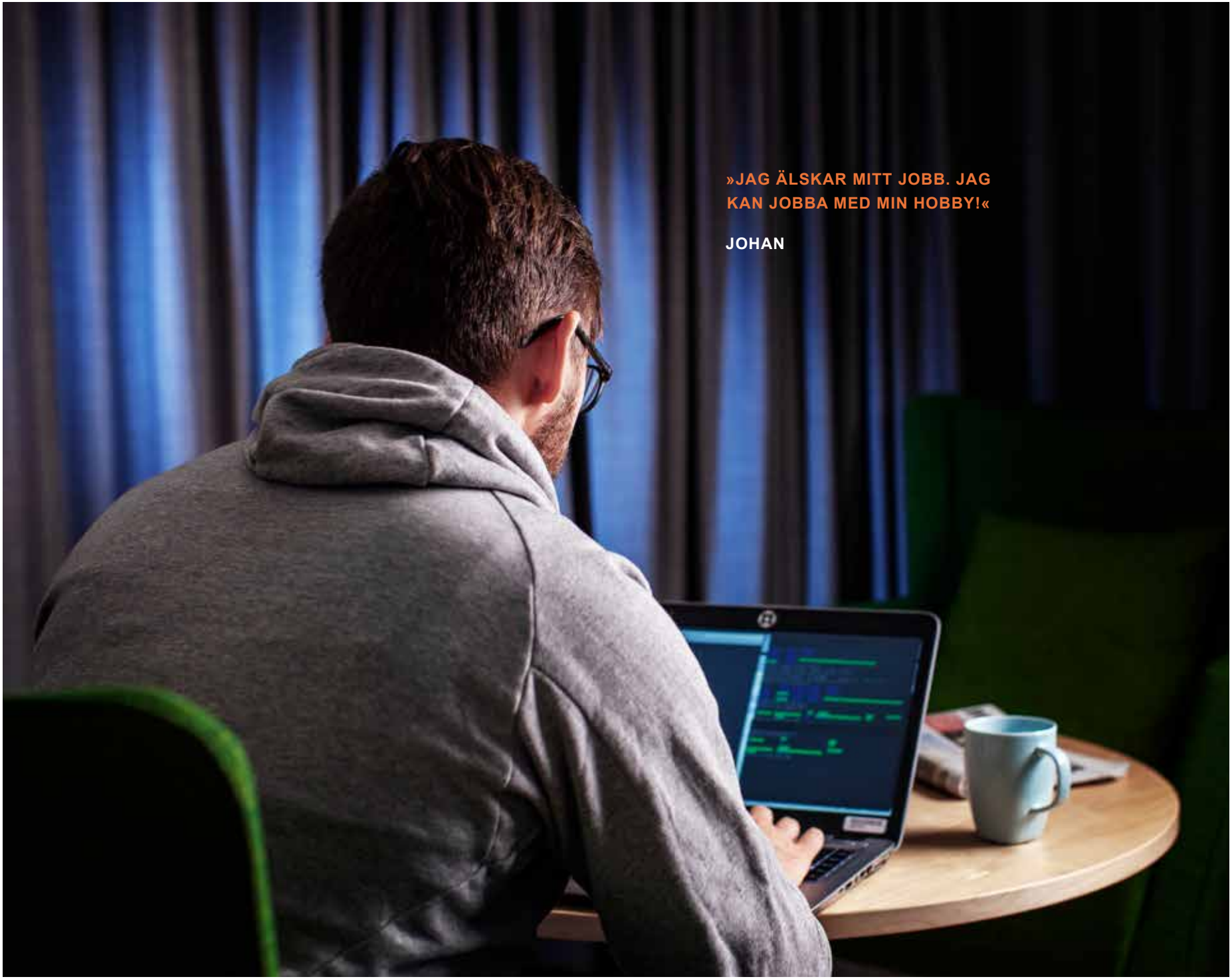
FRA kan bistå myndigheter och statligt ägda bolag med att testa säkerheten i deras IT-system. Vid sådana tillfällen försöker vår personal ”hacka sig in” hos uppdragsgivaren på deras uppdrag för att upptäcka brister och svagheter. Därefter lämnar vi förslag till förbättringar av säkerheten som bör genomföras.

Resultaten av dessa tester varierar. Nästan alltid hittar man någon sårbarhet. Detta ska inte tolkas som att säkerheten generellt sett är låg, men som en påminnelse om att myndigheternas informationssäkerhet ständigt behöver prövas för att hitta sådant som bör förbättras.

Regeringsuppdrag och stöd till utveckling av offensiv förmåga

Vidare har FRA arbetat enligt ett regeringsuppdrag att tillsammans med Säkerhetspolisen ge ett ökat stöd till informationssäkerheten hos de mest skyddsvärda verksamheterna. Det innebär bland annat ett stärkt proaktivt stöd och förbättringar i förmågan till incidenthantering. Som en del i uppdraget har man även börjat ta fram aggregerad information om hot och sårbarheter. Denna information kan utgöra ett underlag för beslutsfattare och ligga till grund för olika åtgärder inom informationssäkerhetsområdet.

FRA lämnar även stöd till Försvarsmakten i att analysera och utveckla en svensk offensiv förmåga på cyberområdet.



»JAG ÄLSKAR MITT JOBB. JAG KAN JOBBA MED MIN HOBBY!«

JOHAN

Vi hjälper andra att bli bättre

Johan är 29 år och jobbar på FRA:s Cyberavdelning.

När började du hålla på med datorer?

Mitt stora intresse började väl när jag var 16–17 år. Jag blev intresserad av Linux. Började hålla på att sätta upp egna servrar och så. Jag är lite av en Linux-fantast.

När jag gjort klart lumpen blev jag tekniker i armén. På fritiden höll jag på med Linux som hobby. Sen tänkte jag att jag kanske kunde tjäna pengar på mina kunskaper, så jag gick en kurs på yrkeshögskolan för att få papper på vad jag kunde. Efter ett år fick jag ett jobb.

Men det har faktiskt alltid varit mitt mål att jobba på FRA, i säkert tio år. Ända sedan FRA-debatten.

Blev du avskräckt av FRA-debatten?

Jag var ju själv en de unga datorentusiasterna på den tiden. Men jag tänkte att det här som de sa att FRA skulle jaga fildelare, det kunde ju inte stämma. Nog måste de ha viktigare saker för sig?

Men varför ville du jobba på just FRA?

För mig har det alltid varit viktigt att göra något större än jag själv, att hjälpa andra. Det var därför jag ville bli militär, men sen fick jag upp ögonen för att det fanns andra sätt att göra något för Sverige än i det militära.

Hur ser en dag ut för dig?

Just nu är det mycket kundbesök för att få till planering och avtal inför kommande jobb. Och om det inte är jobb åt kunder så är det mycket kompetensutveckling, och utveckling av vår teknik.

Vilken typ av kompetensutveckling ägnar ni er åt?

Ofta är det självstudier. I princip får jag betalt för att lära mig grejer som jag tycker är kul. Man behöver faktiskt inte vara bäst för att jobba på FRA, som det står i våra rekryteringsannonser, men man måste vara nyfiken och ha en vilja att utvecklas.

Vad är roligast med att jobba på FRA?

Jag tycker det är kul att hjälpa andra att bli bättre, hjälpa dem att lyckas. Hjälpa dem att hitta bristerna i deras system. Men det är tyvärr ganska många brister vi hittar.

Vilka är de vanligaste säkerhetsbristerna ni hittar?

Ingen segmentering i nätverken, alltså att vanliga användare kommer åt administratörsfunktioner.

Svag autentisering. Man borde ha tvåfaktorsautentisering (anm: att man måste ha både lösenord och någon fysisk utrustning, till exempel kort, för att logga in).

Och det är dåliga lösenord.

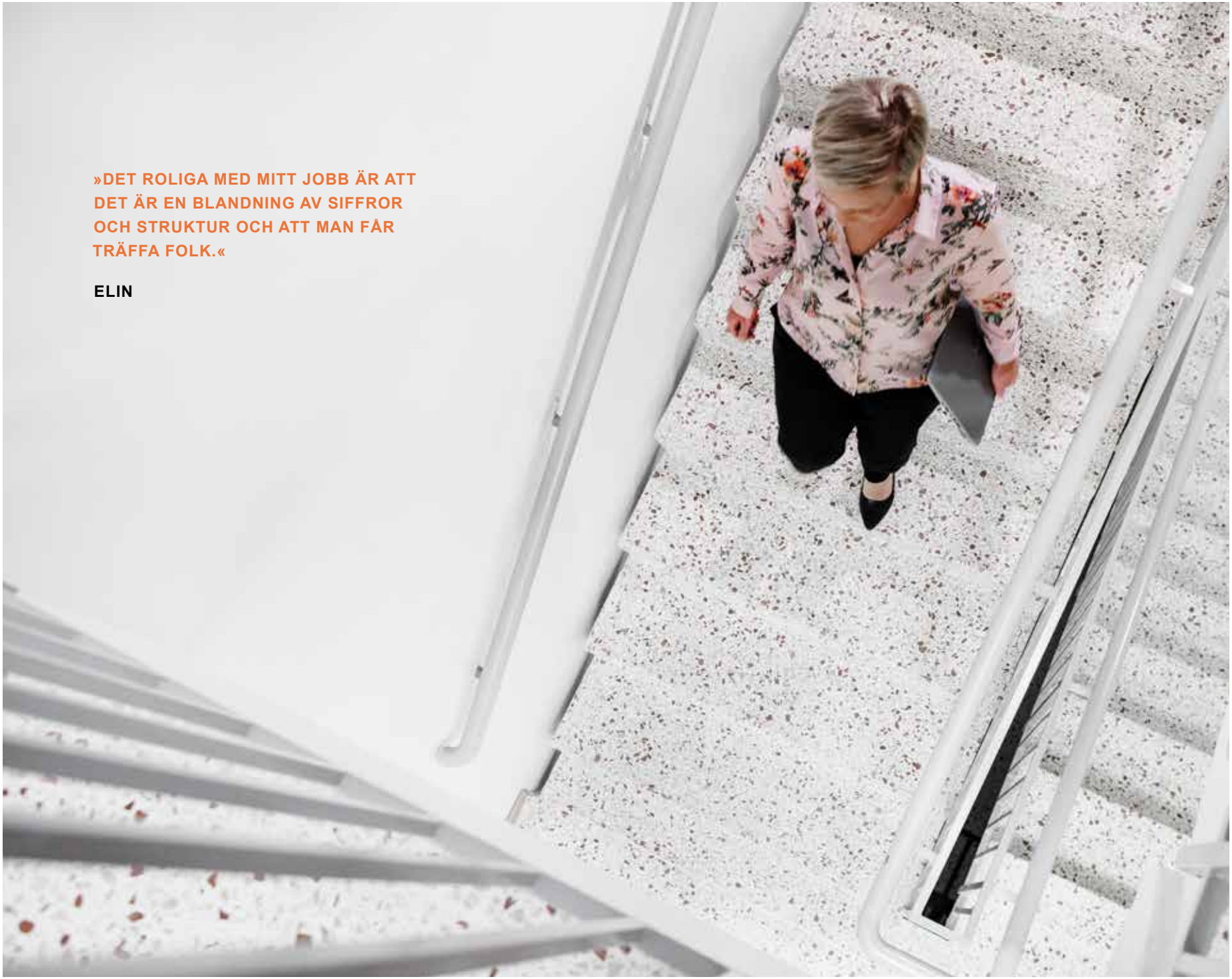
Finns det något som är dåligt med att jobba på FRA?

Jag älskar mitt jobb. Jag kan jobba med min hobby! Men om det är något som inte är så bra är det lokalerna. Det strider lite mot FRA-bilden jag hade innan jag började, jag tänkte mig det lite science fiction-artat, men det har varit mycket strul med lokalerna, just nu sitter vi ganska trångt.

Läget är lite off, men det finns fördelar med det också. Man kan gå lunchpromenader i omgivningarna. Det är bra att det finns eget gym också. Jag går på gymmet 3–4 dagar i veckan. Jag har ju barn, och när man kommer hem finns det inte tid att gå och träna.

Vad skulle du ge som viktigaste säkerhetstips?

Stäng inte av det inbyggda säkerhetsskyddet! Många stänger av skyddsmekanismer för att det blir bekvämare då, men då öppnar de sig för angrepp. Så stäng aldrig av brandväggar eller applikationslås bara för att det är bekvämt!



»DET ROLIGA MED MITT JOBB ÄR ATT DET ÄR EN BLANDNING AV SIFFROR OCH STRUKTUR OCH ATT MAN FÅR TRÄFFA FOLK.«

ELIN

Hur man bäst använder de pengar man fått

Elin är controller och har tidigare arbetat inom den privata sektorn, men arbetar nu sedan tre år på FRA.

Vad gör en controller?

Det kan vara lite olika saker på olika ställen. Det är mycket budget, prognoser, ekonomisk analys och uppföljning. Man deltar i bokslutsarbete och i arbete med årsredovisningen. Sen är det olika utvecklingsprojekt. Till exempel hur vi ska förbättra redovisningen för att cheferna ska förstå sina ekonomiska utfall bättre.

Vad har en controller för utbildning?

Jag är civilekonom, jag har gått det internationella ekonomprogrammet med språkinriktning. Det finns faktiskt en hel del likheter mellan redovisning och språk. Det finns struktur och former, både inom ekonomi och när det gäller språk. Jag tycker det är roligt med siffror och struktur. Och det roligaste, det är när jag kan förklara för andra så att de förstår!

Vilket språk lärde du dig?

Jag hade inriktning tyska och tillbringade en termin som utbytesstudent i södra Tyskland. Sedan har jag jobbat på ett tyskt företag.

Har du alltid velat bli ekonom?

Det var under gymnasiet som jag upptäckte ekonomi och redovisning. Jag gillade logiken och ordningen. Ett tag hade jag tankar på att bli journalist eller bibliotekarie. Men det blev ekonomi.

Hur ser en arbetsdag ut för dig?

Det beror en del på vilken tid på året det är. Just nu är det mycket med budget och med förberedelser för årsbokslutet. Idag har jag förklarat budgetprocessen för en nyanställd. Sedan har jag träffat avdelningschefen och redogjort för det ekonomiska läget. Och jag har förberett ett möte om årsredovisningen.

Det som är roligt med mitt jobb är att det är en blandning av siffror och struktur och att man får träffa folk. Jag är bollplank till drygt 30 chefer på olika nivåer när det gäller ekonomin. Jag får både tillfälle att vara social och att sitta själv framför datorn och tänka.

Vad är det bästa med att jobba på FRA?

Att så många kan så mycket om olika saker här. Det finns så mycket olika kunskaper. Och det är roligt att möta alla de chefer jag har att göra med, de fungerar alla lite olika.

Hur är det att arbeta på en statlig myndighet jämfört med att arbeta i den privata sektorn?

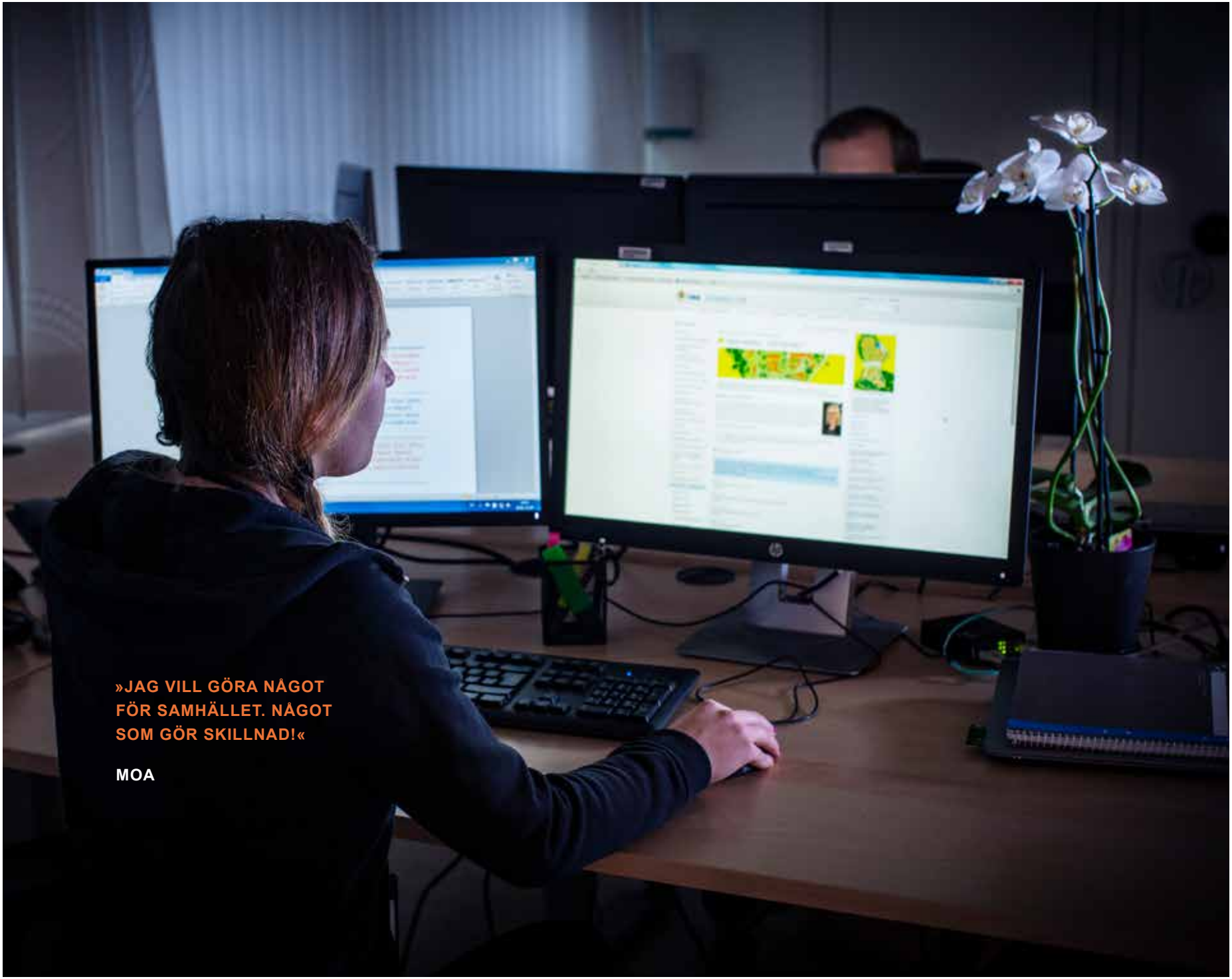
När man jobbar privat har man ju ett lönsamhetsfokus, hur man ska få så bra avkastning på pengarna som möjligt. I staten handlar det om hur man bäst använder de pengar man har fått. Men i det dagliga så skiljer det sig inte så mycket.

Många tycker kanske att det låter tråkigt med ekonomi?

Jo, oavsett var jag jobbar tycker ju folk att det här med ekonomi låter lite tråkigt. Och pratar man revision då tycker de flesta verkligen att det låter torrt. Men jag tycker om att förklara, och ibland märker jag att min entusiasm smittar av sig.

Vad gör du på fritiden?

Jag umgås med familj och vänner. Och jag tränar en hel del. Just nu tränar jag för Vasaloppet. Annars gillar jag friluftsliv och att vara utomhus överhuvudtaget. Segling, paddla kajak, långfärdsskridsko. Jag är uppvuxen med segelbåt.



»JAG VILL GÖRA NÅGOT FÖR SAMHÄLLET. NÅGOT SOM GÖR SKILLNAD!«

MOA

Från KTH till FRA

Moa har arbetat på FRA i två månader och kommer direkt från en utbildning på Kungliga Tekniska högskolan i Stockholm.

Hur kom du till FRA?

Jag gick på KTH, och så var jag på arbetsmarknadsdagarna Armada. Det var flera myndigheter som var där. Jag fastnade för FRA och stod och pratade där en stund. De visade bland annat hur man hackar en dator. Just när jag skulle gå så sa de att de tyckte att jag skulle vara med i deras tävling. Jag gjorde tävlingen, och vann. Så jag var en av femton studenter som fick komma på besök till FRA, det var jättespännande. Där berättade de mer om FRA, och uppmanade mig att skicka in mitt CV.

Sen ringde de och frågade om jag ville komma på intervju. Jag frågade vilken tjänst det gällde, men det kunde de såklart inte säga då. Jag gick på flera intervjuer, och så småningom blev jag anställd.

En av mina kompisar som också var på Armada blev jätteavundsjuk. Hon hade också tyckt att FRA verkade intressant.

Vad läste du på KTH?

Jag läste civilingenjörsprogrammet med inriktning på beräkningsmatematik.

Vad gör du nu på dagarna på FRA?

Jag har bara jobbat i två månader så jag är fortfarande under upplärning. Nu har jag en uppgift där jag programmerar i Python, jag gör ett program som ska underlätta för analytikerna. Det här programmet kommer att hjälpa mycket. Saker som tog lång tid förut kommer de att kunna göra mycket fortare. Man kan säga att det gör det mycket lättare att söka och presentera data.

Vad är roligast med jobbet?

Jag lär mig nya saker hela tiden. Jag behöver aldrig göra samma sak. Jag utbyter kunskap med andra, människor som kan saker som jag inte kan.

Vad är det som är mindre roligt?

Oj! Jag tror inte det finns något sånt. Det är roligt att gå till jobbet varje dag!

Vad är det som är bäst med att jobba på just FRA?

Alla är trevliga. Man gör saker som har betydelse här. Men det verkar inte som folk utanför FRA har så bra koll på vad vi gör här.

Vad säger du om du är på en middag och den bredvid dig frågar om ditt jobb?

Jag försöker att inte berätta så mycket. Ibland om man säger att man jobbar på FRA så blir det ofta att de frågar om man läser deras e-post och så. Det kan man ju oftast skoja bort.

Vilka egenskaper tycker du att man ska ha om man ska jobba här på FRA?

Man ska vara nyfiken och driven. Och man ska vilja göra något för samhället. Något som gör skillnad.

Vad ville du bli när du var liten?

Jag ville bli danslärare, och sen ville jag bli kock. Men då sa min mamma att då behövde man jobba på högtiderna, så då tänkte jag om.

Vad gör du på fritiden?

Jag tränar mycket och umgås med kompisar. Sen tycker jag om att resa.

KUNSKAP OM UTLANDET –
FÖR SVERIGES SÄKERHET OCH INTEGRITET

Utgiven av FRA | Grafisk form: SINFO YRA | Foto: Björn Tesch, Jonathan Nackstrand, AFP, James Ross, Saab AB, iStock | Tryck: Åtta45 2019